Secret Sharing from Correlated Gaussian Random Variables and Public Communication

Vidhi Rana, Rémi A. Chou, and Hyuck Kwon
Wichita State University, Wichita, Kansas, U.S.A.
vxrana@shockers.wichita.edu, remi.chou@wichita.edu, and hyuck.kwon@wichita.edu

***Abstract*—We study a secret sharing problem, where a dealer distributes shares of a secret among a set of participants under the constraints that (i) authorized sets of users can recover the secret by pooling their shares, (ii) non-authorized sets of colluding users cannot learn any information about the secret. We assume that the dealer and the participants observe the realizations of correlated Gaussian random variables and that the dealer can communicate with the participants through a one-way, authenticated, rate-limited, and public channel. Our main result is a closed-form characterization of the trade-off between secret rate and public communication rate. Unlike traditional secret sharing protocols, in our setting, no perfectly secure channel is needed between the dealer and the participants, and the size of the shares does not depend exponentially but rather linearly on the number of participants and the size of the secret for arbitrary access structures.**

I. Introduction

Secret sharing has been introduced in [1], [2]. 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 [1], it is assumed that the dealer and each participant can communicate over a perfectly secure channel at no cost. While these resources could be implemented with public-key cryptography techniques [3], 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 cryptographic results such as public-key cryptography*. In other words, we want to avoid the assumption that perfectly secure communication channels are available at no cost. An information-theoretic approach to secret sharing over wireless channels has been introduced in [4] for this purpose. The main idea is to leverage channel noise by remarking that secret sharing over wireless channels is similar to compound wiretap channel models [5]. This information-theoretic approach is also formulated for source models in [6], [7], where participants and dealers hold correlated random variables. These models are related to compound secret key generation, e.g., [8], and biometric systems with access structures [9].

While capacity results are known for Gaussian channel models [5], in this paper, we study the trade-off between public communication and secret rate for a Gaussian source model similar to [7]. 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 public communication channel. In wireless networks, independently and identically distributed realizations of correlated random variables can, for instance, be obtained from channel gain measurement after appropriate manipulations [10], [11]. Our approach for the achievability consists in handling the reliability and secrecy requirement separately. 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 [12]. However, unlike in [12], 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 degradedness assumption on the source model.

The main features of our work can be summarized as follows: (i) Unlike traditional secret sharing schemes [1], [2], our model does not rely on the assumption that perfectly secure channels between the dealer and the participants are available, instead, our model relies on correlated Gaussian random variables. (ii) We strengthen the security of traditional secret sharing schemes, by providing 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 depends linearly on the number of participants and the size of the secret, which contrasts with traditional secret sharing schemes for which the size of the shares can grow exponentially with the number of the participants for arbitrary access structures [13]. (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 *not* a

Rémi A. Chou was supported in part by NSF grant CCF-1850227.

978-1-7281-5962-1/21/$31.00 ©2021 IEEE

monotonic decreasing 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 their 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 the 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 a random variable X, let σ_X^2 denote its variance. $N \sim \mathcal{N}(0, \Sigma)$ denotes 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.

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 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 which belongs to $\mathbb{A}$, then $\mathcal{T}$ also belongs to $\mathbb{A}$, i.e., $\mathbb{A}$ is a monotone access structure [13]. 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 $\mathcal{A} \in \mathbb{A}$, 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 said to be 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, which is meant to maximize the uncertainty of guessing S by the users in $\mathbb{U}$. The secret capacity region is defined as $\mathcal{R}(p_{XY_{\mathcal{L}}}, \mathbb{A}) \triangleq \{(R_p, R_s) : (R_p, R_s)$ is achievable$\}$. 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 $C_s(\mathbb{A}, R_p)$. Finally, one can write for any $\mathcal{A} \in \mathbb{A}$ and for any $\mathcal{U} \in \mathbb{U}$

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

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

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 $W_{Y_{\mathcal{U}}} \sim \mathcal{N}(0, I_{|\mathcal{U}|})$. The proof is omitted due to space constraints.

