Secret-Key Generation in Many-to-One Networks: An Integrated Game-Theoretic and Information-Theoretic Approach

Rémi A. Chou, *Member, IEEE*, and Aylin Yener, *Fellow, IEEE*

***Abstract*— This paper considers secret-key generation between several agents and a base station that observe independent and identically distributed realizations of correlated random variables. Each agent wishes to generate the longest possible individual key with the base station by means of public communication. All keys must be jointly kept secret from all external entities. In this many-to-one secret-key generation setting, it can be shown that the agents can take advantage of a collective protocol to increase the sum rate of their generated keys. However, when each agent is only interested in maximizing its own secret-key rate, agents may be unwilling to participate in a collective protocol. Furthermore, when such a collective protocol is employed, how to fairly allocate individual key rates arises as a valid issue. This paper studies the tension between cooperation and self-interest with a game-theoretic treatment. This paper establishes that cooperation is in the best interest of all individualistic agents and that there exist individual secret-key rate allocations that incentivize the agents to follow the protocol. In addition, an explicit coding scheme that achieves such allocations is proposed.**

***Index Terms*— Multiterminal secret-key generation, strong secrecy, coalitional game theory, hash functions, polar codes.**

I. Introduction

MULTITERMINAL communication settings subject to limited total resources bring about issues pertaining to competition, and fairness among users. Such issues are typically studied by means of game theory; see, for instance, [2]–[4] which deal with the Gaussian multiple access channel, and [5]–[10] which deal with interference channels.

In this paper, we study a multiterminal secret-key generation problem that involves selfish users, and propose to study the tension between cooperation and selfishness by means of cooperative game theory, more specifically, coalitional game theory. We refer to [11]–[13] for an introduction to coalitional game theory, and to [14] for a review of some of its applications to telecommunications. Our setting can be explained as follows. Each agent wishes to generate an individual key of maximal length with the base station to securely and individually report information, using a one-time pad for instance. There are many such agents and a single base station. The generated keys must be jointly kept secret from all external entities. We consider a source model for secret-key generation [15], [16], i.e., the agents and the base station observe independent and identically distributed (i.i.d.) realizations of correlated random variables (possibly obtained, after appropriate manipulations, from *channel gains measurements* [17]–[20]), and can communicate over an authenticated public noiseless channel. It can be shown that when agents are altruistic, the agents increase the sum of their key lengths by agreeing to participate in a joint protocol, in contrast to operating separately on their own. However, when each agent is interested in maximizing its own key length only, as we consider, there exists a tension between cooperation and the sole interest of a given agent. Moreover, assuming that the agents collaborate to maximize the sum of their key lengths, another issue is to determine a fair allocation of individual key lengths, so that no agent has any incentive to deviate from the protocol. The goal of our study is to study this tension between cooperation and selfishness.

Note that when the agents are assumed to be altruistic, and when fairness issues are ignored, the secret-key generation model we consider reduces to the one studied in [21] and is related to multiple-key generation in a network with trusted helpers [22]–[24]. Note also that once the secret-key generation protocol is done, the subsequent transmission to the base station of messages protected by means of a one-time pad with the generated secret keys can be viewed as a noiseless multiple access wiretap channel [25].

Our contributions are three-fold. (i) We formally introduce an integrated game-theoretic and information-theoretic formulation of the problem in Section II. Specifically, we cast the problem as a coalitional game in which the value function is determined under information-theoretic guarantees, i.e., the value associated with a coalition is computed with no restrictions on the strategies that the users outside the coalition could adopt. We then derive properties of the defined game and propose rate allocations as candidates for fair solutions in Section III. (ii) By adding the constraint that the agents are selfish, we derive a converse using the core of the game we define, which differs from the techniques used for a setting

Manuscript received September 19, 2017; revised August 26, 2018; accepted February 5, 2019. Date of publication February 27, 2019; date of current version July 12, 2019. This work was supported by the National Science Foundation under Grant CNS-1314719. This paper was presented in part at the 2017 IEEE International Symposium on Information Theory in [1].

R. A. Chou is with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260 USA (e-mail: remi.chou@wichita.edu).

A. Yener is with the Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802 USA (e-mail: yener@ee.psu.edu).

Communicated by R. La, Associate Editor for Communication Networks.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2902068

that does not involve selfihness constraints [21], [23]. (iii) We provide in Section IV an explicit coding scheme based on polar codes for source coding [26] and hash functions to implement the solutions proposed in Section III. Note that a few explicit coding schemes have been proposed for multiterminal secret-key generation problems [27]–[29], however, the coding schemes in these references do not seem to easily apply to our setting. Specifically, the distributed nature of our setting is challenging as each agent must locally generate a key without the knowledge of the source observations of the other agents, and all the generated keys must be collectively secure.

The remainder of the paper is organized as follows. We formally state the problem in Section II. We study in Section III the game we have defined in Section II. We propose an explicit coding scheme to achieve any point in the core of our game in Section IV. We study our model in the case of non-degraded sources in Section V. We generalize our model to a setting with multiple clearance levels in Section VI. Finally, we provide concluding remarks in Section VII.

II. Problem Statement

We define an auxiliary secret-key generation model with no selfishness constraints in Section II-A, and provide additional definitions in Section II-B. In Section II-C, we explain our objective using the model of Section II-A to which selfishness constraints are added, and describe the integrated game-theoretic and information-theoretic problem formulation.

Notation: For any $a \in \mathbb{N}^*$, define $[\![1, a\,]\!] \triangleq [1, a] \cap \mathbb{N}$. For a given set $\mathcal{S}$, we let $2^{\mathcal{S}}$ denote the power set of $\mathcal{S}$. For two probability distributions p and q defined over the same alphabet $\mathcal{X}$, we define the variational distance between p and q as $\mathbb{V}(p, q) \triangleq \sum_{x\in\mathcal{X}} |p(x) - q(x)|$. Finally, $\bigtimes$ denotes the Cartesian product.

A. An Auxiliary Secret-Key Generation Model (Without Selfishness Constraints)

Let $L \in \mathbb{N}^*$ and $\mathcal{L} \triangleq [\![1, L]\!]$. In the following, we consider L agents represented by the set $\mathcal{L}$ and one base station.

1) Definition of the Source Model: Define $\mathcal{X}_{\mathcal{L}}$ as the Cartesian product of L finite alphabets $\mathcal{X}_l$, $l \in \mathcal{L}$. Consider a discrete memoryless source (DMS) $\left(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0, p_{X_{\mathcal{L}}X_0}\right)$, where $\mathcal{X}_0$ is a finite alphabet and $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$. For $l \in \mathcal{L}$, Agent l observes the component X_l of the DMS, and the base station observes the component X_0. The source is assumed to follow the following Markov chain: for any $\mathcal{S}, \mathcal{T} \subset \mathcal{L}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$,

$$X_{\mathcal{S}} - X_0 - X_{\mathcal{T}}. \tag{1}$$

Note that such a source model has already been considered in [28]–[30]. Assuming that all the random variables are binary, an instance of this model is $X_l \triangleq X_0 \oplus B_l$, $\forall l \in \mathcal{L}$, where the B_l's are independent Bernoulli random variables and $\oplus$ is the modulo-two addition.

The source's statistics are assumed known to all parties, and communication is allowed over an authenticated noiseless public channel.

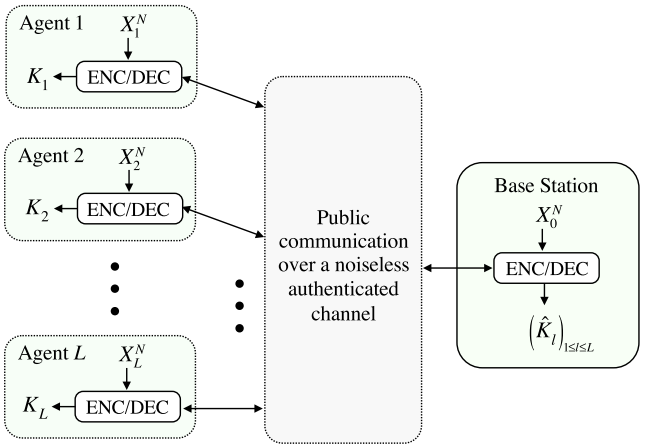

Fig. 1. Many-to-one secret-key generation setting.

2) Description of the Objectives for the Agents: The goal of Agent $l \in \mathcal{L}$ is to generate an individual secret-key with the base station. We formalize the definition of a secret-key generation protocol for this setting, which is depicted in Figure 1.

Definition 1. *For $l \in \mathcal{L}$, let $\mathcal{K}_l$ be a key alphabet of size 2^{NR_l} and define $\mathcal{K}_{\mathcal{L}}$ as the Cartesian product $\bigtimes_{l\in\mathcal{L}}\mathcal{K}_l$. A $((2^{NR_l})_{l\in\mathcal{L}}, N)$ secret-key generation strategy for the agents in $\mathcal{L}$ is as follows.*

1) *The base station observes X_0^N and Agent l, $l \in \mathcal{L}$, observes X_l^N.*
2) *The agents in $\mathcal{L}$ and the base station communicate, possibly interactively, over the public channel. The global public communication between the agents in $\mathcal{L}$ and the base station is denoted by $A \in \mathcal{A}$, for some discrete alphabet $\mathcal{A}$.*
3) *Agent l, $l \in \mathcal{L}$, computes $K_l(X_l^N, A) \in \mathcal{K}_l$.*
4) *The base station computes $\widehat{K}_l(X_0^N, A) \in \mathcal{K}_l$, $l \in \mathcal{L}$.*

In the following, we use the notation $K_{\mathcal{L}} \triangleq (K_l)_{l\in\mathcal{L}}$.

Definition 2. *A secret-key rate tuple $(R_l)_{l\in\mathcal{L}}$ is achievable if there exists a sequence of $((2^{NR_l})_{l\in\mathcal{L}}, N)$ secret-key generation strategies for the agents in $\mathcal{L}$ such that*

$$\lim_{N\to\infty} \mathbb{P}[\widehat{K}_{\mathcal{L}} \neq K_{\mathcal{L}}] = 0 \text{ (Reliability)}, \tag{2}$$

$$\lim_{N\to\infty} I\left(K_{\mathcal{L}}; A\right) = 0 \text{ (Collective Secrecy)}, \tag{3}$$

$$\lim_{N\to\infty} \log|\mathcal{K}_{\mathcal{L}}| - H(K_{\mathcal{L}}) = 0 \text{ (Keys Uniformity)}. \tag{4}$$

The secrecy constraint (3) ensures that the keys generated by the agents in $\mathcal{L}$ are independent from the public communication. Note, however, that (3) does not mean that the key of a particular agent in $\mathcal{L}$ is secret from the other agents. Moreover, (4) ensures that the keys generated are almost jointly independent, so that the simultaneous use of the keys by the agents in $\mathcal{L}$ is secure. Note that this setting has been introduced in [21].

Observe that in the presented setting we implicitly assumed that the agents in $\mathcal{L}$ are willing to agree on a common secret key generation protocol. In Section II-C, we study a similar setting but with the additional constraint that the agents

are selfish. Before we move to this setting we introduce additional definitions in Section II-B.

B. Additional Definitions

We provide additional definitions that will be useful to incorporate selfishness constraints in the model presented in Section II-A. These definitions generalize the setting described in Section II-A when security constraints with respect to a subset of agents hold, i.e., the keys generated by a given subset of agents are required to be secret from the rest of the agents. We formalize the definition of a secret-key generation protocol for a group of agents $\mathcal{S} \subseteq \mathcal{L}$ in the following definitions.

Definition 3. *Let $\mathcal{S} \subseteq \mathcal{L}$. For $i \in \mathcal{S}$, let $\mathcal{K}_i$ be a key alphabet of size 2^{NR_i} and define $\mathcal{K}_{\mathcal{S}} = \bigtimes_{i\in\mathcal{S}}\mathcal{K}_i$. A $((2^{NR_i})_{i\in\mathcal{S}}, N)$ secret-key generation strategy for the coalition of agents $\mathcal{S}$ is as follows.*

1) *The base station observes X_0^N and Agent i, $i \in \mathcal{S}$, observes X_i^N.*
2) *The agents in $\mathcal{S}$ and the base station communicate, possibly interactively, over the public channel. The global public communication between the agents in $\mathcal{S}$ and the base station is denoted by $A_{\mathcal{S}} \in \mathcal{A}_{\mathcal{S}}$, for some discrete alphabet $\mathcal{A}_{\mathcal{S}}$.*
3) *Agent i, $i \in \mathcal{S}$, computes $K_i(X_i^N, A_{\mathcal{S}}) \in \mathcal{K}_i$.*
4) *The base station computes $\widehat{K}_i(X_0^N, A_{\mathcal{S}}) \in \mathcal{K}_i$, $i \in \mathcal{S}$.*

In the following, we use the notation $K_{\mathcal{S}} \triangleq (K_i)_{i\in\mathcal{S}}$.

Definition 4. *Let $\mathcal{S} \subseteq \mathcal{L}$. A secret-key rate tuple $(R_i)_{i\in\mathcal{S}}$ is achievable if there exists a sequence of $((2^{NR_i})_{i\in\mathcal{S}}, N)$ secret-key generation strategies for the coalition of agents $\mathcal{S}$ such that*

$$\lim_{N\to\infty} \mathbb{P}[\widehat{K}_{\mathcal{S}} \neq K_{\mathcal{S}}] = 0 \text{ (Reliability)}, \tag{5}$$

$$\lim_{N\to\infty} I\left(K_{\mathcal{S}}; A_{\mathcal{S}}, X_{\mathcal{L}\setminus\mathcal{S}}^N\right) = 0 \text{ (Collective Secrecy)}, \tag{6}$$

$$\lim_{N\to\infty} \log|\mathcal{K}_{\mathcal{S}}| - H(K_{\mathcal{S}}) = 0 \text{ (Key Uniformity)}. \tag{7}$$

The secrecy constraint (6) with respect to the agents outside of $\mathcal{S}$ means that the agents in $\mathcal{S}$ follow a protocol for secret-key generation under the information-theoretic constraint that the agent in $\mathcal{L}\setminus\mathcal{S}$ are not assumed to follow *any specific communication strategy*. Note that choosing $\mathcal{S} = \mathcal{L}$ recovers the setting of Section II-A.

Remark 1. (6) *and* (7) *can be combined in only one condition. If*

$$\lim_{N\to\infty} N\mathbb{V}\left(p_{K_{\mathcal{S}}A_{\mathcal{S}}X_{\mathcal{L}\setminus\mathcal{S}}^N}, p_{\mathcal{U}_{\mathcal{S}}}p_{A_{\mathcal{S}}X_{\mathcal{L}\setminus\mathcal{S}}^N}\right) = 0, \tag{8}$$

then (6) *and* (7) *hold by [31, Lemma 1] and [32, Lemma 2.7], where $p_{\mathcal{U}_{\mathcal{S}}}$ denotes the uniform distribution over $\mathcal{K}_{\mathcal{S}}$.*

C. Secret-Key Generation With Selfish Users

We consider the secret-key generation problem described by Definitions 1 and 2 when the agents are selfish, i.e., they are solely interested in maximizing their own secret-key rate. The agents can potentially form coalitions to achieve this goal, in the sense that subsets of agents can agree on a collective protocol to follow before the actual secret-key generation protocol occurs. Note that the model allows the agents to communicate with each other over the public channel and determine whether or not they want to be part of a coalition. However, we do not assume any privilege for coalitions, in particular, if the members of a given coalition need to communicate with each other, they only have access to the aforementioned public communication channel. In the following, *cooperation among a set of agents $\mathcal{S} \subseteq \mathcal{L}$ means that the agents in $\mathcal{S}$ agree on participating in a secret key generation scheme as defined in Definition 3*.

