Distributed Secret Sharing Over a Public Channel From Correlated Random Variables

Rémi A. Chou

Abstract—We consider a secret-sharing model where a dealer distributes the shares of a secret among a set of participants with the constraint that only predetermined subsets of participants must be able to reconstruct the secret by pooling their shares. Our study generalizes Shamir’s secret-sharing model in three directions. First, we allow a joint design of the protocols for the creation of the shares and the distribution of the shares, instead of constraining the model to independent designs. Second, instead of assuming that the participants and the dealer have access to information-theoretically secure channels at no cost, we assume that they have access to a public channel and correlated randomness. Third, motivated by a wireless network setting where the correlated randomness is obtained from channel gain measurements, we explore a distributed setting where the dealer is an entity made of multiple sub-dealers. Our main results are inner and outer regions for the achievable secret rates that the dealer and the participants can obtain in this model. To this end, we develop two new achievability techniques, a first one to successively handle reliability and security constraints in a distributed setting, and a second one to reduce a multi-dealer setting to multiple single-user dealer settings. Our results yield the capacity region for threshold access structures when the correlated randomness corresponds to pairwise secret keys shared between each sub-dealer and each participant, and the capacity for the all-or-nothing access structure in the presence of a single dealer and arbitrarily correlated randomness.

Index Terms—Secret sharing, distributed secret-key generation, multiterminal source, privacy amplification.

I. INTRODUCTION

Consider a dealer who distributes to $L$ participants the shares of a secret $S$ with the requirements that any $t$ participants are able to reconstruct $S$ by pooling their shares, and any subsets of participants with cardinality strictly smaller than $t$ must be unable to learn anything about the secret, in an information-theoretic sense. More specifically, the dealer forms $L$ shares $(M_1, \ldots, M_L)$ from the secret $S$, and transmits each share $S_l$ to Participant $l \in \{1, \ldots, L\}$ via an individual and information-theoretically secure channel. The setting is depicted in Figure 1 for the case $(L, t) = (3, 2)$.

This secret-sharing problem was first introduced by Shamir in [2] and, independently, by Blakley in [3]. Subsequently, numerous variants have been extensively studied in the computer science literature, see, for instance, [4], [5] and references therein. In these studies of information-theoretically secure secret sharing, it is assumed that the dealer can distribute to the participants the shares of the secret through information-theoretically secure channels that are available at no cost, as in the setting depicted in Figure 1a. Recently, to avoid this assumption, an information-theoretic treatment of secret sharing over noisy channels has been proposed in [6] by leveraging information-theoretic security results at the physical layer. Specifically, in [6], the information-theoretically secure channels of traditional secret-sharing models are replaced by a noisy broadcast channel from the dealer to the participants so that secret sharing reduces to physical-layer security for a compound wiretap channel [7].

In this paper, as illustrated in Figure 2, we formulate a secret-sharing model that generalizes Shamir’s secret-sharing model in three directions. First, our model allows a joint design of the creation of the shares by the dealer and the distribution of the shares by the dealer to the participants. This contrasts with Shamir’s model which considers these two phases independently, since information-theoretically secure channels are available between the dealer and each participant for the distribution phase. Second, while Shamir’s model assumes that the participants and the dealer have access to information-theoretically secure channels for the distribution of shares, we, instead, only rely on a public channel and corre-
labeled randomness in the form of realizations of independently and identically distributed random variables. Third, motivated by a wireless network setting discussed next, we further explore the problem of secret sharing in a distributed setting where the dealer is an entity made of multiple sub-dealers.

Our setting is formally described in Section III and can be explained at a high level as follows. Assume that the participants and the dealer, made of multiple sub-dealers distributed in space, observe independently and identically distributed realizations of correlated random variables, that have, for instance, been obtained in a wireless communication network from channel gain measurements after appropriate manipulations [8], [9], [10], [11]. The dealer wishes to share a secret with the participants with the requirement that only predefined subsets of participants are able to reconstruct the secret, while any other subsets of participants that pool all their knowledge must remain ignorant, in an information-theoretic sense, of the secret. We are interested in characterizing the set of all achievable secret rates that the dealer can obtain via its sub-dealers when those are allowed to communicate with the participants over a public channel. Note that a potential limitation in the presence of a single dealer is that the correlated random variables available at the dealer and the participants could be such that no positive secret rates are achievable. It is precisely to mitigate this eventuality that we consider a dealer that can deploy in space sub-dealers using, for instance, mobile stations or drones whose positions are steriley spatial configurations.

We summarize the main features of our work as follows:

(i) We study a secret-sharing model that extends Shamir’s secret-sharing model in three directions by considering
- (1) a joint, instead of independent, design of the share creation and distribution phases,
- (2) a public channel and correlated randomness, instead of secure channels, and
- (3) a dealer made of distributed sub-dealers, instead of a single dealer. Specifically, we derive inner and outer regions for the achievable secret rates that the dealer and the participants can obtain in this model. We obtain capacity results in the case of threshold access structures when the correlated randomness corresponds to pairwise secret keys shared between each sub-dealer and each participant, and in the case of a single-dealer setting for the all-or-nothing access structure and arbitrarily correlated randomness.

(ii) In all our achievability results, the length of each share always scales linearly with the size of the secret for any access structures. This comes from the fact that the size of the secret is linear with the number of source observations $n$, and a share corresponds to the public communication plus $n$ source observations, whose lengths are both linear with $n$. Indeed, the public communication corresponds to a compressed version of the $n$ source observations of all the sub-dealers. The length of the public communication does not depend on the number of participants but does depend on the access structure, in particular, the public communication must allow the secret reconstruction for the group of authorized participants that has the least amount of information in their source observations about the secret. This contrasts with Shamir’s secret-sharing model, for which the best known coding schemes require the share size to depend exponentially on the number of participants for some access structures [5].

(iii) As a by-product of independent interest, for distributed settings, we develop two novel achievability techniques to simultaneously satisfy reliability and security constraints. The first one consists in successively handling the reliability and security constraints. This is done by deriving a new variant of the distributed leftover hash lemma and developing a new coding scheme for distributed reconciliation that can be combined with it. The second one consists in reducing a distributed setting to multiple single-user settings.

### A. Related Work

Our work is related to secret-key generation from correlated random variables and public communication [12], [13], as correlated randomness and public communication are also the main resources considered in our setting. However, the analysis of our proposed secret-sharing model does not follow from known results for the secret-key generation models in [12] and [13], as these models only consider a key exchange between two parties, whereas our setting considers a secret exchange between multiple dealers and multiple participants.

The analysis of our proposed secret-sharing model does not follow either from subsequent multiuser secret-key generation models, e.g., [14], [15], [16], and [17], that either do not consider multiple reliability and security constraints simultaneously (and are thus unable to support access structures as in our secret-sharing model) or do not consider distributed settings (and are thus unable to support our distributed dealer setting). The main technical difficulties in our study precisely
come from having to simultaneously deal with (i) a distributed setting due to the presence of multiple sub-dealers, and (ii) information-theoretic security constraints able to support an access structure, i.e., able to ensure that all the unauthorized subsets of participants cannot learn information about the secret. More specifically, for the all-or-nothing access structure, i.e., when all the participants are needed to reconstruct the secret, we develop a new achievability technique that successively handles the reliability and security constraints in the presence of distributed sub-dealers. Perhaps surprisingly, we show that this achievability technique is superior to a random binning strategy that simultaneously handles the reliability and security constraints, in the sense that no elimination of auxiliary rates in the obtained achievability region is necessary. To this end, we derive a new variant of the distributed leftover hash lemma [18], [19], [20]. While the standard leftover hash lemma [21] has been extensively used for secret key generation, e.g., [22], [23], and [24], known proofs techniques to study the distributed leftover hash lemma in our problem do not seem optimal. Specifically, at least two new technical challenges arise in our study: (i) while in a non-distributed setting only one min-entropy appears in the leftover hash lemma, the presence of multiple min-entropies (defined from the marginals of the same joint probability distribution) for a distributed setting complicates the task of finding good approximations of theses min-entropies, further, (ii) usual techniques for non-distributed settings, e.g., [24, Lemma 10]; to study the impact of public communication on the leaked information to an eavesdropper do not lead to tight results in a distributed setting. Additionally, we also develop for the all-or-nothing access structure another new achievability technique to reduce the task of coding for a distributed-dealer setting to the task of coding for multiple separate single-dealer settings.

As alluded to earlier, [6] considers a channel model version of the model studied in this paper but in the presence of a single dealer. Note that subsequently to the preliminary version [1] of this paper, Reference [25] investigated a similar model to the one in this study, but only in the presence of a single-dealer, when the participants and the dealer observe realizations of correlated Gaussian variables. Note also that [26] investigated another secret-sharing problem from correlated random variables and public discussion in the absence of a designated dealer and for special kinds of access structures that are not monotone. By contrast, in this work, we consider arbitrary monotone access structures, as defined in [27].

Finally, note that distributed secret sharing has also been studied from a different perspective in [28] and [29]. In these references, a dealer stores information in multiple storage nodes such that each participant who has access to predefined storage nodes can reconstruct a secret but cannot learn information about the secrets of the other participants. The main difference, in terms of assumptions, between [28] and [29] and our setting is that it is assumed in [28] and [29] that the dealer can store information in multiple nodes and thus that there exist information-theoretically secure channels between the dealer and each node, similar to the standard assumption in Shamir’s secret sharing. By contrast, we do not make this assumption in our setting and instead only rely on a public channel and correlated randomness. For this reason, in [28] and [29] the nature of the problem studied is different, specifically, in [28] and [29], the minimization of communication rates is sought out, whereas in our setting, for given source statistics, the maximization of the secret length is sought out.

B. Paper Organization

The remainder of the paper is organized as follows. We formally define the problem in Section III and state our main results in Section IV. We present our achievability proofs and converse proofs in Sections V and VI, respectively. We prove the optimality of our results in some special cases in Section VII. We propose an extension of all our results to the case of chosen (instead of random) secrets in Section VIII. Finally, we provide concluding remarks in Section IX.

II. Notation

For any $a \in \mathbb{R}^*$, define $[1, a] = [1, \lfloor a \rfloor] \cap \mathbb{N}$. The indicator function is denoted by $1(\omega)$, which is equal to 1 if the predicate $\omega$ is true and 0 otherwise. Let $V(\cdot, \cdot)$ denote the variational distance. For a given set $\mathcal{S}$, let $2^\mathcal{S}$ denote the power set of $\mathcal{S}$, and $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$. Finally, let $\otimes$ denote the Cartesian product.

III. Problem Statement

For $L, D \in \mathbb{N}^*$, define the sets $L \triangleq [1, L]$ and $D \triangleq [1, D]$. Consider $L$ finite alphabets $(X_l)_{l \in L}$, $D$ finite alphabets $(Y_d)_{d \in D}$, and define $X_{\mathcal{L}} \triangleq \bigotimes_{l \in L} X_l$ and $Y_{\mathcal{D}} \triangleq \bigotimes_{d \in D} Y_d$. Then, consider a discrete memoryless source $(X_{\mathcal{L}} \times Y_{\mathcal{D}}, p_{X_{\mathcal{L}} Y_{\mathcal{D}}})$, where $X_{\mathcal{L}} \triangleq (X_l)_{l \in L}$ and $Y_{\mathcal{D}} \triangleq (Y_d)_{d \in D}$, $n \in \mathbb{N}$ independent and identically distributed realizations of the source are denoted by $(X_{\mathcal{L}}^n, Y_{\mathcal{D}}^n)$, where $X_{\mathcal{L}}^n \triangleq (X_l^n)_{l \in L}$ and $Y_{\mathcal{D}}^n \triangleq (Y_d^n)_{d \in D}$. In the following, for any subset $T \subseteq L$, we use the notation $X_{\mathcal{L}}^n_T \triangleq (X_l^n)_{l \in T}$.

As formalized next, we consider $D$ sub-dealers and $L$ participants, who each observes one component of the discrete memoryless source. Through public communication from the sub-dealers to the participants, their objective is to generate $D$ random secrets such that authorized subsets of participants can reconstruct the secrets, whereas unauthorized subsets of participants cannot learn any information about the secrets. We highlight that in the following definitions the secrets are random, however, in Section VIII, we explain how to address the same setting when the values of the secrets are chosen by the sub-dealers.

Definition 1 (Monotone Access Structure [27]): A set $\mathcal{A}$ of subsets of $L$ is a monotone access structure when for any $T \subseteq L$, if $T$ contains a set that belongs to $\mathcal{A}$, then $T$ also belongs to $\mathcal{A}$. We write the complement of $\mathcal{A}$ in $2^L$ as $\overline{\mathcal{A}} \triangleq 2^L \setminus \mathcal{A}$.

Definition 2: For $d \in D$, define the alphabet $S_d \triangleq [1, 2^{n R_d}]$ and $S_{\mathcal{D}} \triangleq \bigotimes_{d \in D} S_d$. A $((2^{n R_d})_{d \in D}, \mathcal{A}, U, n)$ secret-sharing strategy consists of:

- A monotone access structure $\mathcal{A}$.
- $D$ sub-dealers indexed by the set $D$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.