IV. Main Results

A. Results for general access structures

For any access structure $\mathbb{A}$, we consider two sets $\mathcal{A}^\star \in \arg\min_{\mathcal{A} \in \mathbb{A}} H_{\mathcal{A}}^T H_{\mathcal{A}}$ and $\mathcal{U}^\star \in \arg\max_{\mathcal{U} \in \mathbb{U}} H_{\mathcal{U}}^T H_{\mathcal{U}}$.

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*

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

The converse and achievabilty 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*

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

Note that in Theorem 1 and Corollary 1, the length of the total communication is linear with the length of the secret by construction. Hence, the size of the share of one participant, which comprises the public communication from the dealer and n observations of a Gaussian random variable, scales linearly with the length of the secret for any choice of the access structure $\mathbb{A}$. This is in sharp contrast with traditional secret sharing models, where the size of the shares may scale exponentially with the number of participants for general access structures [13].

B. Results for threshold access structures

We now consider a special kind of access structure. 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.

Theorem 2 provides necessary and sufficient conditions to determine whether the secret capacity increases or decreases as the threshold t increases. It also illustrates the fact that the

secret capacity is not a monotonic decreasing function of the threshold t. We omit the proof due to space constraints.

Theorem 2. *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*

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

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

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

Example. *Consider a dealer and five participants. For $\sigma_X^2 \triangleq 2$, $H_\mathcal{L} \triangleq [1, 0.85, 0.9, 0.95, 0.75]^T$, one can compare the secret capacities for different thresholds using Theorem 2, as shown in Figure 1. For example, 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 $R_p \geq 0$.*

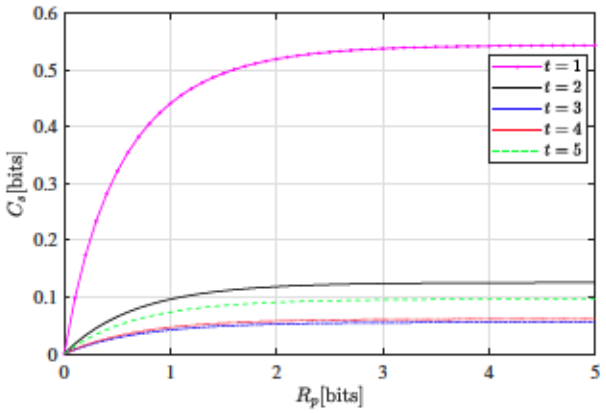

Figure 1. Secret capacity for a threshold access structure.

V. Converse Proof of Theorem 1

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). *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 $f_{c,d}$ from $\mathbb{R}_+$ to $\mathbb{R}$ is non-decreasing, where*

$$f_{c,d} : x \mapsto \frac{1}{2}\log\frac{cx+1}{dx+1}.$$

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*

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

The proof is omitted due to space constraints.

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*

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

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

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

we have that $I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U})$ is a non-increasing function of $\sigma_{X|V}^2$ by Lemma 2 because $O_\mathcal{A} \geq O_\mathcal{U}$. Hence, $\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U})$ must be the smallest $\sigma_{X|V}^2 \in (0, \sigma_X^2]$ that satisfies the constraint $I_p(\sigma_{X|V}^2, \mathcal{A}) \leq R_p$. However, $I_p(\sigma_{X|V}^2, \mathcal{A})$ is a non-increasing function of $\sigma_{X|V}^2$, thus we must have $I_p(\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}), \mathcal{A}) = R_p$, from which one can deduce that

$$\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}) = \frac{\sigma_X^2}{\sigma_X^2 O_\mathcal{A}(2^{2R_p}-1) + 2^{2R_p}}. \quad (8)$$