The questions we are interested in are the following. (i) Can selfish agents find a consensus about which coalitions to form? (ii) If such consensus exists, how should the value, i.e., the secret-key sum-rate, of each coalition be allocated among its agents?

We define a game corresponding to this problem as follows. For $\mathcal{S} \subseteq \mathcal{L}$, let $\mathfrak{S}(\mathcal{S})$ be the set of all sequences $(S_N(\mathcal{S}))_{N\in\mathbb{N}}$, where $S_N(\mathcal{S})$ is a $((2^{NR_i})_{i\in\mathcal{S}}, N)$ secret-key generation strategy as defined in Definition 3. The set of strategies that coalition $\mathcal{S} \subseteq \mathcal{L}$ can adopt is $\mathfrak{S}(\mathcal{S})$. Consider a sequence of payoff functions $(\pi_l)_{l\in\mathcal{L}}$, where for $l \in \mathcal{L}$, $\pi_l(a_{\mathcal{L}})$ represents the payoff of agent l, i.e., the rate of its secret key, when the strategies $a_{\mathcal{L}} \in \bigcup_{\mathcal{P}\in\mathfrak{P}}\left(\bigtimes_{\mathcal{S}\in\mathcal{P}}\mathfrak{S}(\mathcal{S})\right)$ are played by the agents, where $\mathfrak{P}$ denotes the set of all partitions of $\mathcal{L}$. We assume a decentralized setting in the sense that the base station does not influence the strategies of the agents, i.e., is not a player but a passive entity.

Remark 2. *Our study aims at modeling selfish constraints for the agents, and how they can be accounted in a decentralized manner without an external authority entity. However, considering an active base station that could force coalition-building is an interesting avenue for future research.*

We next wish to formulate a coalitional game by associating with each coalition of cooperating agents $\mathcal{S} \subseteq \mathcal{L}$ a certain worth $v(\mathcal{S})$. As detailed in Section III, such mapping v provides with a tool to study the stability of coalitions formed by the agents, where stability of a coalition means that there is no incentive to merge with another coalition or to split into smaller coalitions. Two potential choices for the worth $v(\mathcal{S})$ of coalition $\mathcal{S} \subseteq \mathcal{L}$ are the following, [33], [34]

$$\max_{a_{\mathcal{S}}\in\mathfrak{S}(\mathcal{S})} \min_{a_{\mathcal{L}\setminus\mathcal{S}}\in\mathfrak{S}(\mathcal{L}\setminus\mathcal{S})} \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{L}\setminus\mathcal{S}}), \tag{9}$$

$$\min_{a_{\mathcal{L}\setminus\mathcal{S}}\in\mathfrak{S}(\mathcal{L}\setminus\mathcal{S})} \max_{a_{\mathcal{S}}\in\mathfrak{S}(\mathcal{S})} \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{L}\setminus\mathcal{S}}), \tag{10}$$

where the quantity in (9) corresponds to the payoff that coalition $\mathcal{S}$ can ensure to its members regardless of the strategies adopted by the member of $\mathcal{L}\setminus\mathcal{S}$, and the one in (10) to the payoff that coalition $\mathcal{L}\setminus\mathcal{S}$ cannot prevent coalition $\mathcal{S}$ to receive. See, for instance, [35] for a detailed explanation of the subtle difference between these two notions in general. Observe also that for our problem both quantities are equal since for any $\mathcal{S} \subseteq \mathcal{L}$, there exists $a^*_{\mathcal{L}\setminus\mathcal{S}} \in \mathfrak{S}(\mathcal{L}\setminus\mathcal{S})$ such that for any strategies $a_{\mathcal{S}} \in \mathfrak{S}(\mathcal{S})$, we have

$$\sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{L}\setminus\mathcal{S}}) \geq \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a^*_{\mathcal{L}\setminus\mathcal{S}}). \tag{11}$$

Indeed, consider $a^*_{\mathcal{L}\backslash\mathcal{S}}$ as the strategies consisting in publicly disclosing X_i^N for all agents $i \in \mathcal{L}\backslash\mathcal{S}$.

To summarize, for a DMS $\left(\mathcal{X}_\mathcal{L} \times \mathcal{X}_0, p_{X_\mathcal{L} X_0}\right)$, the secret-key generation problem described in Definitions 1, 2, when the agents are selfish is cast as a coalitional games $(\mathcal{L}, v)$ where the value function is defined as

$$v : 2^\mathcal{L} \to \mathbb{R}^+, \mathcal{S} \mapsto \max_{a_\mathcal{S} \in \mathfrak{S}(\mathcal{S})} \min_{a_{\mathcal{L}\backslash\mathcal{S}} \in \mathfrak{S}(\mathcal{L}\backslash\mathcal{S})} \sum_{i\in\mathcal{S}} \pi_i(a_\mathcal{S}, a_{\mathcal{L}\backslash\mathcal{S}}) \quad (12)$$

such that for any $\mathcal{S} \subseteq \mathcal{L}$, $v(\mathcal{S})$ corresponds to the maximal secret-key sum-rate achievable by coalition $\mathcal{S}$ when *no specific strategy is assumed* for the agents in $\mathcal{L}\backslash\mathcal{S}$.

III. Game Analysis

For any $\mathcal{S} \subseteq \mathcal{L}$, we define the complement of $\mathcal{S}$ as $\mathcal{S}^c \triangleq \mathcal{L}\backslash\mathcal{S}$. In Section III-A, we study the properties of the game defined in Section II-C and, in Section III-B, we propose candidates for the secret-key rate allocation.

A. Properties of the Game and Characterization of Its Core

We first provide the following characterization of the value function v defined in (12).

Theorem 1. *We have for any coalition $\mathcal{S} \subseteq \mathcal{L}$*

$$\max_{a_\mathcal{S} \in \mathfrak{S}(\mathcal{S})} \min_{a_{\mathcal{S}^c} \in \mathfrak{S}(\mathcal{S}^c)} \sum_{i\in\mathcal{S}} \pi_i(a_\mathcal{S}, a_{\mathcal{S}^c}) = I\left(X_\mathcal{S}; X_0 | X_{\mathcal{S}^c}\right). \quad (13)$$

Hence, for any $\mathcal{S} \subseteq \mathcal{L}$

$$v(\mathcal{S}) = I\left(X_\mathcal{S}; X_0 | X_{\mathcal{S}^c}\right). \quad (14)$$

Proof. Consider the secret-key generation problem described in Definitions 3 and 4. $v(\mathcal{S})$ corresponds to the secret-key sum-rate capacity $C_\mathcal{S}$ for coalition $\mathcal{S} \subseteq \mathcal{L}$, i.e., the maximal secret-key sum-rate $\sum_{i\in\mathcal{S}} R_i$ achievable by coalition $\mathcal{S}$. Moreover, we have

$$C_\mathcal{S} = I\left(X_\mathcal{S}; X_0 | X_{\mathcal{S}^c}\right). \quad (15)$$

The converse proof for (15) follows from [15] and [16] by considering two legitimate users, each observing $X_\mathcal{S}^N$ and X_0^N, one Eavesdropper, observing $X_{\mathcal{S}^c}^N$, and by the Markov chain (1). The achievability part is more involved and will later follow from Corollary 2 derived in Section IV. We intentionally postpone its proof to streamline presentation. ∎

We now review the notion of superadditivity.

Definition 5. *A game $(\mathcal{L}, v)$ is superadditive if $v : 2^\mathcal{L} \to \mathbb{R}^+$ is such that*

$$\forall \mathcal{S}, \mathcal{T} \subseteq \mathcal{L}, \mathcal{S} \cap \mathcal{T} = \emptyset \implies v(\mathcal{S}) + v(\mathcal{T}) \leq v(\mathcal{S} \cup \mathcal{T}). \quad (16)$$

Property 1. *The game $(\mathcal{L}, v)$ defined in (12) is superadditive.*

Proof. Let $\mathcal{S}, \mathcal{T} \subseteq \mathcal{L}$, $\mathcal{S} \cap \mathcal{T} = \emptyset$. We have

$$\begin{aligned} v(\mathcal{S} \cup \mathcal{T}) &= I\left(X_{\mathcal{S}\cup\mathcal{T}}; X_0 | X_{\mathcal{S}^c \cap \mathcal{T}^c}\right) && (17a)\\ &= I\left(X_\mathcal{S}; X_0 | X_{\mathcal{S}^c \cap \mathcal{T}^c}\right) + I\left(X_\mathcal{T}; X_0 | X_{\mathcal{T}^c}\right) && (17b)\\ &= H\left(X_\mathcal{S} | X_{\mathcal{S}^c \cap \mathcal{T}^c}\right) - H\left(X_\mathcal{S} | X_0\ X_{\mathcal{S}^c}\right) \\ &\quad + I\left(X_\mathcal{T}; X_0 | X_{\mathcal{T}^c}\right) && (17c)\\ &\geq I\left(X_\mathcal{S}; X_0 | X_{\mathcal{S}^c}\right) + I\left(X_\mathcal{T}; X_0 | X_{\mathcal{T}^c}\right) && (17d)\\ &= v(\mathcal{S}) + v(\mathcal{T}), && (17e) \end{aligned}$$

where (17c) holds by (1), (17d) holds because conditioning reduces entropy. ∎

Superadditivity implies that there is an interest in forming a large coalition to obtain a larger secret-key sum rate, however, large coalition might not be in the individual interest of the agents, in the sense that increasing the secret-key sum-rate of a given coalition might not lead to an increased individual secret-key rate for every player in the coalition. A useful concept to overcome this complication is the core of the game.

Definition 6 (e.g. [36])**.** *The core of a superadditive game $(\mathcal{L}, v)$ is defined as follows.*

$$\mathcal{C}(v) \triangleq \left\{ (R_l)_{l\in\mathcal{L}} : \sum_{l\in\mathcal{L}} R_l = v(\mathcal{L}) \text{ and } \sum_{i\in\mathcal{S}} R_i \geq v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L} \right\}. \quad (18)$$

Observe that for any point in the core, the grand coalition, i.e., the coalition $\mathcal{L}$, is in the best interest to all agents, since the set of inequalities in (18) ensures that no coalition of agents can increase its secret-key sum-rate by leaving the grand coalition. Observe also that for any point in the core the maximal secret-key sum rate $v(\mathcal{L})$ for the grand coalition is achieved. In general, the core of a game can be empty. However, we will show that the game we have defined has a non-empty core.

Definition 6 further clarifies the choice of the value function v. A coalition $\mathcal{S}$ wishes to be associated with a value $v(S)$ as large as possible, while the agents outside $\mathcal{S}$ wish $v(S)$ to be as small as possible to demand a higher share of $v(\mathcal{L})$. The latter achieve their goal by waiving a threat argument, which consists in arguing that they could adopt the strategy that minimizes $v(S)$ by publicly disclosing their source observations, whereas coalition $\mathcal{S}$ achieves its goal by arguing that it can always achieve the secret-key sum-rate capacity of Theorem 1, irrespective of the strategy of agents in $\mathcal{S}^c$. This formulation is analogous to the one for the Gaussian multiple access channel problem studied in [2], and the Gaussian multiple access wiretap channel problem studied in [37], where users can also form coalitions to request a larger communication sum-rate by means of jamming threats, and is generically termed as alpha effectiveness or alpha theory [33]–[35].

We now introduce the notion of convexity for a game to better understand the structure of the core of our game.

Definition 7 ([38])**.** *A game $(\mathcal{L}, v)$ is convex if $v : 2^\mathcal{L} \to \mathbb{R}^+$ is supermodular, i.e.,*

$$\forall \mathcal{U}, \mathcal{V} \subseteq \mathcal{L}, v(\mathcal{U}) + v(\mathcal{V}) \leq v(\mathcal{U} \cup \mathcal{V}) + v(\mathcal{U} \cap \mathcal{V}). \quad (19)$$

The intuition behind this definition is that supermodularity provides a stronger incentive to form coalition than superadditity. Indeed, supermodularity of a function $v : 2^\mathcal{L} \to \mathbb{R}^+$ can equivalently be defined as follows [38]

$$\forall l \in \mathcal{L}, \forall \mathcal{T} \subseteq \mathcal{L}\backslash\{l\}, \forall \mathcal{S} \subseteq \mathcal{T}, \quad v(\mathcal{S} \cup \{l\}) - v(\mathcal{S}) \leq v(\mathcal{T} \cup \{l\}) - v(\mathcal{T}), \quad (20)$$

which means that, in addition to superaddivity, the contribution of a single agent to a given coalition increases with the

size of the coalition it joins. We also refer to [38] for other interpretations of supermodularity.

Proposition 1. *The game* $(\mathcal{L}, v)$ *defined in* (12) *is convex.*

Proof. For any $\mathcal{S} \subseteq \mathcal{L}$, we have

$$I(X_{\mathcal{S}}; X_0|X_{\mathcal{S}^c}) = H(X_{\mathcal{S}}|X_{\mathcal{S}^c}) - H(X_{\mathcal{S}}|X_{\mathcal{S}^c}X_0) \quad (21a)$$
$$= H(X_{\mathcal{S}}|X_{\mathcal{S}^c}) - H(X_{\mathcal{S}}|X_0) \quad (21b)$$
$$= H(X_{\mathcal{L}}) - H(X_{\mathcal{S}^c}) - H(X_{\mathcal{S}}|X_0), \quad (21c)$$

where we have used the Markov chain (1) in the second equality. Then, $\mathcal{S} \mapsto -H(X_{\mathcal{S}}|X_0)$ is supermodular because for any $\mathcal{U}, \mathcal{V} \subseteq \mathcal{L}$,

$$H(X_{\mathcal{U}\cup\mathcal{V}}|X_0) + H(X_{\mathcal{U}\cap\mathcal{V}}|X_0) \quad (22a)$$
$$= H(X_{\mathcal{U}}|X_0) + H(X_{\mathcal{V}\setminus\mathcal{U}}|X_{\mathcal{U}}X_0) + H(X_{\mathcal{U}\cap\mathcal{V}}|X_0) \quad (22b)$$
$$\leq H(X_{\mathcal{U}}|X_0) + H(X_{\mathcal{V}\setminus\mathcal{U}}|X_{\mathcal{U}\cap\mathcal{V}}X_0) + H(X_{\mathcal{U}\cap\mathcal{V}}|X_0) \quad (22c)$$
$$= H(X_{\mathcal{U}}|X_0) + H(X_{\mathcal{V}}|X_0), \quad (22d)$$

where (22c) holds because conditioning reduces entropy. Consequently, $\mathcal{S} \mapsto -H(X_{\mathcal{S}^c})$ is also supermodular since for any supermodular function w, $\mathcal{S} \mapsto w(\mathcal{S}^c)$ is supermodular. Hence, by (21c) we conclude that v is supermodular. ∎

A consequence of Proposition 1 is that the core of our game is non-empty.