- $L$ participants indexed by the set $\mathcal{L}$.
- $D$ encoding functions $(f_d)_{d \in D}$, where $f_d: \mathcal{Y}_d^n \rightarrow \mathcal{M}_d$, $d \in D$, with $\mathcal{M}_d$ an arbitrary finite alphabet.
- $D$ encoding functions $(g_d)_{d \in D}$, where $g_d: \mathcal{Y}_d^n \rightarrow \mathcal{S}_d$, $d \in D$.
- $|A| \times D$ decoding functions $(h_{A,d})_{A \in A, d \in D}$, where $h_{A,d}: \mathcal{X}_d^n \rightarrow \mathcal{M}_d$, $A \in A$, with $\mathcal{X}_d^n \triangleq \times_{a \in A} \mathcal{X}_a^n$ and $\mathcal{M}_d \triangleq \times_{d \in D} \mathcal{M}_d$, and operates as follows:
  - Sub-dealer $d \in D$ observes $Y_d^n$.
  - Participant $l \in \mathcal{L}$ observes $X_l^n$.
  - Sub-dealer $d \in D$ sends over a noiseless public authenticated channel the public communication $M_d \triangleq f_d(Y_d^n)$ to the participants. We write the global communication of all the sub-dealers as $M_D \triangleq (M_d)_{d \in D}$.
  - Sub-dealer $d \in D$ computes $S_d \triangleq g_d(Y_d^n)$.
  - Any subset of participants $A \in A$ can compute for $d \in D$, $S_d(A) \triangleq h_{A,d}(X_A^n, M_D)$, and thus form $S_D(A) \triangleq (S_d(A))_{d \in D}$, an estimate of $S_D \triangleq (S_d)_{d \in D}$.

Definition 3: A secret rate-tuple $(R_d)_{d \in D}$ is achievable if there exists a sequence of $((2^n R_d))_{d \in D}$, $A, n$) secret-sharing strategies such that

\[
\begin{align*}
\lim_{n \to \infty} \max_{A \in A} \mathbb{P} \left[ S_D(A) \neq S_D \right] &= 0 \text{ (Reliability),} & (1) \\
\lim_{n \to \infty} \max_{U \subseteq \mathcal{U}} \mathbb{I}(S_D; M_D, X_U^n) &= 0 \text{ (Strong Security),} & (2) \\
\lim_{n \to \infty} \log |S_D| - H(S_D) &= 0 \text{ (Secret Uniformity).} & (3)
\end{align*}
\]

Let $C(A)$ denote the set of all achievable secret rate-tuples. When $D = 1$, $C(A)$ denotes the supremum of all achievable secret rates and is called the secret capacity.

(1) means that any subset of participants in $A$ is able to recover the secret, while (2) means that any subset of participants in $U$ cannot learn any information about the secret even if they pool their observations and the public communication sent by all the sub-dealers. (3) means that the secret is nearly uniform, i.e., the entropy of the secret is nearly equal to its length. In other words, (3) means that we seek secret-sharing strategies that maximize the entropy of the secret.

Example 1: Suppose that there are $L = 3$ participants who observe $(X_1^n, X_2^n, X_3^n)$ and $D = 2$ sub-dealers who observe $(Y_1^n, Y_2^n)$ as depicted in Figure 3a. In a first phase, depicted in Figure 3b, sub-dealer $i \in \{1, 2\}$ computes $S_i \triangleq g_i(Y_i^n)$ and $M_i \triangleq f_i(Y_i^n)$, and publicly shares $M_i$ with all the participants. In this example, suppose that $M_1$, $M_2$, $S_1$, and $S_2$ are created such that any two participants must be able to recover $(S_1, S_2)$, i.e., the access structure is defined as $A \triangleq \{\{1\}, \{2\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$, but a single participant must not learn information about $(S_1, S_2)$ as described by Equation (2) with $\mathcal{U} \triangleq 2^\mathcal{L} \setminus \mathcal{A} = \{\{1\}, \{2\}, \{3\}\}$. Hence, in a second phase, depicted in Figure 3b, any two participants $i \in \{1, 2, 3\}$ and $j \in \{1, 2, 3\} \setminus \{i\}$ who pool their information, i.e., $(M_i, M_j, X_i^n, X_j^n)$, can estimate $(S_1, S_2)$ as $(S_i, S_j) \triangleq (h_{A,1}(X_i^n, M_D), h_{A,2}(X_j^n, M_D))$, where $A \triangleq \{i, j\} \in A$ and $M_D \triangleq (M_1, M_2)$.

IV. RESULTS

In the following, for a rate-tuple $(R_d)_{d \in D} \in \mathbb{R}^D_+$ and $S \subseteq D$, we use the notation $R_S \triangleq \sum_{i \in S} R_i$.

A. General Access Structures

1) Results for an Arbitrary Number $D$ of Sub-Dealers: The achievability scheme to derive Theorem 1 relies on random binning designed to simultaneously satisfy the reliability condition (1) and the security condition (2).

Theorem 1 (Inner Bound): We have $R^{(\text{in})}(A) \subseteq C(A)$, where

\[
R^{(\text{in})}(A) \triangleq \text{Proj}_{(R_d)_{d \in D}} \left\{ (R_d, R'_d)_{d \in D} : \right. \\
R'_S \geq \max_{A \in A} H(Y_S | Y_{S\setminus A} X_A), \forall S \subseteq D \\
R'_S - R_S \leq \min_{U \subseteq \mathcal{U}} H(Y_S | X_U), \forall S \subseteq D \left. \right\},
\]

where $\text{Proj}_{(R_d)_{d \in D}}$ denotes the projection on the space defined by the rates $(R_d)_{d \in D}$.

Proof: See Section V-A.

Theorem 2 (Outer Bound): We have $C(A) \subseteq R^{(\text{out})}(A)$, where

\[
R^{(\text{out})}(A) \triangleq \left\{ (R_d)_{d \in D} : R_S \leq \min_{A \in A} \mathbb{I}(Y_S; X_A Y_S | X_U), \forall S \subseteq D \right\}.
\]

Proof: See Section VI-A.

Note that it is challenging to simplify the inner bound $R^{(\text{in})}(A)$ in Theorem 1 because the set functions
S \rightarrow \max_{A \in \mathcal{A}} H(Y_S|Y_S^C,X_A) \text{ and } S \rightarrow \min_{U \in \mathcal{U}} H(Y_S|X_U) \text{ are not necessarily submodular or supermodular and, consequently, Fourier-Motzkin elimination is not easily applicable for a large number of sub-dealers } D. \text{ As described next, one can, however, obtain simplified bounds when } D = 1 \text{ and } D = 2, \text{ and a capacity result for threshold access structures when the source of randomness corresponds to pairwise secret keys.}

2) Results for a Two-Sub-Dealer Setting, i.e., \( D = 2 \):

Corollary 1 (Inner Bound): Assume that \( D = 2 \). We have \( \mathcal{R}^{(\text{in})}(\mathcal{A}) \subseteq \mathcal{C}(\mathcal{A}) \), where \( \mathcal{R}^{(\text{in})}(\mathcal{A}) \) is defined in (4), shown at the bottom of the page.

Corollary 2 (Outer Bound): Assume that \( D = 2 \). We have \( \mathcal{R}^{(\text{out})}(\mathcal{A}) \supseteq \mathcal{C}(\mathcal{A}) \), where

\[
\mathcal{R}^{(\text{out})}(\mathcal{A}) \triangleq \left\{ (R_1, R_2) : \begin{align*}
R_1 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_1; X_A Y_2 | X_U) \right) \\
R_2 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_2; X_A Y_1 | X_U) \right) \\
R_1 + R_2 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_D; X_A | X_U) \right)
\end{align*} \right\}
\]

Corollary 1 is obtained from Theorem 1 by using Fourier-Motzkin elimination. Corollary 2 is a consequence of Theorem 2.

3) Results for a Single-Dealer Setting, i.e., \( D = 1 \):

Corollary 3: Assume that \( D = 1 \). We have the following lower and upper bounds for the secret capacity \( \mathcal{C}(\mathcal{A}) \)

\[
\min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_1; X_A) - I(Y_1; X_U) \right) \leq \mathcal{C}(\mathcal{A}) \leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_1; X_A | X_U) \right).
\]

Corollary 3 is a consequence of Theorem 1 and Theorem 2.

B. All-or-Nothing Access Structure

In this section, we consider the all-or-nothing access structure denoted by \( \mathcal{A}^* \triangleq \{ \mathcal{L} \} \). This setting corresponds to the case where all the participants are needed to reconstruct the secret.

1) Results for an Arbitrary Number \( D \) of Sub-Dealers:

The achievability proof technique for Theorem 3 is different than the proof technique for a general access structure in Theorem 1. Specifically, we successively, instead of simultaneously, handle the reliability constraint (1) and the security constraint (2). This strategy is, for instance, used for secret-key generation \cite{22,23,24}. However, in our distributed setting, the application of this strategy is not straightforward and we discuss in the proof the main technical challenges that needs to be overcome to obtain this extension. The first step of our coding strategy, to handle the reliability constraint, involves a careful design of an exponential number (with respect to \( D \)) of nested binnings. The second step of our coding strategy, to handle the security constraints, involves a new variant of the distributed leftover hash lemma (Lemma 3 in Appendix V-B.2). Note that the proof technique used to prove Theorem 3 has at least two advantages compared to a joint random binning approach as in Theorem 1. First, no auxiliary rate appears in the achievable region of Theorem 3, second, it provides insight for the design of explicit secret-sharing schemes by showing that a two-layer design approach that separates the reliability constraint from the security constraints can be used.

Theorem 3 (Inner Bound): We have \( \mathcal{R}^{(\text{in})}_1 \subseteq \mathcal{C}(\mathcal{A}^*) \), with

\[
\mathcal{R}^{(\text{in})}_1 \triangleq \left\{ (R_d)_{d \in \mathcal{D}} : R_S \leq \min_{T \subseteq \mathcal{L}} \min_{I \subseteq \mathcal{D}} \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_S; X_L | X_T), \forall S \subseteq \mathcal{D} \right) \right\}.
\]

Proof: See Section V-B.

Theorem 4 (Outer Bound): We have \( \mathcal{R}^{(\text{out})}(\mathcal{A}^*) \supseteq \mathcal{C}(\mathcal{A}^*) \), where

\[
\mathcal{R}^{(\text{out})}(\mathcal{A}^*) \triangleq \left\{ (R_d)_{d \in \mathcal{D}} : R_S \leq \min_{T \subseteq \mathcal{L}} \min_{I \subseteq \mathcal{D}} \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_S; X_L Y_S' | X_T), \forall S \subseteq \mathcal{D} \right) \right\}.
\]

Proof: See Section VI-B.

2) Results for a Two-Sub-Dealer Setting, i.e., \( D = 2 \):

The achievable proof strategy of Theorem 5 is different than the achievability proof strategy of Theorem 3. Note that in the proof of Theorem 3, we deal with the security constraint (2) by jointly considering all the sub-dealers. By contrast, our achievability proof strategy in Theorem 5 considers the sub-dealers individually when ensuring (2). Specifically, when \( D = 2 \), one can first realize a secret-sharing scheme between Sub-dealer 1 and the participants with the requirement \( \lim_{n \rightarrow \infty} \max_{U \in \mathcal{U}} \min_{I \in \mathcal{D}} I(S_1; M_1, X_U^n) = 0 \), and then realize a secret-sharing scheme between Sub-dealer 2 and the participants with the requirement \( \lim_{n \rightarrow \infty} \max_{U \in \mathcal{U}} \min_{I \in \mathcal{D}} I(S_2; M_2, X_U^n, Y^n) = 0 \), as illustrated in Figure 4. As described next, one can show that such an approach is sufficient to ensure the security constraint (2). However, the proof is not trivial as we need to modify the reconciliation protocol of Theorem 3 described in Section V-B, and as an initialization phase is also required, during which Sub-dealer 2 shares a secret with negligible rate with all the participants. Note also that one could exchange the role of the two sub-dealers in the protocol to potentially enlarge the achievable region via this method. This idea leads to Theorem 5.

\[
\mathcal{R}^{(\text{in})}(\mathcal{A}) \triangleq \left\{ (R_1, R_2) : \begin{align*}
R_1 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_1; X_A Y_2 | X_U) \right) \\
R_2 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_2; X_A Y_1 | X_U) \right) \\
R_1 + R_2 &\leq \min_{A \in \mathcal{A}, U \in \mathcal{U}} \min \left( \min_{A \in \mathcal{A}, U \in \mathcal{U}} I(Y_D; X_A | X_U) \right)
\end{align*} \right\}
\]
Theorem 5 (Inner Bound): Assume that $D = 2$. If
\[ \min_{d \in \{1, 2\}} \min_{T \subseteq \mathcal{L}} I(Y_d; X_C|X_T) > 0, \] then $R_1^{(n)} = R_2^{(n)} \subseteq C(A^*)$, with
\[
R_2^{(n)} \triangleq [R(\{1\}) \times R(\{2\})|\{1\}]) \cup [R(\{1\})|\{2\}] \cup R(\{1, 2\}),
\]
where we have defined for any $S, V \subseteq D$,
\[
\mathcal{R}(S|V) \triangleq \left\{ R_d \in S : R_B \leq \min_{T \subseteq \mathcal{L}} I(Y_B; X_C|Y_VX_T), \forall B \subseteq S \right\},
\]
and $\mathcal{R}(S) \triangleq \mathcal{R}(S|\emptyset)$.