□

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 $R_p \in \mathbb{R}_+$. We have*

$$\min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} \max_{\substack{0<\sigma_{X|V}^2\leq\sigma_X^2 \\ \text{s.t. } I_p(\sigma_{X|V}^2,\mathcal{A})\leq R_p}} I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U}) = \max_{\substack{0<\sigma_{X|V}^2\leq\sigma_X^2 \\ \text{s.t. } I_p(\sigma_{X|V}^2,\mathcal{A}^\star)\leq R_p}} \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U}). \quad (9)$$

Proof. By Lemma 2, we have for any $\sigma_{X|V}^2 \in (0, \sigma_X^2]$, $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$,

$$\frac{1}{2}\log\frac{\sigma_X^2 O_\mathcal{A}+1}{\sigma_{X|V}^2 O_\mathcal{A}+1} \geq \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}^\star}+1}{\sigma_{X|V}^2 O_{\mathcal{A}^\star}+1},$$

$$-\frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}}+1}{\sigma_{X|V}^2 O_{\mathcal{U}}+1} \geq -\frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}^\star}+1}{\sigma_{X|V}^2 O_{\mathcal{U}^\star}+1},$$

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

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

Then, we have

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

where in (a) we have defined $\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}) = \arg\max_{\substack{0<\sigma_{X|V}^2\leq\sigma_X^2 \\ \text{s.t. } I_p(\sigma_{X|V}^2,\mathcal{A})\leq R_p}} I_s(\sigma_{X|V}^2,\mathcal{A},\mathcal{U})$ for $\mathcal{A}\in\mathbb{A}$, $\mathcal{U}\in\mathbb{U}$, (b) holds because for any $\mathcal{A}\in\mathbb{A}$, $\mathcal{U}\in\mathbb{U}$, we have $I_s(\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}),\mathcal{A},\mathcal{U}) \geq I_s(\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}),\mathcal{A}^\star,\mathcal{U}^\star) \geq I_s(\sigma_{X|V}^{2\star}(\mathcal{A}^\star,\mathcal{U}^\star),\mathcal{A}^\star,\mathcal{U}^\star)$, where the first inequality holds by (10), and the second inequality holds because $I_s(\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U}),\mathcal{A}^\star,\mathcal{U}^\star)$ is a non-increasing function of $\sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U})$ by Lemma 2, and $\sigma_{X|V}^{2\star}(\mathcal{A}^\star,\mathcal{U}^\star) \geq \sigma_{X|V}^{2\star}(\mathcal{A},\mathcal{U})$ 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 $f_{\sigma_X^2,\sigma_{X|V}^2}$. 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) and (2). Specifically, as described next, we repeat $q\in\mathbb{N}$ times a reconciliation step to handle (1) and then perform a privacy amplification step to handle (2).

1) Reconciliation step: Let $n\in\mathbb{N}$ and $\epsilon>0$. Let $\mathcal{T}_\epsilon^n(X)$ be the set of ϵ-typical sequences with respect to p_X, and define $\mu_X \triangleq \min_{x\in supp(p_X)} p_X(x)$. Define also $\epsilon_1 \triangleq \frac{1}{2}\epsilon$.

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.

Encoding: Given x^n, find a pair (ω,ν) such that $(x^n,v^n(\omega,\nu))\in\mathcal{T}_\epsilon^n(XV)$. 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 $m\triangleq\omega$.

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 $\tilde{\nu}_{\mathcal{A}}$, choose the smallest; otherwise, set $\tilde{\nu}_{\mathcal{A}}=1$. Define $\widehat{v}_{\mathcal{A}}^n \triangleq v^n(\omega,\nu_{\mathcal{A}})$.

Probability of error: The random variable that represents the randomly generated code is denoted by C_n. One can show that 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 $\delta(n,\epsilon,\mathcal{A}) \triangleq 2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{A}}|\exp(-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}\mu_{VXY_{\mathcal{A}}}) + \exp(-(1-2|\mathcal{V}||\mathcal{X}|e^{-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}\mu_{VX}})2^{\epsilon nH(V)}) + 2^{-n\epsilon H(V)} + 2|\mathcal{X}||\mathcal{Y}_{\mathcal{A}}|e^{-n\epsilon_1^2\mu_{XY_{\mathcal{A}}}}$. The proof is omitted due to space constraints.