Corollary 1. *By [38], any convex game has non-empty core. Hence, by Proposition 1, our game defined in* (12) *has a non-empty core* $\mathcal{C}(v)$.

Remark 3. *From a geometric point of view,* $\left\{(R_l)_{l\in\mathcal{L}} : \sum_{i\in\mathcal{S}} R_i \geq v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L}\right\}$ *is a contrapolymatroid [39] when* v *is convex, and its intersection with the hyperplane* $\left\{(R_l)_{l\in\mathcal{L}} : \sum_{l\in\mathcal{L}} R_l = v(\mathcal{L})\right\}$ *forms the core of* v *[38]. See Example 2 and Figure 2 for an illustration.*

Remark 4. *In the case of a convex game, the core coincides with the bargaining set for the grand coalition [40] and thus admits an alternative interpretation, in terms of stable allocations resulting from a sequence of "threats" and "counter-threats", see [40], [41] for further details.*

We provide an alternative characterization of the core that will turn out to be useful in the following. It can also be viewed as a converse for our problem since the secret-key rate-tuples in the core are upper-bounded.

Theorem 2. *The core* $\mathcal{C}(v)$ *of the game* $(\mathcal{L}, v)$ *defined in* (12) *is given by*

$$\left\{(R_l)_{l\in\mathcal{L}} : \forall \mathcal{S} \subseteq \mathcal{L}, \; I(X_{\mathcal{S}}; X_0) - I(X_{\mathcal{S}}; X_{\mathcal{S}^c}) \leq \sum_{i\in\mathcal{S}} R_i \leq I(X_{\mathcal{S}}; X_0)\right\}. \quad (23)$$

Proof. We have the following equivalences

$$\left(\sum_{l\in\mathcal{L}} R_l = v(\mathcal{L}) \text{ and } \sum_{i\in\mathcal{S}} R_i \geq v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L}\right)$$
$$\iff \left(\sum_{i\in\mathcal{S}} R_i = v(\mathcal{L}) - \sum_{i\notin\mathcal{S}^c} R_i \text{ and } \sum_{i\in\mathcal{S}} R_i \geq v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L}\right)$$
$$\iff \left(v(\mathcal{L}) - v(\mathcal{S}^c) \geq \sum_{i\in\mathcal{S}} R_i \geq v(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{L}\right).$$

Finally, for any $\mathcal{S} \subseteq \mathcal{L}$, we have

$$v(\mathcal{L}) - v(\mathcal{S}^c) = I(X_{\mathcal{L}}; X_0) - I(X_{\mathcal{S}^c}; X_0|X_{\mathcal{S}}) \quad (25a)$$
$$= I(X_{\mathcal{S}}; X_0), \quad (25b)$$

and by the Markov chain (1),

$$v(\mathcal{S}) = I(X_{\mathcal{S}}; X_0) - I(X_{\mathcal{S}}; X_{\mathcal{S}^c}). \quad (26)$$

∎

B. Candidates for the Secret-Key Rate Allocation

Although $\mathcal{C}(v)$ has been shown to be non-empty in Section III-A, a remaining issue is now to choose a specific rate-tuple allocation in the core. Shapley introduced a solution concept to ensure fairness according to the following axioms.

(i) Efficiency axiom, i.e., the secret-key sum-rate capacity for the grand coalition is achieved;
(ii) Symmetry axiom, i.e., any two agents that equally contribute to any coalition in the sense that for any $i, j \in \mathcal{L}$, for any $\mathcal{S} \subseteq L$ such that $i \neq j$ and $i, j \notin \mathcal{S}$, $v(\mathcal{S} \cup \{i\}) = v(\mathcal{S} \cup \{j\})$, obtain the same individual secret-key rate;
(iii) Dummy axiom, i.e., any agent that does not bring value to any coalition he can join, in the sense, for any $i \in \mathcal{L}$, for any $\mathcal{S} \subseteq L$ such that $i \notin \mathcal{S}$, $v(\mathcal{S} \cup \{i\}) = v(\mathcal{S})$, receives a null secret-key rate;
(iv) Additivity axiom, i.e., for any two games v and u played by the agents, the individual secret-key length obtained by an agent for the game $u + v$, is the sum of secret-key lengths when u and v are played separately.

We give an interpretation of the additivity axiom in the situation described next. For $i \in \{1, 2\}$, assume that the agents collect N source observations, denoted by $(X^N_{\mathcal{L},i}, X^N_{0,i})$, for a source with fixed probability distribution $p_{X_{\mathcal{L},i}X_{0,i}}$. For instance, when the source is obtained from channel gains measurements [17]–[20], the source statistics will change if the agents randomly change their physical location over time. We also assume that $p_{X_{\mathcal{L},1}X_{0,1}X_{\mathcal{L},2}X_{0,2}} = p_{X_{\mathcal{L},1}X_{0,1}} p_{X_{\mathcal{L},2}X_{0,2}}$. Let $i \in \{1, 2\}$ and define $\bar{i} = 3 - i$. We define the game v_i as extracting keys from $(X^N_{\mathcal{L},i}, X^N_{0,i})$ *when the distribution* $p_{X_{\mathcal{L},\bar{i}},X_{0,\bar{i}}}$ *is unknown*, and we define the game w as extracting keys from $(X^N_{\mathcal{L},1}, X^N_{0,1}, X^N_{\mathcal{L},2}, X^N_{0,2})$ *when both distributions* $p_{X_{\mathcal{L},1}X_{0,1}}$ *and* $p_{X_{\mathcal{L},2}X_{0,2}}$ *are known*. By independence and by Theorem 1, the value function associated with w is the sum of the value functions of v_1 and v_2. In this setup, we interpret the additivity axiom as follows. If the agents extract keys from $(X^N_{\mathcal{L},i}, X^N_{0,i})$ being ignorant of the distribution $p_{X_{\mathcal{L},\bar{i}},X_{0,\bar{i}}}$, then they obtain the same payoff as if they had to extract keys from $(X^N_{\mathcal{L},1}, X^N_{0,1}, X^N_{\mathcal{L},2}, X^N_{0,2})$ with the knowledge of both $p_{X_{\mathcal{L},1},X_{0,1}}$ and $p_{X_{\mathcal{L},2},X_{0,2}}$. Hence, under the same assumptions, the additivity axiom means that even if the agents do not know in advance the number M of source observation batches from independent sources they are going to obtain, they can, after obtaining each batch of observations, successively generate keys without this knowledge and obtain the same individual

key lengths as if they had waited to obtain the M batches to generate keys.

Example 1. *We have the following intuitive property. If there exist $i, j \in \mathcal{L}$ such that $i \neq j$ and $p_{X_i|X_0} = p_{X_j|X_0}$, then Agent i and Agent j satisfy the symmetry axiom described above.*

Proof. Let $i, j \in \mathcal{L}$, and $\mathcal{S} \subseteq L$ such that $i \neq j$ and $i, j \notin \mathcal{S}$. Define $\overline{\mathcal{S}^c} \triangleq \mathcal{S}^c \backslash \{i, j\}$. We have

$$\begin{aligned} &v(\mathcal{S} \cup \{i\}) \\ &\quad = H(X_{\mathcal{L}}) - H(X_{(\mathcal{S}\cup\{i\})^c}) - H(X_{\mathcal{S}\cup\{i\}}|X_0) && \text{(27a)} \\ &\quad = H(X_{\mathcal{L}}) - H(X_j X_{\overline{\mathcal{S}^c}}) - H(X_i|X_0) - H(X_{\mathcal{S}}|X_0) && \text{(27b)} \\ &\quad = H(X_{\mathcal{L}}) - H(X_i X_{\overline{\mathcal{S}^c}}) - H(X_j|X_0) - H(X_{\mathcal{S}}|X_0) && \text{(27c)} \\ &\quad = v(\mathcal{S} \cup \{j\}), && \text{(27d)} \end{aligned}$$

where (27a) holds by (21c), (27b) holds by definition of $\overline{\mathcal{S}^c}$ and by the Markov chain (1), (27c) holds because by the Markov chain (1) $p_{X_i X_{\overline{\mathcal{S}^c}} X_0} = p_{X_i|X_0} p_{X_{\overline{\mathcal{S}^c}} X_0} = p_{X_j|X_0} p_{X_{\overline{\mathcal{S}^c}} X_0} = p_{X_j X_{\overline{\mathcal{S}^c}} X_0}$, which implies by marginalization over X_0, $p_{X_i X_{\overline{\mathcal{S}^c}}} = p_{X_j X_{\overline{\mathcal{S}^c}}}$, which in turn implies $H(X_i X_{\overline{\mathcal{S}^c}}) = H(X_j X_{\overline{\mathcal{S}^c}})$, (27d) holds similar to (27a) and (27b). ∎

Proposition 2 (e.g. [42])**.** *Given a coalitional game $(\mathcal{L}, v)$, there exists a unique L-tuple $\left(R_l^{\text{Shap}}\right)_{l\in\mathcal{L}}$ that satisfies the efficiency, symmetry, dummy, and additivity axiom described above. $\left(R_l^{\text{Shap}}\right)_{l\in\mathcal{L}}$ is called the Shapley value.*

For convex games, the Shapley value is in the core, and is explicited in the following proposition.

Proposition 3. *The Shapley value of $(\mathcal{L}, v)$ defined in* (12) *is in $\mathcal{C}(v)$ and is given by $\forall l \in \mathcal{L}$,*

$$\begin{aligned} R_l^{\text{Shap}} &= \sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \frac{|\mathcal{S}|!(L-|\mathcal{S}|-1)!}{L!} \left(v(\mathcal{S}\cup\{l\}) - v(\mathcal{S})\right) && \text{(28a)} \\ &= I\left(X_l; X_0\right) - \frac{1}{L} \sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \binom{L-1}{|\mathcal{S}|}^{-1} I\left(X_l; X_{\mathcal{S}}\right). && \text{(28b)} \end{aligned}$$

Proof. The fact that the Shapley value belongs to the core follows by [38] from the convexity of $(\mathcal{L}, v)$ proved in Proposition 1. (28a) is also from [38]. (28b) is obtained by remarking that for any $l \in \mathcal{L}$, for any $\mathcal{S} \subseteq \mathcal{L}\backslash\{l\}$

$$\begin{aligned} &v(\mathcal{S}\cup\{l\}) - v(\mathcal{S}) \\ &\quad = H(X_{\mathcal{S}^c}) + H(X_{\mathcal{S}}|X_0) - H(X_{(\mathcal{S}\cup\{l\})^c}) \\ &\qquad - H(X_{\mathcal{S}\cup\{l\}}|X_0) && \text{(29a)} \\ &\quad = H(X_{\mathcal{S}^c\cap\{l\}}|X_{\mathcal{S}^c\backslash\{l\}}) - H(X_l|X_0\ X_{\mathcal{S}}) && \text{(29b)} \\ &\quad = H\left(X_l|X_{\mathcal{S}^c\backslash\{l\}}\right) - H\left(X_l|X_0\right) && \text{(29c)} \\ &\quad = I\left(X_l; X_0\right) - I\left(X_l; X_{\mathcal{S}^c\backslash\{l\}}\right), && \text{(29d)} \end{aligned}$$

where (29a) holds by (21c), (29c) holds because $l \notin \mathcal{S}$ and by the Markov chain (1). Finally, we conclude by observing that

$$\begin{aligned} &\sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \frac{|\mathcal{S}|!(L-|\mathcal{S}|-1)!}{L!} \\ &\qquad = \sum_{k=0}^{L-1} \binom{L-1}{k} \frac{k!(L-k-1)!}{L!} = 1, \quad \text{(30)} \end{aligned}$$

and that a change of variables yields

$$\begin{aligned} &\sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \frac{|\mathcal{S}|!(L-|\mathcal{S}|-1)!}{L!} I\left(X_l; X_{\mathcal{S}^c\backslash\{l\}}\right) \\ &\qquad = \sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \frac{|\mathcal{S}|!(L-|\mathcal{S}|-1)!}{L!} I\left(X_l; X_{\mathcal{S}}\right). \quad \text{(31)} \end{aligned}$$

∎

Remark 5. *Geometrically, the Shapley value corresponds to the center of gravity of the vertices of $\mathcal{C}(v)$ [38]. See Example 2 and Figure 2 for an illustration.*

Observe that (28b) quantifies the difference of key length obtained for Agent l, $l \in \mathcal{L}$, between the case $L = 1$ and the case $L > 1$. Note also that the term $\frac{1}{L}\sum_{\mathcal{S}\subseteq\mathcal{L}\backslash\{l\}} \binom{L-1}{|\mathcal{S}|}^{-1} I\left(X_l; X_{\mathcal{S}}\right)$ is upper-bounded by $I\left(X_l; X_{\mathcal{L}\backslash\{l\}}\right)$ according to Theorem 2 since the Shapley value belongs to the core.

Note that the Shapley value might not always be meaningful as a solution concept. In particular, the additivity axiom might not always be relevant in our problem, for instance, if the agents do not obtain several batches of observations from sources with independent statistics. Finding an axiomatized solution concept that could be universally agreed upon in our setting remains an open problem.

We next discuss the nucleolus as solution concept and one of its non-axiomatized interpretation that has attracted a certain interest in many studies.