Proof: See Section V-C.

From Theorem 5, we deduce the following sum-rate achievability result.

Corollary 4 (Sum-Rate Achievability): Assume that $D = 2$ and
\[ \min_{d \in \{1, 2\}} \min_{T \subseteq \mathcal{L}} I(Y_d; X_C|X_T) > 0. \] Define for any $S, V \subseteq D$,
\[
R(S|V) \triangleq \min_{T \subseteq \mathcal{L}} I(Y_S; X_C|Y_VX_T).
\]
For convenience, we also define for $S \subseteq D$, $R(S) \triangleq R(S|\emptyset)$.

Theorem 3 shows the achievability of the secret sum-rate $R_1^{\text{sum}}$, while Theorem 5 shows the achievability of the secret sum-rate $\max(R_1^{\text{sum}}, R_2^{\text{sum}}, R_3^{\text{sum}})$, where
\[
R_1^{\text{sum}} \triangleq \min \{ R(\{1, 2\}) ; R(\{1\}) + R(\{2\}) \}, \quad \quad R_2^{\text{sum}} \triangleq \min \{ R(\{1\}) + R(\{2\})|\{1\} \}, \quad \quad R_3^{\text{sum}} \triangleq R(\{2\}) + R(\{1\})|\{2\}).
\]

From Theorem 4, we will also have the following outer bound.

Corollary 5 (Outer Bound): Assume that $D = 2$. We have
\[
\mathcal{R}(\text{out})(A^*) \supseteq C(A^*), \quad \text{where}
\]
\[
\mathcal{R}(\text{out})(A^*) \triangleq \left\{ R_1 \leq \min_{T \subseteq \mathcal{L}} I(Y_1; X_C|X_T), \quad R_2 \leq \min_{T \subseteq \mathcal{L}} I(Y_2; X_C|X_T) \right\}.
\]

Next, we provide a sufficient condition for having found the optimal secret sum-rate in Corollary 4.

Corollary 6: We use the same notation as in Corollary 5. If $R(\{1, 2\}) \leq R(\{1\}) + R(\{2\})$, then the secret sum-rate $R_1^{\text{sum}}$ in Corollary 4 is optimal by Corollary 5.

3) Result for a Single-Dealer Setting, i.e., $D = 1$: In the presence of a single dealer, i.e., when $D = 1$, we have the following capacity result.

Theorem 6: Assume that $D = 1$. The secret capacity $C(A^*)$ is given by
\[
C(A^*) = \min_{T \subseteq \mathcal{L}} I(Y_D; X_C|X_T).
\]

Proof: See Section VII-A.

Theorem 6 can be seen as a counterpart to the result for a channel model in [6].

Example 2: Suppose that $D = 1$ and $L = 2$. Then, by Theorem 6, we have
\[
C(A^*) = \min [ I(Y_D; X_1|X_2), I(Y_D; X_2|X_1) ].
\]

Example 3: Suppose that $D = 1$ and consider $L$ identical and independent channels $C_l = (\mathcal{X}, p_X|\mathcal{Y}, \mathcal{X})$ with $\mathcal{X}$ and $\mathcal{Y}$ two finite alphabets. Suppose that, for any $l \in \mathcal{L}$, $X_l = \mathcal{X}$, and $X_1$ is the output of the channel $C_1$ when $Y_D$, distributed according to $p_Y$, is the input. Then, by Theorem 6, we have
\[
C(A^*) = I(Y_D; X_1|X_{[2:L]}).
\]

C. Threshold Access Structures When the Source of Randomness Corresponds to Pairwise Secret Keys

We define threshold access structures as follows. Let $t \in \{1, 2, \ldots, L\}$ and $z \in \{1, t - 1\}$. Define the access structure
\[
A_{t,z} \triangleq \{ S \subseteq \mathcal{L} : |S| \geq t \},
\]
and consider Definition 3 with the substitution $A \leftarrow A_\ell$ and $U \leftarrow U_\ell$. We denote the capacity region by $C(A_\ell, U_\ell)$ instead of $C(A)$, and the secret capacity by $C(t, z)$ instead of $C(A)$ when $D = 1$. This setting means that any set of participants of size larger than or equal to $t$ must be able to recover the secrets, and any set of participants of size smaller than or equal to $z$ must be unable to learn any information about the secrets.

Clearly, for arbitrarily correlated source randomness, the results of Section IV-A apply for any $t \in [1, L]$ and $z \in [1, t−1]$, and the results of Section IV-B apply for $(t, z) = (L, L−1)$. We then have the following capacity result when the source of randomness corresponds to pairwise secret keys.

**Theorem 7 (Capacity Region):** Suppose that Participant $l \in L$ and Sub-dealer $d \in D$ share a secret key $K_{l,d}^n$ uniformly distributed over $\{0,1\}^n$, and that all the keys are jointly independent. With the notation of Section III, we thus have $X_l^n = (K_{l,d}^n)_{d \in D}$ for User $l \in L$ and $Y_d^n = (K_{l,d}^n)_{l \in L}$ for Sub-dealer $d \in D$. Let $t \in [1, L]$ and $z \in [1, t−1]$. Then, we have

$$C(A_\ell, U_\ell) = \{(R_d)_{d \in D} : R_S \leq |S|(t−z), \forall S \subseteq D\}$$

$$= \{(R_d)_{d \in D} : R_d \leq t−z, \forall d \in D\},$$

moreover, the rate-tuple $(R_d)_{d \in D}$ is achievable with $R_d^n \triangleq t−z$.

**Proof:** See Section VII-B.

Note that Theorem 7 is consistent with known results for Shamir’s secret sharing model. Indeed, suppose that $D = 1$ and $z = t−1$ in Theorem 7. Using Shamir’s secret sharing, the dealer can first form $L$ shares of $n$ bits for a secret $S$ with entropy $H(S) = n$, and then secretly transmit each share to a participants via a one-time pad over the public channel by using the secret keys of length $n$. The dealer has thus shared a secret with rate $\frac{n}{n} = 1$. Now, since $C(t, z) = t−z = 1$ by Theorem 7, we also conclude in this example that there is no loss of optimality in independently handling the share generation phase and the secure share distribution phase.

**Example 4:** Suppose that $D = 1$ and $L = 10$. Then, $C(t, z) = t−z$ is depicted in Figure 5.

---

**Fig. 5.** Secret capacity for threshold access structures when $D = 1$ and $L = 10$.

---

**V. ACHIEVABILITY PROOFS**

Sections V-A, V-B, V-C contain the achievability proofs of Theorems 1, 3, and 5, respectively. In the following, we will use the following notation. For a pair of discrete random variables $(X, Y)$ distributed according to $p_{XY}$ over a finite alphabet $\mathcal{X} \times \mathcal{Y}$, let $T^n_{\alpha}(X) \triangleq \{x^n \in \mathcal{X}^n : \sum_{x \in \mathcal{X}} p_X(x) \leq \alpha p_{XY}(x), \forall x \in \mathcal{X}\}$ denote the $\epsilon$-letter-typical set associated with $p_X$ for sequences of length $n$, e.g., [30], and define $\mu_X \triangleq \min_{x \in \mathcal{X}} x p_X(x) > 0 p_X(X)$. Let also $T^n_{\alpha}(XY|x^n) \triangleq \{y^n \in \mathcal{Y}^n : (x^n, y^n) \in T^n_{\alpha}(XY)\}$ be the conditional $\epsilon$-letter-typical set associated with $p_{XY}$ with respect to $x^n \in \mathcal{X}^n$.

**A. Proof of Theorem 1**

Theorem 1 relies on random binning. The coding scheme and its analysis are described in Sections V-A.1 and V-A.2, respectively.

1) **Coding Scheme: Binnings:** Fix $i \in D$. Define the functions $g_i : \mathcal{Y}^n \rightarrow [1, 2^n R_i]$ and $h_i : \mathcal{Y}^n \rightarrow [1, 2^n R_i]$, where, for $y^n \in \mathcal{Y}^n$, $g_i(y^n)$ is drawn uniformly at random in the set $[1, 2^n R_i]$, and $h_i(y^n)$ is drawn uniformly at random in the set $[1, 2^n R_i]$.

Then, the encoding at the sub-dealers and the decoding at the participants is as follows:

**Encoding at Sub-dealer $i \in D$:** Given $y^n_i$, Sub-dealer $i \in D$ computes $m_i \triangleq g_i(y^n_i)$ and $s_i \triangleq h_i(y^n_i)$.

**Decoding for a set of participants $A \in \mathcal{A}$:** Given $m_D \triangleq (m_d)_{d \in D}$ and $\pi_A^n$, the set of participants $A$ returns $\hat{y}_D^n(A) = (\hat{y}_i^n)_{i \in A}$ if it is the unique sequence such that $(\hat{y}_D^n(A), \pi_A^n) \in T^n_{\alpha}(Y_D | X_A)$ and $(g_i(\hat{y}_i^n))_{i \in A} = m_D$, otherwise it returns an error.

Next, we determine how to choose $R_i$ and $R_i'$, $i \in D$, to ensure the reliability, security, and uniformity conditions as described in Definition 3.

2) **Coding Scheme Analysis:** Fix $A \in \mathcal{A}$. Define for any $S \subseteq D$, $S \neq \emptyset$,

$$E_0 \triangleq \{(X_A^n, Y_B^n) \notin T^n_{\alpha}(X_A Y_D)\},$$

$$E_S \triangleq \{\forall i \in S, \exists y^n_i \neq Y_i^n, g_i(y_i^n) = g_i(Y_i^n) \}$$

and $(X_A^n, Y_B^n, Y_D^n) \in T^n_{\alpha}(X_A Y_D)$,

so that by the union bound,

$$\mathbb{E}[\mathbb{P}(Y_D^n(A) \neq Y_B^n)] \leq \mathbb{P}[E_0] + \sum_{S \subseteq D, S \neq \emptyset} \mathbb{P}[E_S],$$

where the expectation is over the random choice of the binnings.

**Lemma 1:** For any $S \subseteq D$, $S \neq \emptyset$, we have

$$\mathbb{P}[E_S] \leq 2^{(1+\epsilon) \max_{A \in \mathcal{A}} H(Y_S | Y_{D \setminus X_A})} - n R_S',$$

$$\mathbb{P}[E_0] \leq 2 |X| |Y_D| e^{-n \epsilon \mu_X \mu_Y \epsilon \dim D}.$$  

**Proof:** See Appendix A. Hence, by (5), (6), and (7), we have

$$\mathbb{E} \left[ \max_{A \in \mathcal{A}} \mathbb{P}(Y_D^n(A) \neq Y_B^n) \right]$$
\[
\begin{align*}
\leq \mathbb{E} \left[ \sum_{A \in \mathcal{A}} \mathbb{P}[Y_D(A) \neq Y_B] \right] \\
= \sum_{A \in \mathcal{A}} \mathbb{E} \left[ \mathbb{P}[Y_D(A) \neq Y_B] \right] \\
\leq 2|A||X| |Y_D| e^{-n \mu_X \epsilon_Y D} \\
+ |A| \sum_{S \subseteq D, S \neq \emptyset} 2^{n(1-\epsilon) \max_{A \in \mathcal{A}} H(Y_S|Y_S, X_A) - n R_S}. 
\end{align*}
\]

(8)

b) Security and uniformity analysis: Fix \( \mathcal{U} \subseteq \mathbb{U} \). For all \( m_D, s_D, x_D^u \), we have
\[
\begin{align*}
p_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \\
= \sum_{y_D^u \in D} p(y_D^u, x_D^u) \prod_{i \in D} 1\{g_i(y_D^u) = m_i\} 1\{h_i(y_D^u) = s_i\}. 
\end{align*}
\]