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 $\frac{H(M)}{N}\leq\max_{\mathcal{A}\in\mathbb{A}} I(X;V|Y_{\mathcal{A}})+6\epsilon H(V)$. 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 $g:\{0,1\}^N\times\{0,1\}^d\to\{0,1\}^k$ is an extractor [14] and U_d is a sequence of d uniformly distributed random bits such that $d\leq N\delta(N)$ with $\lim_{N\to+\infty}\delta(N)=0$.

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.

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

Analysis of secrecy: We choose the secret length as $k \triangleq \lfloor N[\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}}\delta_\epsilon^2(q,n,\mathcal{U}) - N^{-1/2}]\rfloor$, where $\delta_\epsilon^2(q,n,\mathcal{U}) \triangleq \epsilon I(X;V|Y_{\mathcal{U}}) + (1-\epsilon)[2\epsilon H(X|Y_{\mathcal{U}}V) + 2n^{-1} + \log|\mathcal{X}|(4|S_{XY}|e^{-n\epsilon^2\mu_{XY}} + 2|S_{VXY_{\mathcal{U}}}|e^{-\epsilon^2 n\mu_{VXY_{\mathcal{U}}}/6})] + N^{-1}\delta_\epsilon^1(q,n,\mathcal{U}) + 6\epsilon H(V) + N^{-1/2}$ with $\delta_\epsilon^1(q,n,\mathcal{U}) \triangleq -\log(1-2|S_{V^nY_{\mathcal{U}}^n}|e^{-\epsilon^2 q\mu_{V^nY_{\mathcal{U}}^n}/6})$, $S_{XY} \triangleq supp(p_{XY})$, $S_{VXY_{\mathcal{U}}} \triangleq supp(p_{VXY_{\mathcal{U}}})$, and $S_{V^nY_{\mathcal{U}}^n} \triangleq supp(p_{V^nY_{\mathcal{U}}^n})$. Using [14, Lem. 6, Lem. 9, Lem. 10], [15, Lem. 1.1, Th. 3.2], one can show (we skip the details due to space constraint)

$$\max_{\mathcal{U}\in\mathbb{U}} I(S;U_dY_{\mathcal{U}}^N M)\leq\delta_\epsilon^3(N), \tag{12}$$

where $\delta_\epsilon^3(N) \triangleq \delta^\star(N) + \left(\max_{\mathcal{U}\in\mathbb{U}}\delta_\epsilon^0(n,\mathcal{U}) + 2^{-\sqrt{N}}\right)k$ with $\delta^\star(N) \triangleq 2^{-\sqrt{N}/\log N}\left(k+\sqrt{N}/\log N\right)$, $\delta_\epsilon^0(n,\mathcal{U}) \triangleq$

$2|S_{Y_{\mathcal{U}}^n}|e^{-\epsilon^2 q\mu_{Y_{\mathcal{U}}^n}/3} + 2|S_{V^n Y_{\mathcal{U}}^n}|e^{-\epsilon^2 q\mu_{V^n Y_{\mathcal{U}}^n}/3}$, where $S_{Y_{\mathcal{U}}^n} \triangleq supp(p_{Y_{\mathcal{U}}^n})$.

Analysis of uniformity: Similar to (12), one can show

$$H(S) \geq \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M) \geq k - \delta_\epsilon^3(N). \tag{13}$$

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

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

Achievable secret rate: The secret rate $R_s \triangleq k/N$ satisfies

$$R_s \geq \min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U}) - N^{-1/2} - N^{-1}. \tag{14}$$

B. Continuous case

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

$$R_p = \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}^*}+1}{\sigma_{X|V}^2 O_{\mathcal{A}^*}+1}, \tag{15}$$

$$R_s = \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}^*}+1}{\sigma_{X|V}^2 O_{\mathcal{A}^*}+1} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}^*}+1}{\sigma_{X|V}^2 O_{\mathcal{U}^*}+1}. \tag{16}$$

We extend Section VI-A to the continuous case by means of quantization. As stated below, one can show that a quantization does not affect the requirement (2).