Definition 8 ([43])**.** *Define the set $\mathcal{Y} \triangleq \{\mathbf{y} = (y_i)_{i\in\mathcal{L}} \in \mathbb{R}_+^L : \sum_{i\in\mathcal{L}} y_i = v(\mathcal{L})\}$. For $\mathbf{y} \in \mathcal{Y}$, for $\mathcal{S} \in 2^{\mathcal{L}}$, define the excess $e(\mathbf{y}, \mathcal{S}) \triangleq v(\mathcal{S}) - \sum_{i\in\mathcal{S}} y_i$, and define the vector $\theta(\mathbf{y}) = (\theta_i(\mathbf{y}))_{i\in[\![1,2^L]\!]} \in \mathbb{R}^{2^L}$ as $(e(\mathbf{y}, \mathcal{S}))_{\mathcal{S}\in 2^{\mathcal{L}}}$ sorted in nonincreasing order, i.e., for $i, j \in [\![1, 2^L]\!], i < j \implies \theta_i(\mathbf{y}) \geq \theta_j(\mathbf{y})$. The nucleolus is defined as*

$$\{\mathbf{y}_0 \in \mathcal{Y} : \theta(\mathbf{y}_0) \preceq \theta(\mathbf{y}), \forall y \in \mathcal{Y}\}, \quad \text{(32)}$$

where $\preceq$ denote the lexicographic order, i.e., for $\mathbf{y}^{(1)}, \mathbf{y}^{(2)} \in \mathcal{Y}$,

$$\begin{aligned} \left(\mathbf{y}^{(1)} \preceq \mathbf{y}^{(2)}\right) \iff &\left(\mathbf{y}^{(1)} = \mathbf{y}^{(2)}\right. \\ &\left. \text{or } \exists i_0, \left(\forall j < i_0, y_j^{(1)} = y_j^{(2)} \text{ and } y_{i_0}^{(1)} < y_{i_0}^{(2)}\right)\right). \quad \text{(33)} \end{aligned}$$

A possible interpretation of the nucleolus is to see the excess $e(\mathbf{y}, \mathcal{S}) \triangleq v(\mathcal{S}) - \sum_{i\in\mathcal{S}} y_i$ for some $\mathbf{y} \in \mathcal{Y}$, $\mathcal{S} \in 2^{\mathcal{L}}$, as an indicator of dissatisfaction of coalition $\mathcal{S}$ associated with $\mathbf{y}$ (the higher the excess, the higher the dissatisfaction). One thus might want to choose the $\mathbf{y}$ that minimizes the maximal excess, i.e., the first component of θ. If several choices for $\mathbf{y}$ are possible, one can decide to select $\mathbf{y}$ such that the second largest excess, i.e., the second component of θ, is minimized. One can then continue until a unique choice for $\mathbf{y}$ is obtained as stated in Proposition 4. This interpretation appears, for instance, in [36].

Proposition 4 ([43])**.** *For a convex game, the nucleolus is a singleton and belongs to the core.*

The nucleolus has, however, no closed-form formula and involves the resolution of successive minimization problems. We illustrate this concept in the following example.

Algorithm 1 Nucleolus Computation

$k \leftarrow 0$
$\mathcal{E}_0 \leftarrow \emptyset$
while the system (S_k) has rank $< L$ **do**
  $k \leftarrow k+1$
  Solve the following linear program and let z_k^* denote the value of the objective function obtained

$$\text{Minimize } z_k \text{ subject to}$$

$$\begin{cases} z_k + \sum_{i\in\mathcal{S}} x_i \geq v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L} \text{ s.t. } \mathcal{S} \notin \cup_{j=0}^{k-1}\mathcal{E}_j & (E_k) \\ \left(\begin{array}{c} z_j^* + \sum_{i\in\mathcal{S}} x_i = v(\mathcal{S}), \forall \mathcal{S} \in \mathcal{E}_j,\ j \in [\![1, k-1]\!] \\ \sum_{i\in\mathcal{L}} x_i = v(\mathcal{L}) \end{array}\right) & (S_k) \end{cases}$$

  Define $\mathcal{E}_k \triangleq \{\mathcal{S} \subset \mathcal{L} : (E_k) \text{ holds with equality}\}$
end whilereturn the nucleolus $\left(R_i^{\text{Nucl}}\right)_{i\in\mathcal{L}} = (x_i)_{i\in\mathcal{L}}$

For completeness and to compute the nucleolus in Example 2, we summarize in Algorithm 1 a concise description of the method described in [44] and [45].

Remark 6. *In the case of a convex game, the nucleolus coincides with the kernel [36] and thus admits another interpretation, see [36, Sec. 5] for further details.*

Example 2. *Let X_0 be a Bernoulli random variable with parameter $q \in]0, 1/2[$. Define $X_l \triangleq X_0 \oplus B_l$, $\forall l \in \mathcal{L}$, where the B_l's are independent Bernoulli random variables with parameter $p_l \in]0, 1/2[$. Let $H_b(\cdot)$ denote the binary entropy and define for any $x \in [0, 1]$, $\bar{x} = 1 - x$. For any $\mathcal{S} \subseteq \mathcal{L}$, we have the following formula*

$$\begin{aligned} v(\mathcal{S}) &= H(X_{\mathcal{L}}) - H(X_{\mathcal{S}^c}) - H(X_{\mathcal{S}}|X_0) && (34a)\\ &= H(X_{\mathcal{L}}) - H(X_{\mathcal{S}^c}) - \textstyle\sum_{i\in\mathcal{S}} H_b(p_i) && (34b)\\ &= -\textstyle\sum_{\mathcal{T}\subseteq\mathcal{L}} f_{\mathcal{L}}(\mathcal{T}) \log f_{\mathcal{L}}(\mathcal{T}) \\ &\quad + \textstyle\sum_{\mathcal{T}\subseteq\mathcal{S}^c} f_{\mathcal{S}^c}(\mathcal{T}) \log f_{\mathcal{S}^c}(\mathcal{T}) \\ &\quad - \textstyle\sum_{i\in\mathcal{S}} H_b(p_i), && (34c) \end{aligned}$$

where (34a) *holds by* (21c), (34b) *holds by independence of the B_l's, and where in* (34c) *we have defined for any $\mathcal{S} \subseteq \mathcal{L}$*

$$f_{\mathcal{S}}: 2^{\mathcal{S}} \to \mathbb{R}_+, \mathcal{T} \mapsto q \prod_{i\in\mathcal{T}} p_i \prod_{j\in\mathcal{S}\setminus\mathcal{T}} \bar{p}_j + \bar{q} \prod_{i\in\mathcal{T}} \bar{p}_i \prod_{j\in\mathcal{S}\setminus\mathcal{T}} p_j. \quad (35)$$

Assume now that $L = 3$, and $(q\ p_1\ p_2\ p_3) = (0.40\ 0.20\ 0.27\ 0.25)$. We obtain $v(\{1\}) \approx 0.17\,134$, $v(\{2\}) \approx 0.08\,205$, $v(\{3\}) \approx 0.10\,142$, $v(\{1, 2\}) \approx 0.28\,771$, $v(\{1, 3\}) \approx 0.31\,679$, $v(\{2, 3\}) \approx 0.20\,155$, $v(\{1, 2, 3\}) \approx 0.46\,921$. Using Algorithm 1 and Proposition 3, we obtain the following secret-key rates

$$\begin{aligned} R_1^{\text{Nucl}} &\in [0.2109, 0.2110], \quad R_1^{\text{Shap}} \in [0.2165, 0.2166], \\ R_2^{\text{Nucl}} &\in [0.1172, 0.1173], \quad R_2^{\text{Shap}} \in [0.1142, 0.1143], \\ R_3^{\text{Nucl}} &\in [0.1410, 0.1411], \quad R_3^{\text{Shap}} \in [0.1384, 0.1385]. \end{aligned}$$

The core of the game, as well as the Shapley value and the nucleolus are depicted in Figure 2.

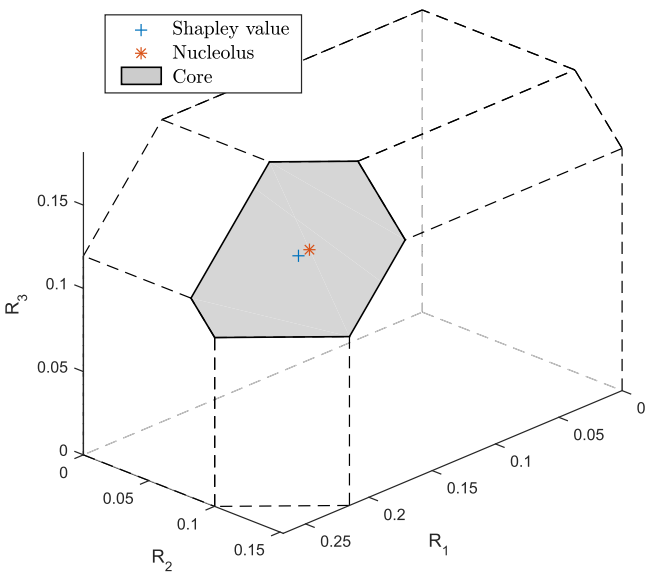

Fig. 2. Core, Shapley value, and nucleolus of the game described in Example 2.

IV. How to Achieve Any Point of the Core

We have seen in Section III that the grand coalition, i.e., the coalition $\mathcal{L}$, is in the best interest of all agents, and we have characterized the acceptable operating points as the core of the game. Assuming that the grand coalition agrees on an operating point in the core, we now would like to answer whether there exists a secret-key generation protocol for this specific operating point. We show in this section the following three results. In Theorem 3, we claim that the coding scheme presented in Section IV-A achieves for the grand coalition a region that contains the core $\mathcal{C}(v)$. The proof is presented in Section IV-B. In Theorem 4, we provide an achievable region for any coalition $\mathcal{S} \subset \mathcal{L}$ of agents. The coding scheme and its analysis partly rely on Theorem 3 and are discussed in Appendix C. Finally, we complete the proof of Theorem 1 with Corollary 2 obtained from Theorem 4.

Theorem 3. *Consider a DMS $\left(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0, p_{X_{\mathcal{L}}X_0}\right)$ such that $\forall l \in \mathcal{L}, |\mathcal{X}_l| = 2$. Any rate tuple in*

$$\mathcal{R}_{\mathcal{L}} \triangleq \left\{ (R_l)_{l\in\mathcal{L}} : 0 \leq \sum_{i\in\mathcal{S}} R_i \leq I(X_{\mathcal{S}}; X_0), \forall \mathcal{S} \subseteq \mathcal{L} \right\} \quad (36)$$

is achievable by the grand coalition, in the sense of Definition 2, with the coding scheme of Section IV-A. Moreover, by Theorem 2 we have

$$\mathcal{R}_{\mathcal{L}} \supseteq \mathcal{C}(v). \quad (37)$$

Theorem 4. *Consider a DMS $\left(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0, p_{X_{\mathcal{L}}X_0}\right)$ such that $\forall l \in \mathcal{L}, |\mathcal{X}_l| = 2$ and the Markov chain* (1) *holds. Any rate tuple in*

$$\mathcal{R}_{\mathcal{S}} \triangleq \left\{ (R_l)_{l\in\mathcal{S}} : 0 \leq \sum_{i\in\mathcal{T}} R_i \leq I(X_{\mathcal{T}}; X_0|X_{\mathcal{S}^c}), \forall \mathcal{T} \subseteq \mathcal{S} \right\} \quad (38)$$

is achievable in the sense of Definition 4 by the coalition of agents $\mathcal{S} \subset \mathcal{L}$.

Proof. See Appendix C. ∎

Corollary 2. *Theorem 4 implies the achievability part of Theorem 1, i.e., the secret-key sum rate $I(X_{\mathcal{S}}; X_0|X_{\mathcal{S}^c})$ is achievable by the coalition $\mathcal{S} \subseteq \mathcal{L}$.*

Proof. See Appendix D. ∎

Remark 7. *Note that Theorem 3 does not require the Markov chain* (1)*. Note also that Theorem 3 and Theorem 4 extend to prime size alphabets by using [46, Lemma 7] in place of Lemma 2.*

Remark 8. *Note that the region in Theorem 3 has also been shown achievable in [23] without the requirements of prime size alphabets. The main difference between Theorem 3 and [23] is that Theorem 3 provides an explicit coding scheme.*

A. Coding Scheme

The principle of the coding scheme is to separately deal with reliability and secrecy, as it can be done for secret-key generation between two users [47], albeit with additional complications. More specifically, a reconciliation step is first performed to allow the base station to reconstruct the observations $X_{\mathcal{L}}^N$ of the agents. Then, during a privacy amplification step, each agent extracts from its observations a key that can be reconstructed at the base station. The reconciliation step itself does not present any difficulty, the main complications, compared to a two-user scenario, are (i) to deal with a distributed setting in the privacy amplification step and (ii) to analyze the combination of the reconciliation and privacy amplification steps, as detailed in the next section.

Our coding scheme operates over B blocks of length N, where N and B are powers of 2. We define $\mathcal{B} \triangleq [\![1, B]\!]$. We omit indexation of the variables over blocks because encoding is identical for all blocks. The reconciliation step, described in Algoritm 2, makes use of polar codes. In particular we introduce the following notation. For $n \in \mathbb{N}$ and $N \triangleq 2^n$, let $G_n \triangleq \left[\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right]^{\otimes n}$ be the source polarization transform defined in [26]. For any $l \in \mathcal{L}$, we define

$$U_l^N \triangleq X_l^N G_n, \tag{39}$$

moreover, for any set $\mathcal{I} \subseteq [\![1, N]\!]$, we define $U_l^N[\mathcal{I}] \triangleq ((U_l)_i)_{i\in\mathcal{I}}$, where $(U_l)_i$ denotes the i-th component of the vector U_l^N, $i \in \mathcal{I}$. For any $l \in \mathcal{L}$, for any $\mathcal{S} \subseteq \mathcal{L}$, we also define the following "high entropy" and "very high entropy" sets.

$$\mathcal{H}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}} \triangleq \left\{i \in [\![1, N]\!] : H\left((U_l)_i|(U_l)^{i-1}X_0^N X_{1:l-1}^N X_{\mathcal{S}}^N\right) \geq \delta_N\right\}, \tag{40}$$

$$\mathcal{V}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}} \triangleq \left\{i \in [\![1, N]\!] : H\left((U_l)_i|(U_l)^{i-1}X_0^N X_{1:l-1}^N X_{\mathcal{S}}^N\right) \geq 1 - \delta_N\right\} \tag{41}$$

where we have defined $X_{1:l-1} \triangleq (X_j)_{j\in[\![1:l-1]\!]}$ and $X_{\mathcal{S}} \triangleq (X_j)_{j\in\mathcal{S}}$. An interpretation of these sets that will be used in our analysis can be summarized in the following two lemmas.