Hence, on average over the random choice of the binnings, for all \( m_D, s_D, x_D^u \), we have
\[
\begin{align*}
\mathbb{E} \left[ p_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] = p(x_D^u) 2^{-n(R_D + R'_D)}, 
\end{align*}
\]
which allows us to write
\[
\begin{align*}
\mathbb{E}[\mathbb{V}(p_{M_D, S_D, X_D^u}^{(\text{uniform})), p_{M_D, S_D, X_D^u}^{(\text{uniform}})]] \\
= \sum_{m_D, s_D, x_D^u} \mathbb{E} \left[ p_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
\leq 2 \sum_{k=1}^2 \mathbb{E} \left[ \sum_{m_D, s_D, x_D^u} p^{(k)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
\leq \mathbb{E} \left[ \sum_{m_D, s_D, x_D^u} p^{(1)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
\leq 2 |\mathcal{U}| |X| |Y_D| e^{-n \mu_X \epsilon_Y D}, 
\end{align*}
\]
(9)

where \( p_{M_D, S_D}^{(\text{uniform}} \) is the uniform distribution over the sample space of \( p_{M_D, S_D} \), and \( \forall m_D, s_D, x_D^u, \)
\[
\begin{align*}
p^{(1)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \\
= \sum_{y_D^u \in T^n(y_D X_u|x_D^u)} p(y_D^u, x_D^u) \prod_{i \in D} 1\{g_i(y_D^u) = m_i\} 1\{h_i(y_D^u) = s_i\}, 
\end{align*}
\]
\[
\begin{align*}
p^{(2)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \\
= \sum_{y_D^u \in T^n(y_D X_u|x_D^u)} p(y_D^u, x_D^u) \prod_{i \in D} 1\{g_i(y_D^u) = m_i\} 1\{h_i(y_D^u) = s_i\}.
\end{align*}
\]

Lemma 2: We have
\[
\begin{align*}
\mathbb{E} \left[ \sum_{m_D, s_D, x_D^u} p^{(2)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
= \mathbb{E} \left[ \sum_{m_D, s_D, x_D^u} p^{(1)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
\leq 2 |\mathcal{U}| |X| |Y_D| e^{-n \mu_X \epsilon_Y D}. 
\end{align*}
\]
(10)

and
\[
\begin{align*}
\mathbb{E} \left[ \sum_{m_D, s_D, x_D^u} p^{(1)}_{M_D, S_D, X_D^u}(m_D, s_D, x_D^u) \right] \\
\leq \sum_{S \subseteq D, S \neq \emptyset} 2^{-n(1-\epsilon) \min_{U \subseteq U} H(Y_S|X_U) 2^{\frac{2}{2} (R_S + R'_S)}. 
\end{align*}
\]
(11)

Proof: See Appendix B.

Finally, by (9), (10), and (11), we obtain
\[
\begin{align*}
\mathbb{E} \left[ \sum_{U \subseteq U} \mathbb{V}(p_{M_D, S_D, X_D^u}^{(\text{uniform}}), p_{M_D, S_D, X_D^u}^{(\text{uniform}}) \right] \\
\leq \sum_{U \subseteq U} \mathbb{E} \left[ \sum_{S \subseteq D, S \neq \emptyset} 2^{-n(1-\epsilon) \min_{U \subseteq U} H(Y_S|X_U) 2^{\frac{2}{2} (R_S + R'_S). 
\end{align*}
\]
(12)

3) Rate Choices: By Markov’s inequality, (8), and (12), there exists a random binning choice and a constant \( a > 0 \) such that \( \max_{A \in \mathcal{A}} \mathbb{P}[Y_D \neq Y_B] + \max_{U \subseteq U} \mathbb{V}(p_{M_D, S_D, X_D^u}^{(\text{uniform}}), p_{M_D, S_D, X_D^u}^{(\text{uniform}}) = o(e^{-na}) \) provided that for any \( S \subseteq D \), \( (1 + \epsilon) \max_{A \in \mathcal{A}} H(Y_S|Y_S, X_A) < R_S \) and \( R_S + R'_S < (1 - \epsilon) \min_{U \subseteq U} H(Y_S|X_U) \). Finally, we remark that \( \mathbb{V}(p_{M_D, S_D, X_D^u}^{(\text{uniform}}), p_{M_D, S_D, X_D^u}^{(\text{uniform}}) = o(e^{-na}) \) implies (2) and (3) by [31, Lemma 2.7].

B. Proof of Theorem 3

Our coding scheme operates in two steps to successively deal with reliability and secrecy by means of reconciliation and privacy amplification. The main difficulty compared to the case \( D = 1 \) is the analysis of privacy amplification because of the distributed setting induced by the multiple sub-dealers. Additionally, our analysis of the privacy amplification step requires a modified reconciliation protocol with additional properties compared to the case \( D = 1 \). We describe our coding scheme in Section V-B.1 and provide its analysis in Section V-B.2. We use the same notation as in Appendix V-A.

1) Coding Scheme:

a) Reconciliation: We define the encoding and decoding procedures for reconciliation through \( 2D + 1 \) nested random binnings as follows.

Binnings: Fix \( i \in D \). For \( y_i^n \in Y_i^n \), for \( j \in \llbracket 1, 2D + 1 \rrbracket \), draw uniformly at random an index in the set \( \llbracket 1, 2nR_{i,j} \rrbracket \) and let this index assignment define the function \( b_{i,j} : Y_i^n \rightarrow \llbracket 1, 2nR_{i,j} \rrbracket \). The value of \( R_{i,j} \) will be chosen later. For any subset \( S \subseteq \llbracket 1, 2D + 1 \rrbracket \), we define \( R_{i,S} \triangleq \sum_{j \in S} R_{i,j} \).

Encoding at Sub-dealer \( i \in D \): Given \( y_i^n \), Sub-dealer \( i \in D \) computes \( (m_{i,j})_{j \in \llbracket 1, 2D + 1 \rrbracket} \triangleq (b_{i,j}(y_i^n))_{j \in \llbracket 1, 2D + 1 \rrbracket} \).

Decoding at the participants: For \( i \in D \), given \( m_i \triangleq (m_{i,j})_{j \in \llbracket 1, 2D + 1 \rrbracket}, y_i^{n-1} \triangleq (y_j^n)_{j \in \llbracket 1, i-1 \rrbracket} \), and \( x_i^{n-1} \), output \( \hat{y}_i^n \) if it is the unique sequence such that \( (\hat{y}_i^n, y_i^{n-1}, x_i^{n-1}) \in T^n(Y_i, X^n, \mathcal{L}^n) \) and \( (b_{i,j}(\hat{y}_i^n))_{j \in \llbracket 1, 2D + 1 \rrbracket} = (m_{i,j})_{j \in \llbracket 1, 2D + 1 \rrbracket} \), otherwise output 1.

Design properties of the reconciliation protocol: Fix \( i \in D \). We first introduce additional definitions. Let \( \delta > 0 \). Define for \( S \subseteq D \), \( R_{i,S} \triangleq H(Y_i | Y_i^{i-1}Y_SX_L) - \delta \) if \( H(Y_i | Y_i^{i-1}Y_SX_L) \neq 0 \) and \( R_{i,S} \triangleq 0 \) otherwise. We sort the sequence \( (R_{i,S})_{S \subseteq D} \) in increasing order and denote the
result by \((R_{i,j})_{j\in[1,2^D]}\). For notation convenience, we denote by \(S_j, j \in [1,2^D]\), the subset of \(D\) such that \(R_{i,j} = H(Y_j|Y_{1:i-1}X_L) - \delta\). Observe that \(R_{i,1} = 0\) and \(R_{i,2^0} = H(Y_1|Y_{1:i-1}X_L) - \delta\).

(i) We will design the reconciliation such that, for any \(i \in D\), the participants in \(L\) can form an approximation \(\tilde{Y}_i^n\) of \(Y_i^n\), from \((M_{i,j})_{j\in[1,2^D+1]}\) and \((Y_i^n, X_L^n)\), such that \(P[\tilde{Y}_i^n \neq Y_i^n] \xrightarrow{n \to \infty} 0\).

(ii) For \(j \in [1,2^D]\) such that \(H(Y_j|Y_{1:i-1}X_L) \neq 0\), we will design the reconciliation such that almost independence holds between \(M_{i,1:j} \triangleq (M_{i,k})_{k\in[1,j]}\) and \((Y_{1:i-1}|S_j,X_L^n)\), in the sense that

\[
\frac{p(M_{i,1:j}, Z_{i,j}^n|m_{i,1:j})}{p(M_{i,1:j})} \xrightarrow{n \to \infty} 1,
\]

where \(p(M_{i,1:j})\) is the uniform distribution over the sample space of \(p_{M_{i,1:j}}\).

Note that the second property is crucial in our analysis of privacy amplification, and is not necessary in the case of \(D = 1\).

b) Privacy amplification: We rely on two-universal hash functions as defined next.

Definition 4 ([32]): A family \(\mathcal{F}\) of two-universal hash functions \(\mathcal{F} = \{f: \{0,1\}^n \to \{0,1\}^s\} \) is such that \(\forall r, x', x \in \{0,1\}^n, x \neq x' \implies P[F(x) = F(x')] \leq 2^{-r}, \) where \(F\) is a function uniformly chosen in \(\mathcal{F}\).

Suppose that the reconciliation step in Scheme V-B.1 is independently repeated \(B\) times. Let \(\tilde{Y}_d^B, d \in D\), be the estimate of \(Y_d^B\). For \(d \in D\), let \(F_d: \{0,1\}^{nB} \to \{0,1\}^{sB}\), be uniformly chosen in a family \(\mathcal{F}_d\) of two-universal hash functions. We leave the quantities \((r_d)_{d \in D}\) unspecified in this section, and will specify them in Section V-B.2. The privacy amplification step operates as follows. Sub-dealer \(d \in D\) computes \(S_d \triangleq F_d(\tilde{Y}_d^B)\), while the participants in \(L\) compute for \(d \in D\), \(S_d \triangleq F_d(\tilde{Y}_d^B)\), where \(\tilde{Y}_d^B\) has been obtained in the reconciliation step.

2) Coding Scheme Analysis: We now show that any rate-tuple \((R_{i,j})_{j\in D} \in R^{\text{in}}\), defined in Theorem 3, is achievable.

a) Analysis of reconciliation: We first prove that Property (i) of Section V-B.1.a holds. The probability of error averaged over the random choice of the binnings \((b_{i,j})_{j\in[1,2^D+1]}\) is upper bounded as

\[
E[P[\tilde{Y}_i^n \neq Y_i^n]] \leq P[\mathcal{E}_{i,1}] + P[\mathcal{E}_{i,2}],
\]

where

\[
\mathcal{E}_{i,1} \triangleq \{(Y_i^n,X_L^n) \notin \mathcal{T}_n(Y_{1:i-1}X_L)\},
\]

\[
\mathcal{E}_{i,2} \triangleq \{(y_i^n)_{j\in[1,2^D+1]} \neq (b_{i,j}(y_i^n))_{j\in[1,2^D+1]}\text{, and } (y_i^n,Y_{1:i-1}X_L^n) \in \mathcal{T}_n(Y_{1:i-1}X_L^n)\}.
\]

Similar to the proof of (6) and (7), one can show that

\[
E[P[\tilde{Y}_i^n \neq Y_i^n]] \leq 2|Y_{1:i-1}|X_L|e^{-n\epsilon} \mu_{Y_{1:i-1}}X_L + 2^{-n(R_{i,2^0+1} - H(Y_i|Y_{1:i-1}X_L)(1+\epsilon))}.
\]

We next prove that Property (ii) of Section V-B.1.a holds. Let \(i \in D\) and \(j \in [1,2^D]\) such that \(H(Y_j|Y_{1:i-1}X_L) \neq 0\).

In the following, for notation convenience, we define \(Z_{i,j} \triangleq (Y_{1:i-1}|S_j,X_L)\).

\[
p_{M_{i,1:j}Z_{i,j}^n(m_{i,1:j}, z_{i,j}^n)} = \sum p(y_{i,j}^n, z_{i,j}^n) I\{b_{i,j}(y_{i,j}^n) = m_{i,1:j}\},\forall m_{i,1:j}, \forall z_{i,j},\]

where \(b_{i,j}(y_{i,j}^n) \triangleq (b_{i,k}(y_{i,k}^n))_{k\in[1,j]}\), hence, on average over \((b_{i,k})_{k\in[1,j]}\),

\[
E[p_{M_{i,1:j}Z_{i,j}^n(m_{i,1:j}, z_{i,j}^n)}] = p(z_{i,j}^n)\frac{1}{2^{nR_{i,1:j}}} , \forall m_{i,1:j}, \forall z_{i,j}.
\]

Then, similar to the proof of (10) and (11), one can show that

\[
E[V(p_{M_{i,1:j}Z_{i,j}^n} p_{\text{uniform}}(p_{Z_{i,j}^n}))] \leq 2|Y_i||Z_{i,j}|e^{-n\epsilon} \mu_{Y_{1:i-1}}X_L + 2^{-n(1-H(Y_i|Y_{1:i-1}X_L)-R_{i,1:j})}.
\]

Finally, we choose the rates as follows. Let \(i \in D\). We define for \(j \in [2,2^D]\), \(R_{i,j} \triangleq R_{i,j} - R_{i,j-1}\), and \(R_{i,1} \triangleq R_{i,1}\). We thus have for any \(j \in [1,2^D]\), \(R_{i,[1,j]} = R_{i,j}\).

Then we choose \(\delta \triangleq 3\epsilon H(Y_i|Y_{1:i-1}X_L) + \epsilon\) and \(R_{i,2^0+1} = \delta + H(Y_{1:i-1}X_L)\).