Lemma 6. *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 $Y_{\mathcal{U}_{\Delta^n}}^n$ of $Y_{\mathcal{U}}^n$, $\mathcal{U}\in\mathbb{U}$, is fine enough, then for any $\delta>0$*

$$\max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U}}^n) \leq \max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U}_{\Delta^n}}^n) + \delta. \tag{17}$$

As in [15, Lemma 1.2], we jointly quantize $X, Y_{\mathcal{A}}, Y_{\mathcal{U}}$, and V to form $X_{\Delta_X}, Y_{\Delta_{Y_{\mathcal{A}}}}, Y_{\Delta_{Y_{\mathcal{U}}}}$, and V_{Δ_V} such that $\Delta_X = \Delta_{Y_{\mathcal{A}}} = \Delta_{Y_{\mathcal{U}}} = \Delta_V = l^{-a}$ and $|\mathcal{X}_{\Delta_X}| = |\mathcal{Y}_{\Delta_{Y_{\mathcal{A}}}}| = |\mathcal{Y}_{\Delta_{Y_{\mathcal{U}}}}| = |\mathcal{V}_{\Delta_V}| = l^a$ with $a>0$. Next, we apply the proof for the discrete case to the random variables $X_{\Delta_X}, Y_{\Delta_{Y_{\mathcal{A}}}}, Y_{\Delta_{Y_{\mathcal{U}}}}$, and V_{Δ_V}. Then, we fix l large enough such that, for any $\mathcal{A}\in\mathbb{A}$, $|I(V_{\Delta_V};Y_{\Delta_{Y_{\mathcal{A}}}}) - I(V;Y_{\mathcal{A}})| < \delta/2$, for any $\mathcal{U}\in\mathbb{U}$, $|I(V_{\Delta_V};Y_{\Delta_{Y_{\mathcal{U}}}}) - I(V;Y_{\mathcal{U}})| < \delta/2$, such that (14) becomes

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

Note that $\delta_\epsilon^2(q,n,\mathcal{U})$, $\mathcal{U}\in\mathbb{U}$, in the above equation hides the terms $2\epsilon(1-\epsilon)H(X_{\Delta_X}|Y_{\Delta_{Y_{\mathcal{U}}}}V_{\Delta_V})$ and $6\epsilon H(V_{\Delta_V})$, 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

$$\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}), \tag{18}$$

$\delta_\epsilon^3(N)$ vanishes to zero in (12), (13), and the asymptotic public communication rate is as close as desired to

$$\max_{\mathcal{A}\in\mathbb{A}} I(V;X|Y_{\mathcal{A}}). \tag{19}$$

By taking the auxiliary random variable V jointly Gaussian with X in (18) and (19), one can obtain (15) and (16). We skipped the details because of space constraints.

VII. Concluding Remarks

We proposed a secret sharing scheme 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 perfectly 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 depends linearly on the number of participants and the size of the secret for any access structure. This also contrasts with traditional secret sharing schemes where the size of the shares can grow exponentially with the number of participants for general access structures. We also characterized the secret capacity for threshold access structures and showed that the secret capacity is not a monotone function of the threshold.

References

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

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. National Computer Conf.*, 1979, pp. 313–317.

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

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

[5] Y. Liang, G. Kramer, H. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Networking*, no. 142374, 2009.

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

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

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

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

[10] C. Ye *et al.*, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 240–254, 2010.

[11] A. Pierrot, R. Chou, and M. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *IEEE SPAWC*, 2013, pp. 669–673.

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

[13] A. Beimel, "Secret-sharing schemes: A survey," in *Int. Conf. Coding and Cryptology*, 2011, pp. 11–46.

[14] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Springer-Verlag*, pp. 351–368, 2000.

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