Algorithm 2 Reconciliation Protocol

for Block $b \in \mathcal{B}$ **do**
  Define $\check{X}_{\emptyset}^N \triangleq \emptyset$
  for $l \in \mathcal{L}$ **do**
    Agent l computes $U_l^N \triangleq X_l^N G_n$ and transmits $A_l \triangleq U_l^N[\mathcal{H}_{X_l|X_0X_{1:l-1}}]$ to the base station over the public channel
    Given A_l, X_0^N, and $\check{X}_{1:l-1}^N$, the base station forms $\check{X}_l^N$ an estimate of X_l^N using the SC decoder of [26]
  end for
  Define $A_{\mathcal{L}} \triangleq (A_l)_{l\in\mathcal{L}}$
  Define $\check{X}_{\mathcal{L}}^N \triangleq (\check{X}_l^N)_{l\in\mathcal{L}}$
end for
Let $A_{\mathcal{L}}^B$ denote the total public communication over the B blocks
The base station and the agents perform a final round of reconciliation on $(\check{X}_{\mathcal{L}}^N)^B$ (obtained above) and $(X_{\mathcal{L}}^N)^B$ as follows
Define $\widehat{X}_{\emptyset}^{NB} \triangleq \emptyset$
for $l \in \mathcal{L}$ **do**
  Agent $l \in \mathcal{L}$ computes $V^{NB} \triangleq X_l^{NB} G_{\log_2(NB)}$ and transmits $A_{0,l} \triangleq V^{NB}[\mathcal{H}_{X_l^N|X_{1:l-1}^N \check{X}_{\mathcal{L}}^N}]$ to the base station over the public channel
  Given $A_{0,l}$, $(\check{X}_{\mathcal{L}}^N)^B$, and $\widehat{X}_{1:l-1}^{NB}$, the base station forms $\widehat{X}_l^{NB}$ an estimate of X_l^{NB} using the SC decoder of [26]
end for
Define $\widehat{X}_{\mathcal{L}}^{NB} \triangleq (\widehat{X}_l^{NB})_{l\in\mathcal{L}}$
Define $A_0 \triangleq (A_{0,l})_{l\in\mathcal{L}}$

Lemma 1 (Source Coding With Side Information [26])**.** *Consider a discrete memoryless source with joint probability distribution p_{XY} over $\mathcal{X} \times \mathcal{Y}$ with $|\mathcal{X}| = 2$ and $\mathcal{Y}$ finite. Define $A^N \triangleq X^N G_n$, and for $\delta_N \triangleq 2^{-N^\beta}$ with $\beta \in]0, 1/2[$, the set $\mathcal{H}_{X|Y} \triangleq \left\{i \in [\![1, N]\!] : H(A_i|A^{i-1}Y^N) > \delta_N\right\}$. Given $A^N[\mathcal{H}_{X|Y}]$ and Y^N it is possible to form $\widehat{A}^N$ by the successive cancellation (SC) decoder of [26] such that $\lim_{N\to\infty} \mathbb{P}[\widehat{A}^N \neq A^N] = 0$. Moreover, $\lim_{N\to\infty} |\mathcal{H}_{X|Y}|/N = H(X|Y)$.*

Lemma 2 (Privacy Amplification [29])**.** *Consider a discrete memoryless source with joint probability distribution p_{XZ} over $\mathcal{X} \times \mathcal{Z}$ with $|\mathcal{X}| = 2$ and $\mathcal{Z}$ finite. Define $A^N \triangleq X^N G_n$, and for $\delta_N \triangleq 2^{-N^\beta}$ with $\beta \in]0, 1/2[$, the set $\mathcal{V}_{X|Z} \triangleq \left\{i \in [\![1, N]\!] : H(A_i|A^{i-1}Z^N) > 1 - \delta_N\right\}$. $A^N[\mathcal{V}_{X|Z}]$ is almost uniform and independent from Z^N in the sense $\lim_{N\to\infty} \mathbb{V}(p_{A^N[\mathcal{V}_{X|Z}]Z^N}, p_U p_{Z^N}) = 0$, where p_U is the uniform distribution over $\{0, 1\}^{|\mathcal{V}_{X|Z}|}$. Moreover, $\lim_{N\to\infty} |\mathcal{V}_{X|Z}|/N = H(X|Z)$.*

Hence, by Lemma 1, the vector $U_l^N[\mathcal{H}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}}]$, $l \in \mathcal{L}$, ensures near lossless reconstruction of X_l^N given $(X_0^N, X_{1:l-1}^N, X_{\mathcal{S}}^N)$. By Lemma 2, the vector $U_l^N[\mathcal{V}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}}]$, $l \in \mathcal{L}$, is almost uniform and independent from $(X_0^N, X_{1:l-1}^N, X_{\mathcal{S}}^N)$. Note also that by definition $\mathcal{V}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}} \subset \mathcal{H}_{X_l|X_0X_{1:l-1}X_{\mathcal{S}}}$. We refer to [29] and [46] for further discussion of theses sets.

Algorithm 3 Privacy Amplification Protocol

1: **for** Block $b \in \mathcal{B}$ **do**
2: **for** Agent $l \in \mathcal{L}$ **do**
3: Compute $K_l \triangleq F_l(X_l^N)$
4: Publicly transmit the choice of F_l to the base station
5: **end for**
6: **for** $l \in \mathcal{L}$ **do**
7: The base station computes $K_l \triangleq F_l(X_l^N)$
8: **end for**
9: **end for**

The privacy amplification step, described in Algorithm 3, relies on two-universal hash functions [48], [49].

Definition 9. *A family $\mathcal{F}$ of two-universal hash functions $\mathcal{F} = \{f : \{0,1\}^N \to \{0,1\}^r\}$ is such that*

$$\forall x, x' \in \{0,1\}^N, x \neq x' \implies \mathbb{P}[F(x) = F(x')] \leq 2^{-r}, \tag{42}$$

where F is a function uniformly chosen in $\mathcal{F}$.

For $l \in \mathcal{L}$, we let $F_l : \{0,1\}^N \to \{0,1\}^{r_l}$, be uniformly chosen in a family $\mathcal{F}_l$ of two-universal hash functions. Note that r_l represents the key length obtained by Agent l. The main difficulty in the analysis of the privacy amplification step is to find the admissible values, in the sense of Definition 2, for r_l. We leave these quantities unspecified in this section, and will specify them in Section IV-B.

B. Coding Scheme Analysis

1) Reconciliation Analysis: Line 15 in Algorithm 2 ensures that for a fixed N,

$$\begin{aligned}\mathbb{P}\left[\widehat{X}_{\mathcal{L}}^{NB} \neq (X_{\mathcal{L}}^N)^B\right] &\leq \sum_{l\in\mathcal{L}} \mathbb{P}\left[\widehat{X}_l^{NB} \neq X_l^{NB} | \widehat{X}_{1:l-1}^{NB} = X_{1:l-1}^{NB}\right] &\text{(43a)}\\ &\xrightarrow{B\to\infty} 0, &\text{(43b)}\end{aligned}$$

where the limit follows from Lemma 1.

2) Privacy Amplification Analysis: We will use the following notation. The indicator function is denoted by $\mathbb{1}\{\omega\}$, which is equal to 1 if the predicate ω is true and 0 otherwise. For a discrete random variable X distributed according to p_X over the alphabet $\mathcal{X}$, we let

$$\mathcal{T}_\epsilon^N(X) \triangleq \left\{x^N \in \mathcal{X}^N : \left|\frac{1}{N}\sum_{i=1}^N \mathbb{1}\{x_i = a\} - p_X(a)\right| \leq \epsilon p_X(a), \forall a \in \mathcal{X}\right\} \tag{44}$$

denote the ϵ-letter-typical set associated with p_X for sequences of length N, see, for instance, [50], and define $\mu_X \triangleq \min_{x\in S_X} p(x)$, where $S_X \triangleq \{x \in \mathcal{X} : p(x) > 0\}$. Additionally, the min-entropy of X is defined as

$$H_\infty(X) \triangleq -\log\left(\max_{x\in\mathcal{X}} p_X(x)\right). \tag{45}$$

We will need the following two lemmas. Lemma 3 is a refined version of [51] meant to relate a min-entropy to a Shannon entropy, which is easier to study, and Lemma 4 can be interpreted as quantifying how much information is revealed about $X_{\mathcal{S}}^N$ knowing the public communication $A_{\mathcal{L}}$.

Lemma 3 ([51], [52, Lemma 1.1])**.** *Let $\epsilon > 0$. Consider a DMS $(\mathcal{X} \times \mathcal{Z}, p_{XZ})$ and define the random variable Θ as*

$$\Theta \triangleq \mathbb{1}\left\{(X^B, Z^B) \in \mathcal{T}_{2\epsilon}^B(XZ)\right\} \mathbb{1}\left\{Z^B \in \mathcal{T}_\epsilon^B(Z)\right\}, \tag{46}$$

Then, $\mathbb{P}[\Theta = 1] \geq 1 - \delta_\epsilon^0(B)$, with

$$\delta_\epsilon^0(B) \triangleq 2|S_X|e^{-\epsilon^2 B\mu_X/3} + 2|S_{XZ}|e^{-\epsilon^2 B\mu_{XZ}/3}. \tag{47}$$

Moreover, if $z^B \in \mathcal{T}_\epsilon^B(Z)$, then

$$\begin{aligned}H_\infty(X^B|Z^B = z^B, \Theta = 1) &\geq B(1-\epsilon)H(X|Z) + \log(1 - \delta_\epsilon^1(B)), &\text{(48)}\end{aligned}$$

where $\delta_\epsilon^1(B) \triangleq 2|S_{XZ}|e^{-\epsilon^2\ B\mu_{XZ}/6}$.

Lemma 4. *For any $\mathcal{S} \subseteq \mathcal{L}$, we have*

$$H(X_{\mathcal{S}}^N|A_{\mathcal{L}}) \geq NI(X_{\mathcal{S}}; X_0) - o(N). \tag{49}$$

Proof. See Appendix A. ∎

We are now equipped to show (52h). Let $\mathcal{S} \subseteq \mathcal{L}$ and let

$$\begin{aligned}\Theta \triangleq \mathbb{1}\left\{(X_{\mathcal{L}}^{NB}, A_{\mathcal{L}}^B, A_0) \in \mathcal{T}_{2\epsilon}^B(X_{\mathcal{L}}^N A_{\mathcal{L}} A_0)\right\} \\ \times \mathbb{1}\left\{(A_{\mathcal{L}}^B, A_0) \in \mathcal{T}_\epsilon^B(A_{\mathcal{L}} A_0)\right\}. &\text{(50)}\end{aligned}$$

Fix $(a_{\mathcal{L}}^B, a_0) \in \mathcal{T}_\epsilon^B(A_{\mathcal{L}}, A_0)$. We define

$$\begin{aligned}\Omega \triangleq \mathbb{1}\Big\{&H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, A_0 = a_0, \Theta = 1) \\ &\geq H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, \Theta = 1) \\ &\quad - \textstyle\sum_{l\in\mathcal{L}} |\mathcal{H}_{X_l^N|X_{1:l-1}^N \check{X}_{\mathcal{L}}^N}| - \sqrt{NB}\Big\}. &\text{(51)}\end{aligned}$$

We have

$$\begin{aligned}&H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, A_0 = a_0, \Theta = 1, \Omega = 1) &\text{(52a)}\\ &\quad\geq H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, \Theta = 1) \\ &\qquad - \textstyle\sum_{l\in\mathcal{L}} |\mathcal{H}_{X_l^N|X_{1:l-1}^N \check{X}_{\mathcal{L}}^N}| - \sqrt{NB} &\text{(52b)}\\ &\quad= H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, \Theta = 1) \\ &\qquad - \textstyle\sum_{l\in\mathcal{L}} (BH(X_l^N|X_{1:l-1}^N \check{X}_{\mathcal{L}}^N) + o(B)) - \sqrt{NB} &\text{(52c)}\\ &\quad= H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, \Theta = 1) \\ &\qquad - BH(X_{\mathcal{L}}^N|\check{X}_{\mathcal{L}}^N) - o(NB) &\text{(52d)}\\ &\quad\geq H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B = a_{\mathcal{L}}^B, \Theta = 1) \\ &\qquad - o(NB) &\text{(52e)}\\ &\quad\geq B(1-\epsilon)H(X_{\mathcal{S}}^N|A_{\mathcal{L}}) \\ &\qquad + \log(1 - \delta_\epsilon^1(N, B)) - o(NB) &\text{(52f)}\\ &\quad\geq (1-\epsilon)(NB \cdot I(X_{\mathcal{S}}; X_0) - o(N) \cdot B) \\ &\qquad + \log(1 - \delta_\epsilon^1(N, B)) - o(NB) &\text{(52g)}\\ &\quad= (1-\epsilon) \cdot NB \cdot I(X_{\mathcal{S}}; X_0) + \delta_\epsilon^2(N, B), &\text{(52h)}\end{aligned}$$

where (52b) holds by definition of Ω, (52c) holds by Lemma 1, (52e) holds by Fano's inequality because similar to the analysis in Section IV-B.1, $\mathbb{P}[\check{X}_{\mathcal{L}}^N \neq X_{\mathcal{L}}^N] \xrightarrow{N\to\infty} 0$, (52f) holds by

Lemma 3 applied to the DMS $(\mathcal{X}_{\mathcal{S}}^N \times \mathcal{A}_{\mathcal{L}}, p_{X_{\mathcal{S}}^N A_{\mathcal{L}}})$, (52g) holds by Lemma 4, and in (52h) we have defined

$$\delta_\epsilon^2(N,B) \triangleq -o(N)\cdot B(1-\epsilon)+\log(1-\delta_\epsilon^1(N,B))-o(NB). \quad (53)$$

Remark 9. *Unfortunately, unlike the two-user secret-key generation setting considered in [51], it is not possible to use [51, Lemma 10] to obtain a tight lower bound on $H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B=a_{\mathcal{L}}^B)$. We use Lemmas 3, 4 to circumvent this issue.*

We will then need the following version of the leftover hash lemma [49], [53]–[55].

Lemma 5 (Leftover Hash Lemma for Concatenated Hash Functions)**.** *Let $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$ and Z be random variables distributed according to $p_{X_{\mathcal{L}}Z}$ over $\mathcal{X}_{\mathcal{L}}\times\mathcal{Z}$. For $l\in\mathcal{L}$, let $F_l : \{0,1\}^{n_l}\to\{0,1\}^{r_l}$, be uniformly chosen in a family $\mathcal{F}_l$ of two-universal hash functions. Define $s_{\mathcal{L}} \triangleq \prod_{l\in\mathcal{L}} s_l$, where $s_l \triangleq |\mathcal{F}_l|$, $l\in\mathcal{L}$, and for any $\mathcal{S}\subseteq\mathcal{L}$, define $r_{\mathcal{S}} \triangleq \sum_{i\in\mathcal{S}} r_i$. Define also $F_{\mathcal{L}} \triangleq (F_l)_{l\in\mathcal{L}}$ and*

$$F_{\mathcal{L}}(X_{\mathcal{L}}) \triangleq (F_1(X_1)||F_2(X_2)||\ldots||F_L(X_L)), \quad (54)$$

where || denotes concatenation. Then, for any $z\in\mathcal{Z}$, we have

$$\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}|Z=z}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}) \le \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-H_\infty(X_{\mathcal{S}}|Z=z)}}, \quad (55)$$

where $p_{U_{\mathcal{K}}}$ and $p_{U_{\mathcal{F}}}$ are the uniform distribution over $[\![1,2^{r_{\mathcal{L}}}]\!]$, and $[\![1,s_{\mathcal{L}}]\!]$, respectively.