Hence, we have \(R_{i,[1,2^D+1]} = R_{i,2^0+1} + R_{i,2^0} + (1+\epsilon)H(Y_i|Y_{1:i-1}X_L) + \epsilon\) and \((1-3\epsilon)H(Y_{1:i-1}Y_{1:j}X_L) - H(Y_i|Y_{1:i-1}Y_{1:j}X_L)\).

(b) Analysis of privacy amplification: We use the following version of the leftover hash lemma [21], [33] to analyze the privacy amplification step. The lemma is of independent interest as related versions of this lemma [18], [19], [20], [34] had found a wide variety of applications including oblivious transfer [18], [19], [35], commitment [36], secret generation [20], [37], multiple-access channel resolvability [38], and private classical communication over quantum multiple-access channels [34].

Lemma 3 (Distributed Leftover Hash Lemma): Consider a sub-normalized non-negative function \(p_{X_L Z} \in \mathbb{R}^n\) defined over \(X_L \times Z\), where \(X_L \triangleq (X_l)_{l\in L}\) and, \(Z, X_l, l \in L\), are finite alphabets. For \(l \in L\), let \(F_l : \{0,1\}^n \to \{0,1\}^n\), be uniformly chosen in a family \(\mathcal{F}_l\) of two-universal hash functions. Define \(s_L \triangleq \prod_{l\in L} s_l\), where \(s_l \triangleq |F_l|, l \in L\), and for any \(S \subseteq L\), define \(r_S \triangleq \sum_{l\in S} s_l\). Define also \(F_L \triangleq (F_l)_{l\in L}\) and \(F_{L,X} \triangleq (F_l(X_l))_{l\in L}\). Then, for any \(qz\) defined over \(Z\) such that \(\text{supp}(qz) \subseteq \text{supp}(pz)\), we have

\[
\mathbb{V}(p_{F_L(X_L)F_{L,X}Z}p_{UK}p_{UF}p_{Z}) \leq \sqrt{\sum_{S \subseteq L, S \neq \emptyset} 2^{r_S-H(p_{X_L Z}|qz)}},
\]
where \( p_{UX} \) and \( p_{UZ} \) are the uniform distributions over \([1, 2^n] \) and \([1, s_L] \), respectively, and the min-entropies are defined as in [39], i.e., for any \( S \subseteq L, S \neq \emptyset \),

\[
H_\infty(p_{X_S Z}|q_S) \triangleq -\log \max_{x_S, z \in \supp(q_S)} \frac{p_{X_S Z}(x_S, z)}{q_S(z)}.
\]

**Proof:** See Appendix C.

A challenge with using Lemma 3 is the evaluation of the min-entropies in (15). A possible solution is to use the method in [24] to lower bound a min-entropy in terms of a Shannon entropy. However, one drawback of this method is that an extra round of reconciliation is needed, as in [40], which complicates the coding scheme. Another solution could be to rely on the notion of smooth min-entropy, as in [39]. However, this technique is challenging to apply here because one would need to simultaneously smooth all the min-entropies in (15). Instead, we propose to lower bound the min-entropies in (15) by relying on the following lemma.

**Lemma 4:** Let \( \{Y_d\}_{d \in D} \) be \( D \) finite alphabets and define for \( S \subseteq D \), \( Y_S \triangleq \bigtimes_{d \in S} Y_d \). Consider the random variables \( Y^n_D \triangleq (Y^n_d)_{d \in D} \) and \( Z^n \) defined over \( Y^n_D \times Z^n \) with probability distribution \( q_{Y^n_D Z^n} \). For any \( \epsilon > 0 \), there exists a subnormalized non-negative function \( w_{Y^n_D Z^n} \) defined over \( Y^n_D \times Z^n \) such that \( \Vol(q_{Y^n_D Z^n}, w_{Y^n_D Z^n}) \leq \epsilon \) and

\[
\forall S \subseteq D, H_\infty(w_{Y^n_D Z^n}, q^n_S) \geq nH(Y_S|Z) - n\delta_S(n),
\]

where \( \delta_S(n) \triangleq (\log(|Y_S|) + 3)\sqrt{\frac{2}{n}(D + \log(\frac{1}{\epsilon}))} \).

**Proof:** See Appendix D.

We now combine Lemma 3 and Lemma 4 as follows.

**Lemma 5:** For any \( U \in \mathcal{U} \), we have

\[
\forall(p_{F_D Y^n_D} M^n_{D U} | X^n_U), (p_{U} M^n_{U} | X^n_U), (p_{U} P^n_{U} M^n_{U} X^n_U) \quad (a)
\]

\[
\leq 2 \epsilon + \sum_{S \subseteq D} \frac{2^{-nB \Vol(Y^n_S|M_{D_S} X^n_U) + B \delta_S(n, B)}}{ \mathcal{S} \neq \emptyset},
\]

where \( \delta_S(n, B) \triangleq (\log(|Y_S|) + 3)\sqrt{\frac{2}{n}(D + \log(\frac{1}{\epsilon}))} \).

**Proof:** See Appendix E.

Note that in the case \( D = 1 \), a standard technique could be used [24, Lemma 10] to lower-bound the min-entropy appearing in the leftover hash lemma and study the effect of the public communication on the information leaked to unauthorized participants. However, using [24, Lemma 10] in the case \( D > 1 \) to lower-bound the min-entropies in (39) would result in the achievability of

\[
\{(R_d)_{d \in D} : \quad R_S \leq \min_{T \subseteq \mathcal{L}} [I(Y_S; X_L|X_T) - H(Y_S|X_L)]^+, \forall S \subseteq D \}
\]

which is always contained in the region \( \mathcal{R}_1^{(n)} \) of Theorem 3. For this reason, we did not study the effect of the public communication on the information leaked to unauthorized participants in Lemma 5. Instead, we do it by lower-bounding the Shannon entropies that appear in (16) as follows. Note that Property (ii) in the reconciliation protocol described in Section V-B.1.a plays a key role in the proof of Lemma 6.

**Lemma 6:** For any \( S \subseteq D, S \neq \emptyset \), we have

\[
H(Y^n_S|M_{D_S} X^n_U) \geq n[I(Y_S; X_L|X_U) - \delta(\epsilon)] - \delta(n),
\]

where \( \delta(n) \) is such that \( \lim_{n \to \infty} \delta(n) = 0 \) and \( \delta(\epsilon) \) is such that \( \lim_{n \to \infty} \delta(\epsilon) = 0 \).

**Proof:** See Appendix F.

We are now equipped to prove that (2) and (3) hold. For any \( U \in \mathcal{U} \) and \( \xi > 0 \), we have

\[
\forall(p_{F_D Y^n_D} M^n_{D U} | X^n_U), (p_{U} M^n_{U} | X^n_U), (p_{U} P^n_{U} M^n_{U} X^n_U) \quad (a)
\]

\[
\leq 2 \epsilon + \sum_{S \subseteq D} \frac{2^{-nB \Vol(Y^n_S|M_{D_S} X^n_U) + B \delta_S(n, B)}}{ \mathcal{S} \neq \emptyset},
\]

\[
\leq 2 \epsilon + \frac{2^{D/2} 2^{-n\epsilon/2}},
\]

where \( (a) \) holds by Lemmas 5 and 6, in (b) we have chosen \( r_L \) such that for any \( S \subseteq D \),

\[
r_S \leq \min_{U \in \mathcal{U}} nB \Vol(Y_S; X_L|X_U)
\]

\[
- nB \delta(\epsilon) - B \delta(n) - B \delta_S(n, B) - n\xi.
\]

We conclude that (2) and (3) hold by (17) and [31, Lemma 2.7].

**C. Proof of Theorem 5**

By successively, rather than jointly (as in Theorem 3), considering the security constraints for the two sub-dealers, we prove Theorem 5. The coding scheme and its analysis are described in Sections V-C.1 and V-C.2, respectively. Note that \( \mathcal{R}(\{1, 2\}) = \mathcal{R}_1^{(n)} \), where the achievable \( \mathcal{R}_1^{(n)} \) follows from Theorem 3 with \( D = 2 \). Note also that if one can show the achievability of \( \mathcal{R}(\{1\}) \times \mathcal{R}(\{2\}) \), then one has the achievability of \( \mathcal{R}(\{2\}) \times \mathcal{R}(\{1\}) \) by exchanging the roles of the two dealers. Hence, it is sufficient to prove the achievability of \( \mathcal{R}(\{1\}) \times \mathcal{R}(\{2\}) \).

1) **Coding Scheme:** In this section, we use the notation \( \delta(n) \) to denote a generic function of \( n \) that vanishes to 0 as \( n \) goes to infinity. Our achievable scheme operates in two phases as follows.

a) **Initialization phase:** By using \( n_S^2 \) source observations, Sub-dealer 2 shares a secret \( K_2 \) with non-zero rate with the requirement \( \lim_{n \to \infty} \max_{T \subseteq \mathcal{L}} I(K_2; M_{2, \text{init}} X^n_{T_S}) = \delta(n_S^2) \), where \( M_{2, \text{init}} \) corresponds to the public communication sends by Sub-dealer 2. This is possible by Theorem 6 because we assumed that \( \min_{d \in \{1, 2\}} \min_{T \subseteq \mathcal{L}} I(Y_D; X_L|X_T) > 0 \). Define for \( U \subseteq \mathcal{L}, I_2(U) \triangleq (M_{2, \text{init}}, X^n_{T_S})\).

b) **Successive secret distribution phase:** This phase requires \( n_S \) source observations. Sub-dealer 1 performs the coding scheme in the proof of Theorem 3 for the case \( D = 1 \) with the requirement

\[
\lim_{n \to \infty} \max_{T \subseteq \mathcal{L}} I(S_1; M_1, X^n_T) = 0.
\]
Sub-dealer 2 performs the coding scheme in the proof of Theorem 3 assuming that all the participants have access to $Y_t^n$ with the requirement

$$\lim_{n\to\infty} \max_{T \subseteq \mathcal{L}} I(S_2; M_2, X_T^n, Y_t^n) = 0,$$  \hspace{1cm} (19)$$

for the case $D = 1$ with the following modification: Using the same notation as in the proof of Theorem 3, instead of defining $M_2 \triangleq M_{2,1:3}$, define $M_2$ as $M_2 \triangleq (M_2', M_2'')$ with $M_2' \triangleq K_2 + M_{2,3}$ and $M_2'' \triangleq M_{2,1:2}$. By Property (ii) in the reconciliation step of the proof of Theorem 3, we have

$$I(M'_2; Y_t^n X_L^n) = \delta(n).$$  \hspace{1cm} (20)$$

Then, the proof of Theorem 3 is still valid because $K_2$ is known by the participants (by the initialization phase provided that $n'_2$ is such that $|K_2| = |M_{2,3}|$, and the secrecy rates $R_1 = R(\{1\})$ and $R_2 = R(\{2\})$ are achievable for Requirements (18) and (19). Note that $|K_2| = |M_{2,3}|$ is negligible compared to $n$. More specifically, by inspecting the proof of Theorem 3, one can choose $|M_{2,3}|$, on the order of $n^{1/2-\xi}$, $\xi > 0$, similar to [41] and [42]. Hence, it only remains to show that Requirements (18) and (19) imply Requirements (2) and (3).

2) Coding Scheme Analysis: We first prove that (3) holds. We have

$$\begin{align*}
\log(|S_1|) - H(S_1, S_2) &= \log(|S_1|) - H(S_1) + H(S_2) + I(S_2; S_1) \\ &< \log(|S_1|) - H(S_1) - H(S_2) + I(S_2; Y_t^n) \\ &\xrightarrow{n \to \infty} 0,
\end{align*}$$

where the limit holds by almost uniformity of $S_1$ and $S_2$, and by (19).

We now prove that (2) holds. We first ignore the initialization phase and upper bound the quantity $\max_{T \subseteq \mathcal{L}} I(S_1, S_2; M_1, M_2, X_T^n)$.

Lemma 7: For any $T \subseteq \mathcal{L}$, we have

$$I(S_1, S_2; M_1, M_2, X_T^n) \leq \delta(n) + \delta(n'_2).$$  \hspace{1cm} (21)$$

Proof: See Appendix G.

Next, we jointly consider the initialization phase and the successive secret distribution phase.

Lemma 8: We have for any $U, T \subseteq \mathcal{L}$,

$$I(S_1, S_2; I_2(U), M_1, M_2, X_T^n) \leq \delta(n) + \delta(n'_2).$$

Proof: See Appendix H.