A consequence of (55) *is*

$$\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}},Z}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_Z) \le \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-H_\infty(X_{\mathcal{S}}|Z)}}, \quad (56)$$

where we have used the average conditional min-entropy of X given Z defined as in [54] by

$$H_\infty(X|Z) \triangleq -\log(\mathbb{E}_Z \max_x p_{X|Z}(x|Z)). \quad (57)$$

Proof. See Appendix B. ∎

Combining (52h) and Lemma 5, we are able to determine the admissible values for r_l, $l\in\mathcal{L}$, as follows.

$$\begin{aligned}
&\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{NB})F_{\mathcal{L}}A_{\mathcal{L}}^BA_0}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_{A_{\mathcal{L}}^BA_0})\\
&\le \mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{NB})F_{\mathcal{L}}A_{\mathcal{L}}^BA_0\Theta\Omega}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_{A_{\mathcal{L}}^BA_0\Theta\Omega}) && (58a)\\
&= \mathbb{E}\left[\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{NB})F_{\mathcal{L}}A_{\mathcal{L}}^BA_0|\Theta\Omega}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_{A_{\mathcal{L}}^BA_0|\Theta\Omega})\right] && (58b)\\
&\le 2\mathbb{P}[\Theta=0\vee\Omega=0]+\\
&\quad \mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{NB})F_{\mathcal{L}}A_{\mathcal{L}}^BA_0|\Theta=1,\Omega=1}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_{A_{\mathcal{L}}^BA_0|\Theta=1,\Omega=1}) && (58c)\\
&\le 2\mathbb{P}[\Theta=0\vee\Omega=0]\\
&\quad +\mathbb{E}\left[\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{NB})F_{\mathcal{L}}|A_{\mathcal{L}}^BA_0\Theta=1,\Omega=1}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}})\right] && (58d)\\
&\le 2\mathbb{P}[\Theta=0\vee\Omega=0]\\
&\quad +\mathbb{E}\sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-H_\infty(X_{\mathcal{S}}^{NB}|A_{\mathcal{L}}^B=a_{\mathcal{L}}^B,A_0=a_0,\Theta=1,\Omega=1)}} && (58e)\\
&\le 2\mathbb{P}[\Theta=0\vee\Omega=0]\\
&\quad +\mathbb{E}\sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-(1-\epsilon)\cdot NB\cdot I(X_{\mathcal{S}};X_0)-\delta_\epsilon^2(N,B)}} && (58f)\\
&= 2\mathbb{P}[\Theta=0\vee\Omega=0]\\
&\quad +\sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-(1-\epsilon)\cdot NB\cdot I(X_{\mathcal{S}};X_0)-\delta_\epsilon^2(N,B)}} && (58g)\\
&\le 2\delta_\epsilon^0(N,B)+2\cdot 2^{-\sqrt{NB}}\\
&\quad +\sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-(1-\epsilon)\cdot NB\cdot I(X_{\mathcal{S}};X_0)-\delta_\epsilon^2(N,B)}}, && (58h)
\end{aligned}$$

where (58a) holds by marginalization over Θ and the triangle inequality, in (58b) the expectation is with respect to $p_{\Theta,\Omega}$, (58c) holds because $\mathbb{V}(\cdot,\cdot)$ is upper bounded by 2, in (58d) the expectation is with respect to $p_{A_{\mathcal{L}}^BA_0|\Theta=1,\Omega=1}$, (58e) holds by Lemma 5 with the substitutions $z\leftarrow(a_{\mathcal{L}}^B,a_0,\Theta=1,\Omega=1)$ and $X_{\mathcal{L}}\leftarrow X_{\mathcal{L}}^{NB}$ and the expectation is with respect to $p_{A_{\mathcal{L}}^BA_0|\Theta=1,\Omega=1}$, (58f) holds by (52h) and the expectation is with respect to $p_{A_{\mathcal{L}}^BA_0|\Theta=1,\Omega=1}$, (58h) holds by the union bound, Lemma 3, the definition of Ω and [51, Lemma 10].

Finally, we conclude that Theorem 3 holds by Remark 1 and (58h).

V. Non-Degraded Source Case When $L=2$

In this section, we consider the setting described in Section II when $L=2$, public communication is restricted to be one-way from the agents to the base station, and when (1) does not hold. Similar to Section II, the value function v^* of this game is defined as

$$v^*: 2^{\mathcal{L}}\to\mathbb{R}^+, \mathcal{S}\mapsto \max_{a_{\mathcal{S}}\in\mathfrak{S}(\mathcal{S})}\ \min_{a_{\mathcal{L}\setminus\mathcal{S}}\in\mathfrak{S}(\mathcal{L}\setminus\mathcal{S})}\ \sum_{i\in\mathcal{S}}\pi_i(a_{\mathcal{S}},a_{\mathcal{L}\setminus\mathcal{S}}) \quad (59)$$

such that for any $\mathcal{S}\subseteq\mathcal{L}$, $v(\mathcal{S})$ corresponds to the maximal secret-key sum-rate achievable by coalition $\mathcal{S}$ when *no specific strategy is assumed* for the agents in $\mathcal{L}\setminus\mathcal{S}$.

Next, we characterize the value function v^* by providing a counterpart to Theorem 1.

Proposition 5. *We have*

$$v^*(\{1\}) = \max_{V_1-U_1-X_1-(X_0,X_2)} [I(U_1;X_0|V_1)-I(U_1;X_2|V_1)]^+, \quad (60a)$$

$$v^*(\{2\}) = \max_{V_2-U_2-X_2-(X_0,X_1)} [I(U_2;X_0|V_2)-I(U_2;X_1|V_2)]^+, \quad (60b)$$

$$v^*(\{1,2\}) = I(X_1X_2;X_0), \quad (60c)$$

where $[x]^+\triangleq\max(x,0)$ for any $x\in\mathbb{R}$.

Proof. $v^*(\{1\})$ and $v^*(\{2\})$ are obtained from [15]. $v^*(\{1,2\})$ is obtained from [21], [23]. ∎

Remark 10. *If $L>2$, then $v^*(\mathcal{L})=I(X_{\mathcal{L}};X_0)$ by [23], and for any $l\in\mathcal{L}$, $v^*(\{l\})$ can be obtained from [15].*

However, for any $\mathcal{S} \subset \mathcal{L}$ such that $|\mathcal{S}| > 1$, a closed form expression for $v^*(\mathcal{S})$ is unknown.

Remark 11. *In the case of two-way communication between the base station and the agents, $v^*(\{1,2\})$ has the same expression. However, in this case, no closed-form expression is known for $v^*(\{1\})$ or $v^*(\{2\})$, which both correspond to a secret-key capacity between two parties in presence of an eavesdropper [15], [16].*

Property 2. *The game $(\mathcal{L}, v^*)$ defined in (59) is superadditive.*

Proof. Any two disjoint coalitions $\mathcal{S}, \mathcal{T} \subseteq \mathcal{L}$, $\mathcal{S} \cap \mathcal{T} = \emptyset$, obtain secret-key sum-rate capacities that cannot add up to a quantity strictly larger than the secret-key sum-rate capacity of the coalition $\mathcal{S} \cup \mathcal{T}$. Note indeed that the reliability, secrecy, and uniformity constraints for coalitions $\mathcal{S}$ and $\mathcal{T}$ imply a reliability, secrecy, and uniformity constraint for the coalition $\mathcal{S} \cup \mathcal{T}$. Indeed, we have

$$\mathbb{P}[\widehat{K}_{\mathcal{S}\cup\mathcal{T}} \neq K_{\mathcal{S}\cup\mathcal{T}}] \leq \mathbb{P}[\widehat{K}_{\mathcal{S}} \neq K_{\mathcal{S}}] + \mathbb{P}[\widehat{K}_{\mathcal{T}} \neq K_{\mathcal{T}}]. \quad (61)$$

Next, we have

$$\begin{aligned} I\left(K_{\mathcal{S}\cup\mathcal{T}}; A_{\mathcal{S}\cup\mathcal{T}} X^N_{(\mathcal{S}\cup\mathcal{T})^c}\right) &= I\left(K_{\mathcal{S}}; A_{\mathcal{S}} A_{\mathcal{T}} X^N_{(\mathcal{S}\cup\mathcal{T})^c}\right) \\ &\quad + I\left(K_{\mathcal{T}}; A_{\mathcal{S}} A_{\mathcal{T}} X^N_{(\mathcal{S}\cup\mathcal{T})^c} | K_{\mathcal{S}}\right) \quad (62a) \\ &\leq I\left(K_{\mathcal{S}}; A_{\mathcal{S}} A_{\mathcal{T}} X^N_{(\mathcal{S}\cup\mathcal{T})^c}\right) \\ &\quad + I\left(K_{\mathcal{T}}; A_{\mathcal{T}} A_{\mathcal{S}} X^N_{(\mathcal{S}\cup\mathcal{T})^c} K_{\mathcal{S}}\right) \quad (62b) \\ &\leq I\left(K_{\mathcal{S}}; A_{\mathcal{S}} X^N_{\mathcal{S}^c}\right) + I\left(K_{\mathcal{T}}; A_{\mathcal{T}} X^N_{\mathcal{T}^c}\right), \quad (62c) \end{aligned}$$

where in (62a) we decompose $A_{\mathcal{S}\cup\mathcal{T}}$ in $A_{\mathcal{S}}$ and $A_{\mathcal{T}}$, the public communication emitted by the agents in $\mathcal{S}$ and $\mathcal{T}$, respectively, (62b) holds by positivity of the mutual information and the chain rule, (62c) holds because $(A_{\mathcal{S}}, A_{\mathcal{T}}, X^N_{(\mathcal{S}\cup\mathcal{T})^c})$ is a function of $(A_{\mathcal{S}}, X^N_{\mathcal{S}^c})$ and $(A_{\mathcal{T}}, A_{\mathcal{S}}, X^N_{(\mathcal{S}\cup\mathcal{T})^c}, K_{\mathcal{S}})$ is a function of $(A_{\mathcal{T}}, X^N_{\mathcal{T}^c})$.

Finally, we have

$$\begin{aligned} \log|\mathcal{K}_{\mathcal{S}\cup\mathcal{T}}| - H(K_{\mathcal{S}\cup\mathcal{T}}) &= \log|\mathcal{K}_{\mathcal{S}}| - H(K_{\mathcal{S}}) + \log|\mathcal{K}_{\mathcal{T}}| - H(K_{\mathcal{T}}) \\ &\quad + I(K_{\mathcal{S}}; K_{\mathcal{T}}) \quad (63a) \\ &\leq \log|\mathcal{K}_{\mathcal{S}}| - H(K_{\mathcal{S}}) + \log|\mathcal{K}_{\mathcal{T}}| - H(K_{\mathcal{T}}) \\ &\quad + I\left(K_{\mathcal{S}}; X^N_{\mathcal{S}^c}\right). \quad (63b) \end{aligned}$$

■

Note that the proof of Property 2 is valid for any L, not only $L = 2$. Hence, we can define the core of the game as in Definition 6. From Property 2, we immediately obtain the following property since superadditivity implies convexity for $L = 2$.

Property 3. *The game $(\mathcal{L}, v^*)$ defined in (59) is convex.*

Next, from [38] and Property 3, we deduce the following corollary.

Corollary 3. *The game $(\mathcal{L}, v^*)$ defined in (59) has a non-empty core.*

As an example of solution concept, we characterize the Shapley value discussed in Section III-B for $(\mathcal{L}, v^*)$.

Example 3. *The Shapley value of the game $(\mathcal{L}, v^*)$ defined in (59) is given for $i \in \{1,2\}$ and $\bar{i} \triangleq 3 - i$ by*

$$\begin{aligned} R_i^{\text{Shap}} &= \frac{1}{2} I(X_1 X_2; X_0) \\ &\quad + \frac{1}{2} \max_{V_i - U_i - X_i - (X_0, X_{\bar{i}})} \left[I(U_i; X_0|V_i) - I(U_i; X_{\bar{i}}|V_i)\right]^+ \\ &\quad - \frac{1}{2} \max_{V_{\bar{i}} - U_{\bar{i}} - X_{\bar{i}} - (X_0, X_i)} \left[I(U_{\bar{i}}; X_0|V_{\bar{i}}) - I(U_{\bar{i}}; X_i|V_{\bar{i}})\right]^+. \end{aligned} \quad (64)$$

VI. Extension to Multiple Levels of Security Clearance

We now consider that multiple levels of security clearance exist in our model. Specifically, each agent has a pre-defined security clearance level, and it is required that keys generated by agents at a given level must be kept secret from the agents at a strictly superior level. Note that this setting is related to the problem of simultaneously generating private and secret keys [56], [57].

A. Model

Let $Q \in \mathbb{N}^*$ and define $\mathcal{Q} \triangleq [\![1, Q]\!]$. For $q \in \mathcal{Q}$, let $L_q \in \mathbb{N}^*$ and let $\mathcal{L}_q$ be a set of L_q agents. In the following, we consider Q sets $(\mathcal{L}_q)_{q\in\mathcal{Q}}$ of agents and one base station depicted in Figure 3. We also use the notation $\mathcal{L}_{\mathcal{Q}} \triangleq \bigcup_{q\in\mathcal{Q}} \mathcal{L}_q$ to denote all the agents in the Q sets.

1) Definition of the Source Model: Define $\mathcal{X}_{\mathcal{L}_{\mathcal{Q}}}$ as the Cartesian product of $\sum_{q=1}^{Q} L_q$ finite alphabets $\mathcal{X}_l$, $l \in \mathcal{L}_{\mathcal{Q}}$. Consider a discrete memoryless source (DMS) $\left(\mathcal{X}_{\mathcal{L}_{\mathcal{Q}}} \times \mathcal{X}_0, p_{X_{\mathcal{L}_{\mathcal{Q}}} X_0}\right)$, where $\mathcal{X}_0$ is a finite alphabet and $X_{\mathcal{L}_{\mathcal{Q}}} \triangleq (X_l)_{l\in\mathcal{L}_{\mathcal{Q}}}$. For $l \in \mathcal{L}_{\mathcal{Q}}$, Agent l observes the component X_l of the DMS, and the base station observes the component X_0. The source is assumed to follow the following Markov chain: for any $\mathcal{S}, \mathcal{T} \subset \mathcal{L}_{\mathcal{Q}}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$,

$$X_{\mathcal{S}} - X_0 - X_{\mathcal{T}}. \quad (65)$$

The source's statistics are assumed known to all parties, and communication is allowed over an authenticated noiseless public channel.

2) Description of the Objectives for the Agents: The goal of Agent $l \in \mathcal{L}_{\mathcal{Q}}$ is to generate an individual secret-key with the base station. The index $q \in \mathcal{Q}$ is meant to describe different sets of agents that do not have the same security constraints. In particular, we require that for any $q \in \mathcal{Q}$, the keys generated by the agents in $\mathcal{L}_q$ are secret, in an information-theoretic sense, from the agents in $\bigcup_{i\in[\![q+1,Q]\!]} \mathcal{L}_i$ but need not to be secret from the agents in $\bigcup_{i\in[\![1,q]\!]} \mathcal{L}_i$. One can interpret it in terms of levels of security clearance, where $\mathcal{L}_q$, $q \in \mathcal{Q}$, represents a set of agents that share the same level of security clearance, and for $q' < q$, $\mathcal{L}_{q'}$, represents another set of agents with a higher security clearance than $\mathcal{L}_q$.