VI. CONVERSE PROOFS

A. Proof of Theorem 2

Consider a secret-sharing strategy, as in Definition 2, that satisfies the constraints (1), (2), and (3). For any $T \subseteq \mathcal{D}$, $A \in \mathcal{A}$, $U \in \mathcal{U}$, we have

$$n R_T = \log |S_T|$$

$$\leq H(S_T) + o(n)$$

$$\leq H(S_T | M_D X_U^n) + o(n)$$

$$\leq I(S_T; D^n_A | M_D X_U^n) + o(n)$$

$$\leq I(Y^n_U; X_A^n M_D | M_D X_U^n) + o(n)$$

$$\leq I(Y^n_U; X_A^n T_X^n) + o(n)$$

$$\leq I(Y^n_U; X_A^n T_X^n | X_U^n) + o(n)$$

$$= n I(Y_T^n; X_A X_T^n | X_U^n) + o(n),$$  \hspace{1cm} (22)$$

where (a) holds by (3), (b) holds by (2), (c) holds by Fano’s inequality and (1), (d) holds because $S_D(A)$ is a function of $(X_A^n, M_D)$ and $S_T$ is a function of $Y^n_U$, (e) holds because $M_S$ is a function of $Y^n_S$ for any $S \subseteq D$. Then, since (22) is valid for any $A \in \mathcal{A}$, $U \in \mathcal{U}$, an upper-bound on the sum-rate $R_S = \sum_{d \in S} R_d$, $S \subseteq D$, is

$$\min_{A \in \mathcal{A}} I(Y_S; X_A Y_S | X_U) = \min_{U \in \mathcal{U}} I(Y_S; X_U).$$

B. Proof of Theorem 4

The proof of Theorem 4 follows from the proof of Theorem 2, since for the all-or-nothing access structure we have for any $S \subseteq \mathcal{D}$

$$\min_{A \in \mathcal{A}} I(Y_S; X_A Y_S | X_U) = \min_{U \in \mathcal{U}} I(Y_S; X_U).$$

VII. PROOF OF CAPACITY RESULTS IN SOME SPECIAL CASES

A. Proof of Theorem 6

The result holds by Corollary 3 using the facts that for any $T \subseteq \mathcal{L}$, the Markov chain $Y_D - X_L - X_T$ holds, and that $\mathcal{L}$ is the set of strict subsets of $\mathcal{L}$ for the all-or-nothing access structure.

B. Proof of Theorem 7

In the following, for any $S \subseteq \mathcal{L}$, $\mathcal{T} \subseteq \mathcal{D}$, we use the notation $K_{S,T} \triangleq (K_{L,t})_{d \in S, t \in T}$.

We first prove the achievability part. Let $t \in \llbracket 1, L \rrbracket$ and $S \subseteq \mathcal{D}$. We have

$$\max_{A \in \mathcal{A}_t} H(Y_S | Y_S X_A) \leq \max_{A \in \mathcal{A}_t} H(K_{L,S} | K_{L,S} K_{A,D})$$

$$= \max_{A \in \mathcal{A}_t} H(K_{L,S} | K_{L,S} K_{A,S} K_{A,S'})$$

$$\leq \max_{A \in \mathcal{A}_t} H(K_{L,S} | K_{A,S})$$

$$\leq \max_{A \in \mathcal{A}_t} H(K_{A,S})$$

$$\leq |S| (L - t),$$  \hspace{1cm} (23)$$

where (a) holds by definition of $Y_S^n, Y_S'^n$, and $X_A^n$, (b) holds by independence between $(K_{A,S}, K_{L,S})$ and $(K_{L,S}, K_{A,S})$, (c) holds by independence between $K_{A',S}$ and $K_{A,S}$, (d) holds by independence and uniformity of the keys. Next, let $z \in \llbracket 1, t - 1 \rrbracket$ and $S \subseteq \mathcal{D}$. We have

$$\min_{U \in \mathcal{U}_z} H(Y_S | X_U) \leq \min_{U \in \mathcal{U}_z} H(K_{L,S} | K_{U,D})$$
where (a) holds by definition of $Y_S^t$ and $X_{U,t}^t$, (b) holds by independence between $K_{U,S^c}$ and $(K_{L,S}, K_{U,S})$, (c) holds by independence between $K_{U,S^c}$ and $K_{U,S}$, (d) holds by independence and uniformity of the keys. Next, we have

\[ R_{S}^{(m)}(A_{t}, U_{t}) = \begin{cases} 
\text{(a)} & \text{Proj}_{(R_{d})_{d \in D}} \left\{ (R_{d}, R'_{d})_{d \in D} : 
R'_{S} \geq \max_{A \in A_{t}} H(Y_S|Y_{S}, X_{A_{t}}), \forall S \subseteq D 
\right\} 
\end{cases} 
\]

\[ R'_{S} + R_{S} \leq \min_{u \in U_{t}} H(Y_S|X_{U_{t}}), \forall S \subseteq D \]

\[ \text{(b)} \]

\[ \begin{cases} 
\text{Proj}_{(R_{d})_{d \in D}} \left\{ (R_{d}^{r}, R'_{d}^{r})_{d \in D} : 
R'_{S} \geq |S|(L - t), \forall S \subseteq D 
\right\} 
\end{cases} \]

\[ R'_{S} + R_{S} \leq \min_{u \in U_{t}} H(Y_S|X_{U_{t}}), \forall S \subseteq D \]

where (a) holds by Theorem 1, (b) holds by (23) and (24), (c) holds as follows. First, consider the system

\[ \left( 
R'_{S} \geq |S|(L - t), \forall S \subseteq D 
\right) \]

and that the set remark that $f : 2^D \rightarrow \mathbb{R}, S \mapsto |S| (L - t) - R_{S}$ and $g : 2^D \rightarrow \mathbb{R}$, $f(S) + g(T) \geq g(S \cup T) + g(S \cap T)$ and $f(S) + f(T) \geq f(S \cup T) + f(S \cap T)$. Hence, by Lemma 9 below, we have that the system (25) has a solution if and only if

\[ |S|(L - t) \leq |S|(L - t) - R_{S}, \forall S \subseteq D, \]

which we rewrite as

\[ R_{S} \leq |S|(t - z), \forall S \subseteq D. \]

\[ \text{Lemma 9 (116, Lemma 2)}: \text{Consider two submodular functions } f : 2^D \rightarrow \mathbb{R} \text{ and } g : 2^D \rightarrow \mathbb{R}. \text{ Then, the following system of equations for } (x_{d})_{d \in D} \in \mathbb{R}^D, \]

\[ g(S) \leq \sum_{a \in S} x_{a} \leq f(S), \forall S \subseteq D, \]

has a solution if and only if $-g(S) \leq f(S), \forall S \subseteq D$. We now prove the converse. Let $t \in [1, L]$, $z \in [1, t - 1]$, and $S \subseteq D$. We have

\[ \min_{A \in A_{t}} \min_{u \in U_{t}} I(Y_S; X_{A_{t}} Y_{S}, X_{U_{t}}) \]

\[ \min_{A \in A_{t}} \min_{u \in U_{t}} I(K_{L,S}; K_{A,D} K_{L,S^{c}}|K_{U,D}) \]

\[ \min_{A \in A_{t}} \min_{u \in U_{t}} \left[ I(K_{L,S}; K_{A,D} |K_{U,D}) + I(K_{L,S^{c}}; K_{A,D} |K_{U,D}) \right] \]

\[ \leq \min_{A \in A_{t}} \min_{u \in U_{t}} I(K_{L,S}; K_{A,D} |K_{U,D}) \]

where (a) holds by definition of $Y_S^t$, $Y_{S}^{t}$, and $X_{A_{t}}^{t}$, and $X_{U_{t}}^{t}$, (b) holds by the chain rule, (c) holds by independence between $(K_{L,S}, K_{U,D})$ and $(K_{U,S^c}, K_{U,D})$, (d) and (e) hold by the chain rule, (f) holds by independence between $(K_{L,S}, K_{A,D}, K_{U,D})$ and $(K_{U,S^c}, K_{A,D}, K_{U,D})$, (g) holds because $K_{L,S}$ contains $K_{A,D}$, (h) holds because the minimum is achieved for a choice of $A$ and $U$ which maximizes the cardinality of $A \cup U$, which happens when $u \subseteq A$, $|A|$ is as small as possible, i.e., $|A| = t$, and $u$ is as large as possible, i.e., $|u| = z$. Hence, (26) and Theorem 2 prove the converse of Theorem 7.

VIII. EXTENSION TO CHOSEN SECRETS

Note that, similar to a secret-key generation problem, the secrets in the problem statement in Section III are random. In this section, we prove that if, instead the secrets are chosen by the sub-dealers, then our results remain unchanged. We first formalize the problem statement for chosen secrets in Section VIII-A. Then, in Section VIII-B, we show how the results of Section IV for random secrets extend to the setting of Section VIII-A.

A. Problem Statement

We modify Definitions 2 and 3 of Section III as follows. Additionally, Figure 3a of Section III now becomes Figure 6.

Definition 5: For $d \in D$, define the alphabet $S_d \subseteq \{1, 2^{nR_d}\}$ and $D_d = \bigotimes_{d \in D} D_d$. A $((2^{nR_d})_{d \in D}, A, U, n)$ secret-sharing strategy consists of:

- A monotone access structure $A$.
- $D$ sub-dealers indexed by the set $D$.
- $D$ independent secrets $(S_d)_{d \in D} \subseteq S_d$, where $S_d, d \in D$, is uniformly distributed over $S_d$ and only known at Sub-dealer $d \in D$. Moreover, the secrets are assumed to be independent from the source observations.
- $L$ participants indexed by the set $L$.
- $D$ encoding functions $(f_d)_{d \in D}$, where $f_d : Y_d^t \times S_d \rightarrow M_d$, $d \in D$, with $M_d$ an arbitrary finite alphabet.
Fig. 6. Secret sharing with $D = 2$ sub-dealers, $L = 3$ users. Formation and distribution of shares.

B. Results

Theorem 8: Fix $L, D \in \mathbb{N}^*$. 

- For an arbitrary access structure $\mathcal{A}$, 
  \[ R^{(\text{in})}(\mathcal{A}) \subseteq C^{\text{(chosen)}}(\mathcal{A}) \subseteq R^{(\text{out})}(\mathcal{A}), \]
  where $R^{(\text{in})}(\mathcal{A})$ and $R^{(\text{out})}(\mathcal{A})$ are defined in Theorems 1 and 2.

- For the all-or-nothing access structure $\mathcal{A}^* \triangleq \{L\}$, 
  \[ R_1^{(\text{in})} \subseteq C^{\text{(chosen)}}(\mathcal{A}^*) \subseteq R^{(\text{out})}(\mathcal{A}^*), \]
  where $R_1^{(\text{in})}$ and $R^{(\text{out})}(\mathcal{A}^*)$ are defined in Theorems 3 and 4. And when $D = 2$, if \[ \min_{d \in \{1, 2\}} \min_{T \subseteq L} I(Y_d; X_C|X_T) > 0, \]
  then we also have 
  \[ R_1^{(\text{in})} \subseteq R_2^{(\text{in})} \subseteq C^{\text{(chosen)}}(\mathcal{A}^*) \subseteq R^{(\text{out})}(\mathcal{A}^*), \]
  where $R_2^{(\text{in})}$ is defined in Theorem 5.

Proof: The converse proof is obtained by modifying Equation (22) in Section VI-A as follows. For any $T \subseteq D$, $\mathcal{A} \in \mathcal{A}$, $U \in \mathcal{U}$, we have 

\[ nR_T = \log |S_T| \]

\[ \begin{array}{l}
\quad (a) \quad H(S_T) \\
\quad (b) \quad \leq H(S_T|\tilde{M}_D X^n_T) + o(n) \\
\quad (c) \quad \leq I(S_T;\tilde{S}_D|\tilde{M}_D X^n_T) + o(n) \\
\quad (d) \quad \leq I(S_T;X^n_A\tilde{M}_D|\tilde{M}_D X^n_T) + o(n) \\
\quad \leq I(S_T;X^n_A\tilde{M}_D|\tilde{M}_D X^n_T) + o(n) \\
\quad \leq I(S_T;\tilde{S}_D X^n_T) + o(n) \\
\quad \leq I(S_T;\tilde{S}_D X^n_T) + o(n) \\
\quad \leq I(S_T;\tilde{S}_D X^n_T) + o(n) \\
\quad = nI(Y_T;\tilde{S}_D X^n_T) + o(n).
\end{array} \]

where ($a$) holds by the uniformity of the secrets, ($b$) holds by (28), ($c$) holds by Fano’s inequality and (27), ($d$) holds because $S_D(A)$ is a function of $(X^n_A, \tilde{M}_D)$, ($e$) holds because $M_T$ is a function of $(Y^n_T, S_T)$ for any $T \subseteq D$, ($f$) holds by the chain rule and because $I(S_T;X^n_A\tilde{S}_D T Y^n_T|\tilde{M}_D X^n_T) = 0, (g)$ holds by the chain rule and because $I(Y^n_T;\tilde{S}_D T X^n_T Y^n_T) = 0$.

The achievability proof consists in doing a one-time pad on top of the achievability proofs from Section V. More specifically, suppose that one has generated the secrets $(\tilde{S}_d)d\in\mathcal{D}$ with rate $(R_d)d\in\mathcal{D}$ with the achievability schemes of Section V such that

\[ \begin{array}{l}
\quad \lim_{n \to \infty} \max_{U \in \mathcal{U}} I(\tilde{S}_D;\tilde{M}_D X^n_T) = 0, \\
\quad \lim_{n \to \infty} \max_{U \in \mathcal{U}} \log |S_D| - H(\tilde{S}_D) = 0.
\end{array} \]

Then, sub-dealer $d \in \mathcal{D}$ transmits over the public channel $\tilde{M}_d \triangleq \tilde{S}_d \oplus S_d$ and the security requirement is satisfied because, for any $U \in \mathcal{U}$ and by defining $M_D \triangleq (M_d)d\in\mathcal{D}$, we have

\[ \begin{array}{l}
\quad I(S_D;\tilde{M}_D X^n_T) \\
\quad = I(S_D;\tilde{M}_D) + I(S_D;\tilde{M}_D, X^n_T|\tilde{M}_D) \\
\quad \leq \log |S_D| - H(\tilde{S}_D) + I(S_D;\tilde{S}_D, \tilde{M}_D, X^n_T|\tilde{M}_D) \\
\quad \leq \log |S_D| - H(\tilde{S}_D) + I(S_D, \tilde{S}_D, \tilde{M}_D, X^n_T|\tilde{M}_D) \\
\quad = \log |S_D| - H(\tilde{S}_D) + I(S_D, \tilde{S}_D, \tilde{M}_D, X^n_T) \\
\quad \leq \log |S_D| - H(\tilde{S}_D) + I(S_D, \tilde{S}_D, \tilde{M}_D, X^n_T) \\
\quad \to 0, \quad (a)
\end{array} \]

where ($a$) holds because $H(\tilde{M}_D) \leq \log |S_D|$ and $H(M_D|S_D) = H(\tilde{S}_D|S_D) = H(\tilde{S}_D)$, ($b$) holds because $I(S_D;\tilde{M}_D, X^n_T|\tilde{S}_D) \leq I(S_D;\tilde{M}_D, X^n_T, \tilde{S}_D) = 0$, and the limit holds by (29) and (30).
IX. CONCLUDING REMARKS

We defined a secret-sharing model between multiple participants and a dealer made of multiple sub-dealers, when each party observes the realizations of correlated random variables and each sub-dealer can communicate with the participants over a public channel. Our model extends Shamir’s secret-sharing model in three directions. First, it allows a joint design of the creation of the shares and their distribution to the participants. This contrasts with Shamir’s model which considers the creation of the shares and their distribution independently. Second, unlike Shamir’s model, which assumes that the participants and the dealer have access to information-theoretically secure channels, our model relies on more general resources, namely, a public channel and correlated randomness in the form of realizations of independently and identically distributed random variables. Third, motivated by a wireless network setting, we explored the problem of secret sharing in a distributed setting where the dealer is an entity made of multiple sub-dealers.

We derived inner and outer regions for the achievable secret rates that the dealer can obtain via its sub-dealers. To this end, we developed two new achievability techniques, a first one to successively handle reliability and security constraints in a distributed setting, and a second one to reduce a distributed setting to multiple single-user settings. We obtained capacity results in the case of threshold access structures when the correlated randomness corresponds to pairwise secret keys shared between each sub-dealer and each participant, and in the case of a single-dealer setting for the all-or-nothing access structure and arbitrarily correlated randomness. We highlight that in all our achievability results the length of each share always scales linearly with the size of the secret for any access structures.

Note that constructive and low-complexity coding schemes for secret-sharing source model and channel model have been proposed in the case of a single dealer in [43] and [44], [45], [46], respectively. While the question of providing constructive and low-complexity coding schemes for distributed-dealer settings is not addressed in this paper and represents an open challenge, we expect that our proof technique that separates the reliability and security constraints for the all-or-nothing access structure can lead to such a constructive and low-complexity coding scheme for an arbitrary number of sub-dealers.

APPENDIX A

PROOF OF LEMMA 1

By [47], we have

\[ P[\mathcal{E}_0] \leq 2 |\mathcal{X}_A| |\mathcal{Y}_D| e^{-nc_2 \mu_A \nu D} \leq 2 |\mathcal{X}_C| |\mathcal{Y}_D| e^{-nc_2 \mu_{X_C} \nu D}. \]

Then, for any \( S \subseteq D, S \neq \emptyset \), we have

\[ P[\mathcal{E}_S] = \sum_{x_A, y_D} p(x_A, y_D) P \left[ \forall i \in S, \bar{y}_i^n \neq y_i^n \right], \]

\[ \leq \sum_{x_A, y_D} p(x_A, y_D) \sum_{y_S^n \in T^n(x_A Y_D \mid x_A y_S^n)} P \left[ \forall i \in S, g_i(\tilde{y}_i^n) = g_i(y_i^n) \right], \]

\[ \leq \sum_{x_A, y_D} p(x_A, y_D) \sum_{y_S^n \in T^n(x_A Y_D \mid x_A y_S^n)} \mathbb{P} \left[ \forall i \in S, g_i(\tilde{y}_i^n) = g_i(y_i^n) \right] \]

\[ \leq \sum_{x_A, y_D} p(x_A, y_D) \sum_{y_S^n \in T^n(x_A Y_D \mid x_A y_S^n)} \mathbb{P} \left[ \forall i \in S, g_i(\tilde{y}_i^n) = g_i(y_i^n) \right] \]

where in (a) \( \tilde{y}_i^n \neq y_i^n \) means \( \tilde{y}_i^n \neq y_i^n, \forall i \in S \), (b) holds by independence of the random binning choices across the sub-dealers, (c) holds by [47].

APPENDIX B

PROOF OF LEMMA 2

We first bound the second term in (9) as follows

\[ E \left[ \sum_{m_D, s_D, x_U^n} p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right] - E \left[ p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right] \]

\[ \leq 2 \sum_{m_D, s_D, x_U^n} 2E \left[ p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right] \]

\[ = 2 \sum_{m_D, s_D, x_U^n} \mathbb{P} (y_D^n, x_U^n) e^{-nc_2 \mu_{X_D} \nu D} \]

\[ \leq 2 \mathbb{P} (Y_D^n, X_U^n) e^{-nc_2 \mu_{X_D} \nu D} \]

and upper-bound the variance in (31) as follows

\[ \text{Var} \left( p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right) \]

\[ = E \left[ \left( p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right)^2 \right] - E \left[ \left( p_{M_D, S_D, X_U^n} (m_D, s_D, x_U^n) \right)^2 \right] \]

\[ \leq \sum_{m_D, s_D, x_U^n} \sum_{y_D^n, x_U^n} \mathbb{P} (y_D^n, x_U^n) e^{-nc_2 \mu_{X_D} \nu D} \]

\[ \times \left( \mathbb{P} (y_D^n, x_U^n) e^{-nc_2 \mu_{X_D} \nu D} \right) \]
\[ \begin{align*}
&\quad \times \mathbb{E}\left[ \prod_{i \in D} \mathbf{1}\{g_i(y^n_i) = m_i\} \mathbf{1}\{h_i(y^n_i) = s_i\} \right] \\
&= \sum_{D \subseteq S} \sum_{y^n_D} \sum_{y^n_{\overline{D}}} \mathbf{1}\{y^n_D \in T^n_D(Y_D X_U | x^n_U)\} \\
&\times \mathbf{1}\{y^n_{\overline{D}} \in T^n_{\overline{D}}(Y_D X_U | x^n_U)\} \\
&\times p^2(y^n_{\overline{D}} | x^n_U)p(y^n_{\overline{D}} | x^n_U y^n_D)p(y^n_D | x^n_U y^n_D) \\
&\times 2^{-n(2R_S + 2R_\delta + R_{SC} + R_{SC}')} - (32)
\end{align*} \]

where in (a) the notation \( y^n_\overline{D} \neq y^n_S \) means \( y^n_i \neq y^n_i, \forall i \in S, \)
and (b) holds by [47]. Hence, by (31) and (32), we upper-bound the first term in (9) by

\[ \begin{align*}
&\sum_{m_D, s_D, x^n_U} \sqrt{\text{Var}\left( p_{M_D S D X^n_U (m_D, s_D, x^n_U)}\right)} \\
&\leq \sum_{S \subseteq D} 2^{(n(R_D + R_S))}2^{-n(1-\epsilon)H(Y_S | X_U)} \\
&\quad \times 2^{-n(2R_S + 2R_\delta + R_{SC} + R_{SC}')} - (32)
\end{align*} \]

APPENDIX D
PROOF OF LEMMA 4

For any \( z^n \in Z^n \) such that \( q_{\overline{Z}}(z^n) > 0 \), define
\[ A(z^n) \triangleq \{ y^n_D \in Y^n_D : -\log q_{\overline{Z}}(y^n_S | z^n) \geq H(Y_S | Z^n) - n\delta_S(n) \}, \]
and for \( S \subseteq D, \)
\[ A_S(z^n) \triangleq \{ y^n_S \in Y^n_S : -\log q_{\overline{Z}}(y^n_S | z^n) \geq H(Y_S | Z^n) - n\delta_S(n) \}. \]

Define for \( y^n_D, z^n \in Y^n_D \times Z^n, \)
\[ w_{\overline{Y}_S Z}(y^n_D, z^n) \triangleq \mathbf{1}\{y^n_D \in A(z^n)\} q_{\overline{Y}_S}Z(y^n_D, z^n), \]
for \( S \subseteq D, \)
\[ w_{\overline{Y}_S Z}(y^n_S, z^n) \triangleq \sum_{y^n_D \in Y^n_D} w_{\overline{Y}_S Z}(y^n_D, z^n). \]

We first show that \( \mathbb{V}(p_{\overline{Y}_S Z^n}, w_{\overline{Y}_S Z^n}) \leq \epsilon \). We have
\[ \mathbb{V}(q_{\overline{Y}_S}Z^n, w_{\overline{Y}_S}Z^n) = \sum_{z^n_D} |q_{\overline{Y}_S}Z^n(y^n_D, z^n) - w_{\overline{Y}_S}Z^n(y^n_D, z^n)| = \sum_{z^n_D} q_{\overline{Y}_S}Z^n(y^n_D, z^n) \mathbf{1}\{y^n_D \notin A(z^n)\} \]
\[ = \mathbb{P}[Y^n_D \notin A(Z^n)] = \sum_{S \subseteq D} \mathbb{P}[Y^n_S \notin A_S(Z^n)] \\
\leq \sum_{S \subseteq D} 2^{-D \epsilon} \]
Next, for $S \subseteq D$, we have

$$H_\infty(w_{Y \mid Z}^n | q_{Z^n})$$

$$= - \max_{z^n \in \text{supp}(q_{Z^n})} \max_{y_3^n \in Y^n_3} \log \frac{w_{Y \mid Z}^n(z^n)}{q_{Z^n}(z^n)}$$

$$(a) = - \max_{y_3^n \in Y^n_3} \max_{z^n} \log \frac{\mathbb{1}\{y_3^n \in A(z^n)\} q_{Y \mid Z}^n(y_3^n, z^n)}{q_{Z^n}(z^n)}$$

$$(b) \geq - \max_{y_3^n \in Y^n_3} \max_{z^n} \log \frac{\mathbb{1}\{y_3^n \in A(z^n)\} q_{Y \mid Z}^n(y_3^n, z^n)}{q_{Z^n}(z^n)}$$

$$(c) \geq H(Y_{Z \mid Z}^n) - n\delta_{S}(n),$$

where the first maximum in (a) and (b) is over \text{supp}(q_{Z^n}). (a) holds by (35) and (36), (b) holds because for any $y_3^n \in Y^n_3$, $\mathbb{1}\{y_3^n \in A(z^n)\} \geq \mathbb{1}\{y_3^n \in A(z^n)\}$ and by marginalization over $Y^n_3$, (c) holds by definition of $A_{S}(z^n)$.