Remark 12. *We require information-theoretic security across security clearance levels, meaning that the agents in $\mathcal{L}_q$,*

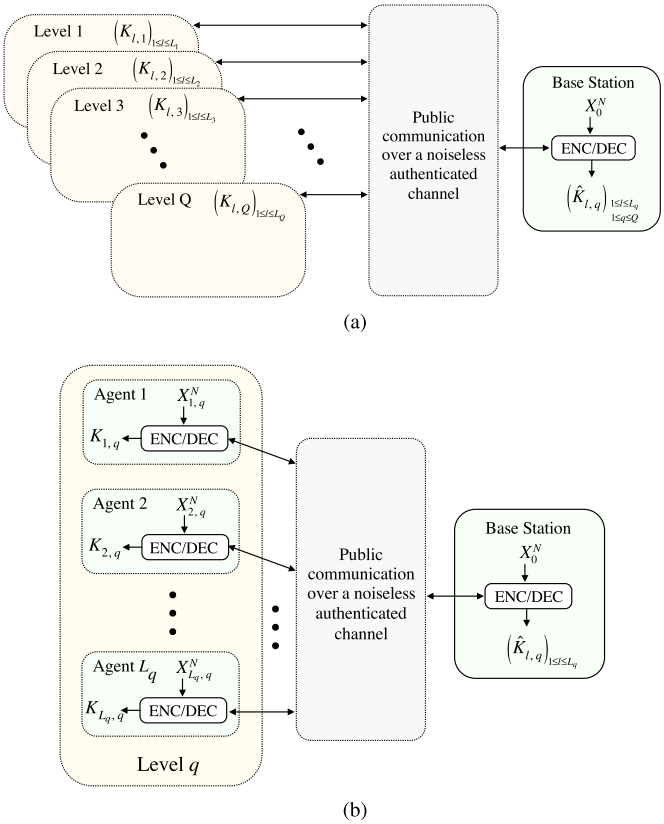

Fig. 3. Many-to-one secret-key generation setting with multiple levels of security clearance. (b) provides details of the setting described in (a) at a given level $q \in \mathcal{Q}$. (a) Overview of the Q sets of agents. (b) Representation of the setting at level $q \in \mathcal{Q}$.

$q \in \mathcal{Q}$, must keep their keys secret from all agents in $(\mathcal{L}_i)_{i\in[\![q+1,Q]\!]}$, for any communication strategy the latter group of agents may decide to adopt. Consequently, we discard the possibility for the agents in $(\mathcal{L}_i)_{i\in[\![q+1,Q]\!]}$ and $\mathcal{L}_q$ to agree on participating in a common secret key generation scheme. Not doing so might imply that the agents in $(\mathcal{L}_i)_{i\in[\![q+1,Q]\!]}$ follow a pre-determined communication strategy, which would contradict the information-theoretic security requirement.

To extend Sections III and IV to this setting with multiple clearance levels, we first consider the following auxiliary setting. We consider the setting described in Definitions 1 and 2 when an eavesdropper that observes the public communication is also in possession of correlated source observations. The auxiliary setting is presented in Section VI-B. Next, to address the multiple levels of security constraints, it is sufficient to apply the results of Section VI-B to each security clearance level $q \in \mathcal{Q}$ by considering for the agents in $\mathcal{L}_q$, the DMS $\left(\mathcal{X}_{\mathcal{L}_q} \times \mathcal{X}_0 \times \mathcal{X}_{\mathcal{L}_{q+1:Q}}\right)$, where $\mathcal{L}_{q+1:Q} \triangleq \bigcup_{i\in[\![q+1,Q]\!]} \mathcal{L}_i$, with the assumption that an eavesdropper observes the components $X_{\mathcal{L}_{q+1:Q}}$ of the DMS.

B. Auxiliary Setting

Consider a DMS $\left(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0 \times \mathcal{Z}, p_{X_{\mathcal{L}}X_0Z}\right)$, where Z is an additional, compared to the source model considered in Section II-A, component of the source observed by an eavesdropper. The source is assumed to follow the following Markov chain: for any $\mathcal{S}, \mathcal{T} \subseteq \mathcal{L}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$,

$$X_{\mathcal{S}} - X_0 - (X_{\mathcal{T}} Z). \tag{66}$$

We then consider the same Definitions 3, 4 as in Section II-B, where the secrecy constraint (6) of Definition 4 becomes for a coalition $\mathcal{S} \subset \mathcal{L}$

$$\lim_{N\to\infty} I(K_{\mathcal{S}}; A_{\mathcal{S}} X^N_{\mathcal{S}^c} Z^N) = 0. \tag{67}$$

Next, we define our object of study as the secret-key generation problem we have just defined when $\mathcal{S} = \mathcal{L}$ and when the users are selfish. Similar to Section II-C, we wish to understand whether the agents can find a consensus about the coalitions to form, and how the secret-sum rate of each coalition should be allocated among its agents. Following Section II-C, we cast the problem as a coalitional game $(\mathcal{L}, v^Z)$ where the value of coalition $\mathcal{S} \subseteq \mathcal{L}$ is defined as the *maximal secret-key sum-rate* that coalition $\mathcal{S}$ can obtain *regardless of the strategies adopted by the member of $\mathcal{S}^c$*.

Similar to the proof of Theorem 1 by using Corollary 5, stated below, in place of Corollary 2, one can show the following characterization of the value function v^Z.

$$v^Z : 2^{\mathcal{L}} \to \mathbb{R}^+, \mathcal{S} \mapsto I(X_{\mathcal{S}}; X_0 | X_{\mathcal{S}^c} Z). \tag{68}$$

Similar to Proposition 1, one can show that the game $(\mathcal{L}, v^Z)$ is convex, and similar to Theorem 2 that its core is given by

$$\mathcal{C}(v^Z) = \left\{ (R_l)_{l\in\mathcal{L}} : \forall \mathcal{S} \subseteq \mathcal{L}, \right. \\ \left. I(X_{\mathcal{S}}; X_0 | X_{\mathcal{S}^c} Z) \le \sum_{i\in\mathcal{S}} R_i \le I(X_{\mathcal{S}}; X_0 | Z) \right\}. \tag{69}$$

Moreover, similar to Proposition 3, the Shapley value is in $\mathcal{C}(v^Z)$ and given by

$$\forall l \in \mathcal{L}, R_l^{\text{Shap}} \\ = I(X_l; X_0 | Z) - \frac{1}{L} \sum_{\mathcal{S}\subseteq\mathcal{L}\setminus\{l\}} \binom{L-1}{|\mathcal{S}|}^{-1} I(X_l; X_{\mathcal{S}} | Z). \tag{70}$$

Finally, it is possible to achieve any point of the core $\mathcal{C}(v^Z)$ with an explicit coding scheme, by deducing from Theorem 4 the following corollary.

Corollary 4. *Consider a DMS $\left(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0 \times \mathcal{Z}, p_{X_{\mathcal{L}}X_0Z}\right)$ such that $\forall l \in \mathcal{L}, |\mathcal{X}_l| = 2$ and the Markov chain* (66) *holds. Any rate tuple in*

$$\mathcal{R}^Z_{\mathcal{S}} \triangleq \\ \left\{ (R_l)_{l\in\mathcal{S}} : 0 \le \sum_{i\in\mathcal{T}} R_i \le I(X_{\mathcal{T}}; X_0 | X_{\mathcal{S}^c} Z), \forall \mathcal{T} \subseteq \mathcal{S} \right\} \tag{71}$$

is achievable by the coalition of agents $\mathcal{S} \subseteq \mathcal{L}$. Moreover,

$$\mathcal{C}(v^Z) \subset \mathcal{R}^Z_{\mathcal{L}}. \tag{72}$$

Finally, from Corollary 4, we deduce, similar to the proof of Corollary 2 the following corollary, which allows us to establish (68).

Corollary 5. *Corollary 4 implies that for any $\mathcal{S} \subseteq \mathcal{L}$, the secret-key sum rate $I(X_{\mathcal{S}}; X_0|X_{\mathcal{S}^c}Z)$ is achievable by Coalition $\mathcal{S}$.*

VII. Concluding Remarks

We have studied a pairwise secret-key generation source model between multiple agents and a base station. Although cooperation among agents can increase their individual key length, it can, at the same time, lead to conflict of interests between agents. We have proposed an integrated information-theoretic and game-theoretic formulation of the problem. Specifically, we have cast the problem as a coalitional game in which the value function is determined under information-theoretic guarantees, i.e., the value associated with a coalition is computed with no restrictions on the strategies that the users outside the coalition could adopt. We have shown that the game associated with our problem is convex, and characterized its core, which is interpreted as a converse for our setting. We have shown that the grand coalition is in the best interest of all agents and stable, in the sense that any coalition of agents has a disincentive to leave the grand coalition. We have also characterized the Shapley value, and used it as a possible solution concept to ensure fairness among agents. Finally, we have proposed an explicit coding scheme relying on polar codes for source coding and hash functions to achieve *any point of the core*, including the Shapley value and the nucleolus.

The framework is general and could be applied to other security problems involving a tension between cooperation and self-interest. The challenge is in characterizing a value function for this framework. For instance, in our setting, being able to determine the value function in the non-degraded setting when $L > 2$ remains an open problem, and is, unfortunately, at least as difficult as determining the secret-key capacity for the two-user secret generation model of [16].

Appendix A
Proof of Lemma 4

Let $\mathcal{S} \subseteq \mathcal{L}$. We have

$$
\begin{aligned}
&H(X_{\mathcal{S}}^N|A_{\mathcal{L}}) \\
&\quad = H(X_{\mathcal{S}}^N A_{\mathcal{S}} A_{\mathcal{L}\setminus\mathcal{S}}) - H(A_{\mathcal{L}}) && (73a)\\
&\quad = H(X_{\mathcal{S}}^N A_{\mathcal{L}\setminus\mathcal{S}}) - H(A_{\mathcal{L}}) && (73b)\\
&\quad = H(X_{\mathcal{S}}^N) + H(A_{\mathcal{L}\setminus\mathcal{S}}|X_{\mathcal{S}}^N) - H(A_{\mathcal{L}}) && (73c)\\
&\quad \geq H(X_{\mathcal{S}}^N) + H(A_{\mathcal{L}\setminus\mathcal{S}}|X_{\mathcal{S}}^N) - \log|\mathcal{A}_{\mathcal{L}}| && (73d)\\
&\quad = H(X_{\mathcal{S}}^N) + H(A_{\mathcal{L}\setminus\mathcal{S}}|X_{\mathcal{S}}^N) - NH(X_{\mathcal{L}}|X_0) - o(N) && (73e)\\
&\quad = NI(X_{\mathcal{S}}; X_0) + H(A_{\mathcal{L}\setminus\mathcal{S}}|X_{\mathcal{S}}^N) \\
&\qquad -NH(X_{\mathcal{L}\setminus\mathcal{S}}|X_0X_{\mathcal{S}}) - o(N), && (73f)
\end{aligned}
$$

where (73b) holds because $A_{\mathcal{S}}$ is a function of $X_{\mathcal{S}}^N$, (73e) holds because

$$
\begin{aligned}
\log|\mathcal{A}_{\mathcal{L}}| &= \sum_{l\in\mathcal{L}} \log|\mathcal{A}_l| && (74a)\\
&= \sum_{l\in\mathcal{L}} |\mathcal{H}_{X_l|X_0X_{1:l-1}}| && (74b)\\
&= \sum_{l\in\mathcal{L}} NH(X_l|X_0X_{1:l-1}) + o(N) && (74c)\\
&= NH(X_{\mathcal{L}}|X_0) + o(N), && (74d)
\end{aligned}
$$

where (74c) holds by [26], [58], [59, Theorem 3.5].

We lower-bound the second term in the right-hand side of (73f) as follows

$$
\begin{aligned}
&H(A_{\mathcal{L}\setminus\mathcal{S}}|X_{\mathcal{S}}^N) \\
&\quad \geq \sum_{j\in\mathcal{L}\setminus\mathcal{S}} H(A_j|A_{1:j-1}X_{\mathcal{S}}^N) && (75a)\\
&\quad \geq \sum_{j\in\mathcal{L}\setminus\mathcal{S}} H(A_j|X_0^N X_{1:j-1}^N X_{\mathcal{S}}^N) && (75b)\\
&\quad = \sum_{j\in\mathcal{L}\setminus\mathcal{S}} H(U_j^N[\mathcal{H}_{X_j|X_0X_{1:j-1}}]|X_0^N X_{1:j-1}^N X_{\mathcal{S}}^N) && (75c)\\
&\quad \geq \sum_{j\in\mathcal{L}\setminus\mathcal{S}} H(U_j^N[\mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}]|X_0^N X_{1:j-1}^N X_{\mathcal{S}}^N) && (75d)\\
&\quad \geq \sum_{j\in\mathcal{L}\setminus\mathcal{S}} \sum_{i\in \mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}} H((U_j)_i|(U_j)^{i-1}X_0^N X_{1:j-1}^N X_{\mathcal{S}}^N) && (75e)\\
&\quad \geq \sum_{j\in\mathcal{L}\setminus\mathcal{S}} \sum_{i\in \mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}} (1-\delta_N) && (75f)\\
&\quad = \sum_{j\in\mathcal{L}\setminus\mathcal{S}} |\mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}|(1-\delta_N) && (75g)\\
&\quad = \sum_{j\in\mathcal{L}\setminus\mathcal{S}} NH(X_j|X_0X_{1:j-1}X_{\mathcal{S}}) - o(N) && (75h)\\
&\quad = \sum_{j\in\mathcal{L}\setminus\mathcal{S}} NH(X_j|X_0X_{[\![1:j-1]\!]\cap\mathcal{L}\setminus\mathcal{S}}X_{\mathcal{S}}) - o(N) && (75i)\\
&\quad = NH(X_{\mathcal{L}\setminus\mathcal{S}}|X_0X_{\mathcal{S}}) - o(N), && (75j)
\end{aligned}
$$

where (75a) and (75e) hold by the chain rule and because conditioning reduces entropy, (75d) holds because $\mathcal{H}_{X_j|X_0X_{1:j-1}} \supset \mathcal{H}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}} \supset \mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}$, (75f) holds by definition of $\mathcal{V}_{X_j|X_0X_{1:j-1}X_{\mathcal{S}}}$, (75h) holds by Lemma 2, (75j) holds by the chain rule.

Finally, combining (73f) and (75j) proves Lemma 4.