**APPENDIX E**

**PROOF OF LEMMA 5**

Let $U \in \mathcal{U}$. By Lemma 4, for any $\epsilon > 0$, there exists a subnormalized non-negative function $w_{Y \mid M}^n B^B X^\nu B$ such that

$$\mathbb{V}(w_{Y \mid M}^n B^B X^\nu B, w_{Y \mid M}^n B^B X^\nu B) \leq \epsilon,$$

$$\forall S \subseteq D, H_\infty(w_{Y \mid M}^n B^B X^\nu B | p_{M} B X^\nu B) \geq BH(Y^n_B \mid M_D X^\nu B) - B\delta_{S}(n, B).$$

(37)
Next, we have
\[
\begin{align*}
&\mathbb{V}(p_{F_D}(Y^n_{D}^{a})F_DMB_X^{a},PU_{P_D}PM_{B}X^{a}U_B) \\
&\leq (a)\mathbb{V}(p_{F_D}(Y^n_{D}^{a})F_DMB_X^{a},U_F(Y^n_{B}^{a})F_DMB_X^{a}) \\
&+\mathbb{V}(U_F(Y^n_{B}^{a})F_DMB_X^{a},U_{P_F}U_{P_D}w_{B}MB_X^{a}) \\
&+\mathbb{V}(p_{U_{P_D}}w_{MB}X^{a}U_B) \\
&\leq (b)\mathbb{V}(p_{Y^n_{B}MB_X^{a}U_B},w_{Y^n_{B}MB_X^{a}U_B}) \\
&+\mathbb{V}(U_F(Y^n_{B}^{a})F_DMB_X^{a},U_{P_F}U_{P_D}w_{B}MB_X^{a}) \\
&+\mathbb{V}(p_{U_{P_D}}w_{MB}X^{a}U_B) \\
&\leq 2\mathbb{V}(p_{Y^n_{B}MB_X^{a}U_B},w_{Y^n_{B}MB_X^{a}U_B}) \\
&+\mathbb{V}(U_F(Y^n_{B}^{a})F_DMB_X^{a},U_{P_F}U_{P_D}w_{B}MB_X^{a}) \\
&+\mathbb{V}(p_{U_{P_D}}w_{MB}X^{a}U_B) \\
&\leq 2\epsilon + \sum_{S \subseteq \mathcal{D}} \frac{\mathbb{I}_{S}^{H}(w_{Y^n_{B}MB_X^{a}U_B}|F_DMB_X^{a})}{\mathbb{I}_{S}^{H}(w_{Y^n_{B}MB_X^{a}U_B})} \\
&\leq 2\epsilon + \sum_{S \subseteq \mathcal{D}} \frac{2^{-n_{B}H(Y^n_{D}^{a}M_{D}X^{a}U_B)+B\delta(n,B)}}{\mathbb{I}_{S}^{H}(w_{Y^n_{B}MB_X^{a}U_B})}
\end{align*}
\]
(39)
where \(a\) holds by the triangle inequality, \(b\) holds by the data processing inequality, \(c\) holds by (37), \(d\) holds by Lemma 3, \(e\) holds by (38).

APPENDIX F
PROOF OF LEMMA 6

Let \(S \subseteq \mathcal{D}\), \(S \neq \emptyset\). We have
\[
\begin{align*}
&H(Y^n_{S}^{a}|M_{D}X^{a}_{U_B}) \\
&= H(Y^n_{S}^{a}M_{D}X^{a}_{U_B}) - H(M_{D}X^{a}_{U_B}) \\
&= H(Y^n_{S}^{a}X^{a}_{U_B}) + H(M_{S}^{a}|Y^n_{S}^{a}X^{a}_{U_B}) - H(M_{D}X^{a}_{U_B}) \\
&\geq H(Y^n_{S}^{a}X^{a}_{U_B}) + H(M_{S}^{a}|Y^n_{S}^{a}X^{a}_{U_B}) - n\sum_{i \in \mathcal{D}} \sum_{j \in [1,2^D+1]} R_{i,j},
\end{align*}
\]
(40)
where we have used in the last inequality that \(H(M_{D}X^{a}_{U_B})\) is upper bounded by the logarithm of the cardinality of the alphabet of \(M_{D}\).

The third term in the right-hand side of (40) is evaluated as follows.
\[
\begin{align*}
&\sum_{i \in \mathcal{D}} \sum_{j \in [1,2^D+1]} R_{i,j} \\
&\leq (a)\sum_{i \in \mathcal{D}} (\bar{R}_{i,2^D} + R_{i,2^D+1}) \\
&\leq (b)\sum_{i \in \mathcal{D}} H(Y_{i}|Y_{1,i-1}X_{L}) + \epsilon H(Y_{i}|Y_{1,i-1}X_{L}) + \epsilon \\
&\leq H(Y_{D}|X_{L}) + \epsilon (H(Y_{D}|X_{L}) + D),
\end{align*}
\]
(41)
where \(a\) and \(b\) holds by the definitions and rates chosen in Section V-B.2.a, \(c\) holds by the chain rule.

Next, the second term in the right-hand side of (40) is lower bounded as follows.
\[
\begin{align*}
&H(M_{S}^{a}|Y^n_{S}^{a}X^{a}_{U_B}) \\
&\geq H(M_{S}^{a}|Y^n_{S}^{a}X^{a}_{U_B}) + n[H(Y_{S}|Y_{S}|X_{L}) - \delta(\epsilon)] - o(1) \\
&- n[H(Y_{D}|X_{L}) + \epsilon (H(Y_{D}|X_{L}) + D)] \\
&= n[H(Y_{S}|X_{U}) - H(Y_{S}|X_{L})] \\
&- n\delta(\epsilon) - o(1) - n\epsilon (H(Y_{D}|X_{L}) + D).
\end{align*}
\]
(42)
where \(a\) and \(b\) holds because conditioning reduces entropy, \(c\) holds because \(M_{1,i-1}\) is a function of \(Y_{1,i-1}^{n}\), \(d\) holds because \(M_{i}\) contains \(M_{i,1,j}\) for any \(j \in [1,2^D]\) by the construction in Section V-B.1.a, \(e\) holds by Property (ii) in Section V-B.1.a and [48, Lemma 1], \(f\) holds by the rates chosen in Section V-B.2.a and Property (ii) in Section V-B.1.a with [31, Lemma 2.7], and in \(g\) we have defined \(\delta(\epsilon) \leq \epsilon (\sum_{i \in \mathcal{S}} (3H(Y_{i}|Y_{1,i-1}X_{L} + 1))\). Hence, combining (40), (41), (42), we obtain
\[
\begin{align*}
&H(Y^n_{S}^{a}|M_{D}X^{a}_{U_B}) \\
&\geq H(Y^n_{S}^{a}|X^{a}_{U_B}) + n[H(Y_{S}|Y_{S}|X_{L}) - \delta(\epsilon)] - o(1) \\
&- n[H(Y_{D}|X_{L}) + \epsilon (H(Y_{D}|X_{L}) + D)] \\
&= n[H(Y_{S}|X_{U}) - H(Y_{S}|X_{L})] \\
&- n\delta(\epsilon) - o(1) - n\epsilon (H(Y_{D}|X_{L}) + D).
\end{align*}
\]

APPENDIX G
PROOF OF LEMMA 7

For any \(T \subseteq \mathcal{L}\), we have
\[
\begin{align*}
&I(S_{1},S_{2};M_{1},M_{2},X^{a}_{T}) \\
&\geq I(S_{1};M_{1},M_{2},X^{a}_{T}) + I(S_{2};M_{1},M_{2},X^{a}_{T}|S_{1}) \\
&\geq (a)I(S_{1};M_{1},X^{a}_{T}) + I(S_{1};M_{2}|M_{1},X^{a}_{T}) \\
&+ I(S_{2};M_{1},M_{2},X^{a}_{T}|S_{1}) \\
&\leq (b)I(S_{1};M_{1},X^{a}_{T}) + I(S_{1};M_{2}|M_{1},X^{a}_{T}) \\
&+ I(S_{2};M_{1},M_{2},X^{a}_{T}|S_{1}) \\
&\leq (c)I(S_{1};M_{1},X^{a}_{T}) + I(S_{1};M_{2}|M_{1},X^{a}_{T}) \\
&+ I(S_{2};M_{1},M_{2},X^{a}_{T}|S_{1}) \\
&\leq (d)\delta(n) + I(S_{1};M_{2}|M_{1},X^{a}_{T}) \\
&\leq (e)\delta(n) + I(S_{1};M_{2}|M_{1},X^{a}_{T}) + I(S_{2};M_{2}|M_{1},X^{a}_{T}) \\
&\leq (f)\delta(n) + I(Y_{1}^{n},X^{a}_{L},M_{2}) + I(S_{2};M_{2}|M_{1},X^{a}_{T})
\end{align*}
\]
\[ (g) \leq \delta(n) + |M'_2| - H(K_2|S_1, M_2, \hat{X}_T^0) \]
\[ (h) = \delta(n) + |M'_2| - H(K_2) \]
\[ (i) = \delta(n) + \delta(n'_2), \]

where \((a)\) and \((b)\) hold by the chain rule, \((c)\) holds because \((M_1, S_1)\) is a function of \(Y^0\), \((d)\) holds by \((18)\) and \((19)\), \((e)\) holds by the chain rule and the definition of \(M_2\), \((f)\) holds because \(I(S_1, M'_2|I_2) \leq I(M_1, X^0_T, S_1; M'_2) \leq I(Y^0_T, X^0_T; M'_2)\), where the first inequality holds by the chain rule and the second inequality holds as in \((c)\), \((g)\) holds by \((20)\) and by the definition of \(M'_2\), \((h)\) holds by independence of the initialization phase and the successive secret distribution phase, \((i)\) holds by almost uniformity of \(K_2\) in the initialization phase.

**APPENDIX H PROOF OF LEMMA 8**

We have for any \(U, T \subset \mathcal{L}\),
\[ I(S_1, S_2; I_2(U), M_1, M_2, X_T^0) - \delta(n) - \delta(n'_2) \]
\[ \leq I(S_1, S_2; I_2(U)|M_1, M_2, X_T^0) \]
\[ \leq I(M_1, M_2, S_2, X_T^0) \]
\[ = I(M_1; I_2(U)|S_1, S_2, X_T^0) + I(M_2; I_2(U)|M_1, S_1, S_2, X_T^0) \]
\[ \leq I(M'_2; I_2(U)|M'_2, M_1, S_1, S_2, X_T^0) \]
\[ \leq |K_2| - H(K_2|I_2(U)) \]
\[ \leq |K_2| - H(K_2) + I(K_2; I_2(U)) \]
\[ \leq \delta(n'_2), \]

where \((a)\) holds by the chain rule and \((43)\), \((b)\) holds because \(I(S_1, S_2; I_2(U)|X_T^0) \leq I(S_1, S_2, X_T^0; I_2(U)) = 0\), where the equality holds by independence of the initialization phase and the successive secret distribution phase, \((c)\) holds by the definition of \(M_2\), the chain rule, and independence of the initialization phase and the successive secret distribution phase, \((d)\) holds by the definition of \(M'_2\), \((e)\) holds by the independence of the initialization phase and the successive secret distribution phase, \((g)\) holds by the initialization phase.

**REFERENCES**

[1] R. A. Chou, “Secret sharing over a public channel from correlated random variables,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2018, pp. 991–995.

[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 Nat. Comput. Conf., vol. 48, 1979, pp. 313–317.

[4] D. Stinson, Cryptography: Theory and Practice. Boca Raton, FL, USA: CRC Press, 2005.

[5] A. Beimel, “Secret-sharing schemes: A survey,” in Proc. Int. Conf. Coding Cryptol., 2011, pp. 11–46.
[32] J. L. Carter and M. N. Wegman, “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[33] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[34] R. A. Chou, “Private classical communication over quantum multiple-access channels,” *IEEE Trans. Inf. Theory*, vol. 68, no. 3, pp. 1782–1794, Mar. 2022.

[35] R. A. Chou, “Pairwise oblivious transfer,” in *Proc. IEEE Inf. Theory Workshop (ITW)*, Apr. 2021, pp. 1–5.

[36] R. Chou and M. R. Bloch, “Commitment over multiple-access channels,” in *Proc. 58th Annu. Allerton Conf. Commun. Control, Comput. (Allerton)*, Sep. 2022, pp. 1–6.

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

[38] R. Sultana and R. A. Chou, “Multiple access channel resolvability codes from source resolvability codes,” *IEEE Trans. Inf. Theory*, vol. 68, no. 6, pp. 3608–3619, Jun. 2022.

[39] H. P. Yuen, “Security of quantum key distribution,” *IEEE Access*, vol. 4, pp. 724–749, 2016.

[40] 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.

[41] R. A. Chou, B. N. Vellambi, M. R. Bloch, and J. Kliewer, “Coding schemes for achieving strong secrecy at negligible cost,” *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1858–1873, Mar. 2017.

[42] R. A. Chou and M. R. Bloch, “Data compression with nearly uniform output,” in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1979–1983.

[43] 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.

[44] R. A. Chou, “Explicit wiretap channel codes via source coding, universal hashing, and distribution approximation, when the channels’ statistics are uncertain,” *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 117–132, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9933484

[45] 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.

[46] R. Sultana, V. Rana, and R. A. Chou, “Secret sharing over a Gaussian broadcast channel: Optimal coding scheme design and deep learning approach at short blocklength,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2023, pp. 1961–1966.

[47] G. Kramer, “Topics in multi-user information theory,” *Found. Trends Commun. Inf. Theory*, vol. 4, nos. 4–5, pp. 265–444, 2008.

[48] I. Csiszár, “Almost independence and secrecy capacity,” *Problemy Peredachi Informatsii*, vol. 32, no. 1, pp. 48–57, 1996.

Rémi A. Chou received the Engineering degree 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 The Pennsylvania State University, University Park, PA, USA. From 2017 to 2023, he was an Assistant Professor with the Electrical Engineering and Computer Science Department, Wichita State University, Wichita, KS, USA. He is currently an Assistant Professor with the Computer Science and Engineering Department, The University of Texas at Arlington, Arlington, TX, USA.