Appendix B
Proof of Lemma 5

We first prove the result when $Z = \emptyset$. For $X_{\mathcal{L}}$, $X'_{\mathcal{L}}$, $F_{\mathcal{L}}$, $F'_{\mathcal{L}}$ independent, we compute the following collision probability

$$
\begin{aligned}
&\mathbb{P}[(F_{\mathcal{L}}(X_{\mathcal{L}}), F_{\mathcal{L}}) = (F'_{\mathcal{L}}(X'_{\mathcal{L}}), F'_{\mathcal{L}})] \\
&\quad = \mathbb{P}[F_{\mathcal{L}} = F'_{\mathcal{L}}]\mathbb{P}[F_{\mathcal{L}}(X_{\mathcal{L}}) = F_{\mathcal{L}}(X'_{\mathcal{L}})] && (76a)\\
&\quad = \prod_{l\in\mathcal{L}} \mathbb{P}[F_l = F'_l]\mathbb{P}[F_{\mathcal{L}}(X_{\mathcal{L}}) = F_{\mathcal{L}}(X'_{\mathcal{L}})] && (76b)\\
&\quad = s_{\mathcal{L}}^{-1} \sum_{x_{\mathcal{L}}, x'_{\mathcal{L}}} \mathbb{P}[F_{\mathcal{L}}(x_{\mathcal{L}}) = F_{\mathcal{L}}(x'_{\mathcal{L}})]\mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}, X'_{\mathcal{L}} = x'_{\mathcal{L}}] && (76c)\\
&\quad = s_{\mathcal{L}}^{-1} \sum_{x_{\mathcal{L}}, x'_{\mathcal{L}}} \mathbb{P}[F_{\mathcal{L}}(x_{\mathcal{L}}) = F_{\mathcal{L}}(x'_{\mathcal{L}})]\mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}]\mathbb{P}[X'_{\mathcal{L}} = x'_{\mathcal{L}}] && (76d)
\end{aligned}
$$

$$= s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}} \\ \text{s.t.} x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathbb{P}[F_{\mathcal{L}}(x_{\mathcal{L}}) = F_{\mathcal{L}}(x'_{\mathcal{L}})] \times \mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}]\mathbb{P}[X'_{\mathcal{L}} = x'_{\mathcal{L}}] \quad (76e)$$

$$= s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}} \\ \text{s.t.} x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \prod_{l\in\mathcal{L}} \mathbb{P}[F_l(x_l) = F_l(x'_l)]\mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}] \times \mathbb{P}[X'_{\mathcal{S}} = x'_{\mathcal{S}}, X'_{\mathcal{S}^c} = x_{\mathcal{S}^c}] \quad (76f)$$

$$\leq s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}} \\ \text{s.t.} x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} 2^{-r_{\mathcal{S}}} \mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}] \times \mathbb{P}[X'_{\mathcal{S}} = x'_{\mathcal{S}}, X'_{\mathcal{S}^c} = x_{\mathcal{S}^c}] \quad (76g)$$

$$\leq s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}} 2^{-r_{\mathcal{S}}} \mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}]\mathbb{P}[X'_{\mathcal{S}^c} = x_{\mathcal{S}^c}] \quad (76h)$$

$$\leq s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}} 2^{-r_{\mathcal{S}}} \mathbb{P}[X_{\mathcal{L}} = x_{\mathcal{L}}] 2^{-H_\infty(p_{X_{\mathcal{S}^c}})} \quad (76i)$$

$$= s_{\mathcal{L}}^{-1} \sum_{\mathcal{S}\subseteq\mathcal{L}} 2^{-r_{\mathcal{S}} - H_\infty(p_{X_{\mathcal{S}^c}})}, \quad (76j)$$

where (76g) holds by the two-universality of the F_l's, $l \in \mathcal{L}$, (76h) holds by marginalization over $X'_{\mathcal{S}}$, (76i) holds by definition of the min-entropy.

Then, viewing $\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}})$ as a scalar product between $(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}} - p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}})$ and its sign, by Cauchy-Schwarz inequality, we have

$$\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}})^2 \leq s_{\mathcal{L}} 2^{r_{\mathcal{L}}} \sum_{m_{\mathcal{L}}, f_{\mathcal{L}}} \left[p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}}(m_{\mathcal{L}}, f_{\mathcal{L}}) - \frac{1}{s_{\mathcal{L}} 2^{r_{\mathcal{L}}}} \right]^2 \quad (77a)$$

$$= s_{\mathcal{L}} 2^{r_{\mathcal{L}}} \left[\sum_{m_{\mathcal{L}}, f_{\mathcal{L}}} p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}}}(m_{\mathcal{L}}, f_{\mathcal{L}})^2 \right] - 1 \quad (77b)$$

$$= s_{\mathcal{L}} 2^{r_{\mathcal{L}}} \mathbb{P}[(F_{\mathcal{L}}(X_{\mathcal{L}}), F_{\mathcal{L}}) = (F'_{\mathcal{L}}(X'_{\mathcal{L}}), F'_{\mathcal{L}})] - 1 \quad (77c)$$

$$\leq 2^{r_{\mathcal{L}}} \sum_{\mathcal{S}\subseteq\mathcal{L}} 2^{-r_{\mathcal{S}} - H_\infty(p_{X_{\mathcal{S}^c}})} - 1 \quad (77d)$$

$$= \sum_{\mathcal{S}\subsetneq\mathcal{L}} 2^{r_{\mathcal{S}^c} - H_\infty(p_{X_{\mathcal{S}^c}})} \quad (77e)$$

$$= \sum_{\substack{\mathcal{S}\subseteq\mathcal{L} \\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}} - H_\infty(p_{X_{\mathcal{S}}})}, \quad (77f)$$

where (77d) holds by (76j).

We now introduce the random variable Z correlated to $X_{\mathcal{L}}$ and proceed as in [54]. Let $z \in \mathcal{Z}$ and $X_{\mathcal{L}}^{(z)}$ be defined by $p_{X_{\mathcal{L}}^{(z)}} = p_{X_{\mathcal{L}}|Z=z}$. We have

$$\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}),F_{\mathcal{L}},Z}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}p_Z) = \mathbb{E}_Z \left[\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}^{(z)}),F_{\mathcal{L}}}, p_{U_{\mathcal{K}}}p_{U_{\mathcal{F}}}) \right] \quad (78a)$$

$$\leq \mathbb{E}_Z \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L} \\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}} - H_\infty(X_{\mathcal{S}}|Z=z)}} \quad (78b)$$

$$\leq \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L} \\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}} - H_\infty(X_{\mathcal{S}}|Z)}}, \quad (78c)$$

where (78b) holds by (77f), (78c) holds by Jensen's inequality and since, by definition, $\mathbb{E}_Z[2^{-H_\infty(X_{\mathcal{S}}|Z=z)}] = 2^{-H_\infty(X_{\mathcal{S}}|Z)}$, $\mathcal{S} \subseteq \mathcal{L}$.

Appendix C
Proof of Theorem 4

We consider the coding scheme of Section IV-A. The only difference with the proof of Theorem 3 is that instead of Lemma 4, we now need to lower bound for any $\mathcal{T} \subseteq \mathcal{S}$, the quantity $H(X_{\mathcal{T}}^N|X_{\mathcal{S}^c}^N A_{\mathcal{S}})$. We do it as follows.

$$H(X_{\mathcal{T}}^N|X_{\mathcal{S}^c}^N A_{\mathcal{S}}) = H(X_{\mathcal{T}}^N X_{\mathcal{S}^c}^N A_{\mathcal{S}}) - H(X_{\mathcal{S}^c}^N A_{\mathcal{S}}) \quad (79a)$$

$$= H(X_{\mathcal{T}}^N X_{\mathcal{S}^c}^N A_{\mathcal{S}\setminus\mathcal{T}}) - H(X_{\mathcal{S}^c}^N A_{\mathcal{S}}) \quad (79b)$$

$$= H(X_{\mathcal{T}}^N|X_{\mathcal{S}^c}^N) + H(A_{\mathcal{S}\setminus\mathcal{T}}|X_{\mathcal{T}}^N X_{\mathcal{S}^c}^N) - H(A_{\mathcal{S}}|X_{\mathcal{S}^c}^N). \quad (79c)$$

We lower bound $H(A_{\mathcal{S}\setminus\mathcal{T}}|X_{\mathcal{T}}^N X_{\mathcal{S}^c}^N)$ in the right hand side of (79c) as follows.

$$H(A_{\mathcal{S}\setminus\mathcal{T}}|X_{\mathcal{T}}^N X_{\mathcal{S}^c}^N) \geq NH(X_{\mathcal{S}\setminus\mathcal{T}}|X_0 X_{\mathcal{T}} X_{\mathcal{S}^c}) + o(N) \quad (80a)$$

$$= NH(X_{\mathcal{S}\setminus\mathcal{T}}|X_0) + o(N), \quad (80b)$$

where (80a) holds similarly to (75j) proved in Appendix A by conditioning on $X_{\mathcal{S}^c}^N$, (80b) holds by the Markov chain (1). We then upper bound $H(A_{\mathcal{S}}|X_{\mathcal{S}^c}^N)$ in the right hand side of (79c) as follows.

$$H(A_{\mathcal{S}}|X_{\mathcal{S}^c}^N) \leq \log|\mathcal{A}_{\mathcal{S}}| \quad (81a)$$

$$= \sum_{i\in\mathcal{S}} \log|\mathcal{A}_i| \quad (81b)$$

$$= \sum_{i\in\mathcal{S}} |\mathcal{H}_{X_i|X_0X_{1:i-1}}| \quad (81c)$$

$$= \sum_{i\in\mathcal{S}} NH(X_i|X_0X_{1:i-1}) + o(N) \quad (81d)$$

$$= NH(X_{\mathcal{S}}|X_0) + o(N) \quad (81e)$$

$$= NH(X_{\mathcal{T}}|X_0) + NH(X_{\mathcal{S}\setminus\mathcal{T}}|X_0) + o(N), \quad (81f)$$

where (81d) holds by [58, Th. 3.5], (81e) and (81f) hold by the Markov chain (1). Hence, we obtain

$$H(X_{\mathcal{T}}^N|X_{\mathcal{S}^c}^N A_{\mathcal{S}}) \geq NH(X_{\mathcal{T}}|X_{\mathcal{S}^c}) - NH(X_{\mathcal{T}}|X_0) - o(N) \quad (82a)$$

$$= NI(X_{\mathcal{T}}; X_0|X_{\mathcal{S}^c}) - o(N), \quad (82b)$$

where (82a) holds by combining (79c), (80b), and (81f), (82b) holds by the Markov chain (1).

Appendix D
Proof of Corollary 2

We first show the following lemma and then use a similar argument than in [60].

Lemma 6. *Let $\mathcal{S} \subset \mathcal{L}$. The set function $w : 2^{\mathcal{S}} \to \mathbb{R}^+, \mathcal{T} \mapsto I(X_{\mathcal{T}}; X_0|X_{\mathcal{S}^c})$ is submodular, i.e., $-w$ is supermodular.*

Proof. Let $\mathcal{U}, \mathcal{V} \subseteq \mathcal{S}$. We have

$$\begin{aligned} &I(X_{\mathcal{U}\cup\mathcal{V}}; X_0|X_{\mathcal{S}^c}) + I(X_{\mathcal{U}\cap\mathcal{V}}; X_0|X_{\mathcal{S}^c}) \\ &\quad = I(X_{\mathcal{U}}; X_0|X_{\mathcal{S}^c}) + I(X_{\mathcal{V}\setminus\mathcal{U}}; X_0|X_{\mathcal{S}^c}X_{\mathcal{U}}) \\ &\qquad + I(X_{\mathcal{U}\cap\mathcal{V}}; X_0|X_{\mathcal{S}^c}) \qquad (83a) \\ &\quad = I(X_{\mathcal{U}}; X_0|X_{\mathcal{S}^c}) + H(X_{\mathcal{V}\setminus\mathcal{U}}|X_{\mathcal{S}^c}X_{\mathcal{U}}) \\ &\qquad - H(X_{\mathcal{V}\setminus\mathcal{U}}|X_0X_{\mathcal{S}^c}X_{\mathcal{U}}) + I(X_{\mathcal{U}\cap\mathcal{V}}; X_0|X_{\mathcal{S}^c}) \qquad (83b) \\ &\quad \le I(X_{\mathcal{U}}; X_0|X_{\mathcal{S}^c}) + I(X_{\mathcal{V}\setminus\mathcal{U}}; X_0|X_{\mathcal{S}^c}X_{\mathcal{U}\cap\mathcal{V}}) \\ &\qquad + I(X_{\mathcal{U}\cap\mathcal{V}}; X_0|X_{\mathcal{S}^c}) \qquad (83c) \\ &\quad = I(X_{\mathcal{U}}; X_0|X_{\mathcal{S}^c}) + I(X_{\mathcal{V}}; X_0|X_{\mathcal{S}^c}), \qquad (83d) \end{aligned}$$

where (83c) holds because $H(X_{\mathcal{V}\setminus\mathcal{U}}|X_{\mathcal{S}^c}X_{\mathcal{U}}) \le H(X_{\mathcal{V}\setminus\mathcal{U}}|X_{\mathcal{S}^c}X_{\mathcal{U}\cap\mathcal{V}})$ and because $H(X_{\mathcal{V}\setminus\mathcal{U}}|X_0X_{\mathcal{S}^c}X_{\mathcal{U}}) = H(X_{\mathcal{V}\setminus\mathcal{U}}|X_0X_{\mathcal{S}^c}X_{\mathcal{U}\cap\mathcal{V}})$ by the Markov chain (1). ∎

For $\mathcal{S} \subset \mathcal{L}$, $(\mathcal{S}, w)$ defines a concave game by submodularity of w shown in Lemma 6. Consequently, its core $\mathcal{C}(w) \triangleq \left\{(R_i)_{i\in\mathcal{S}} : \sum_{i\in\mathcal{S}} R_l = v(\mathcal{S}) \text{ and } \sum_{i\in\mathcal{T}} R_i \le v(\mathcal{T}), \forall \mathcal{T} \subset \mathcal{S}\right\}$ is non-empty by [38], i.e., there exists an achievable rate tuple in $\mathcal{R}_{\mathcal{S}}$ with sum-rate $I(X_{\mathcal{S}}; X_0|X_{\mathcal{S}^c})$.

REFERENCES

[1] R. A. Chou and A. Yener, "A game theoretic treatment for pair-wise secret-key generation in many-to-one networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 1524–1528.

[2] R. La and V. Anantharam, "A game-theoretic look at the Gaussian multiaccess channel," *Discrete Math. Theor. Comput. Sci.*, vol. 66, pp. 87–106, Mar. 2004.

[3] V. Gajic and B. Rimoldi, "Game theoretic considerations for the Gaussian multiple access channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 2523–2527.

[4] Q. Zhu, H. Tembine, and T. Başar, "A constrained evolutionary Gaussian multiple access channel game," in *Proc. Int. Conf. Game Theory Netw.*, May 2009, pp. 403–410.

[5] A. Leshem and E. Zehavi, "Cooperative game theory and the Gaussian interference channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1078–1088, Sep. 2008.

[6] S. Mathur, L. Sankaranarayanan, and N. B. Mandayam, "Coalitional games in Gaussian interference channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2210–2214.

[7] R. Berry and D. Tse, "Shannon meets Nash on the interference channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2821–2836, May 2011.

[8] X. Liu and E. Erkip, "A game-theoretic view of the interference channel: Impact of coordination and bargaining," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2805–2820, May 2011.

[9] E. A. Jorswieck, E. G. Larsson, and D. Danev, "Complete characterization of the Pareto boundary for the MISO interference channel," *IEEE Trans. Signal Process.*, vol. 56, no. 10, pp. 5292–5296, Oct. 2008.

[10] E. G. Larsson and E. A. Jorswieck, "Competition versus cooperation on the MISO interference channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1059–1069, Sep. 2008.

[11] B. Peleg and P. Sudhölter, *Introduction to the Theory of Cooperative Games*, vol. 34. Berlin, Germany: Springer, 2007.

[12] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.

[13] R. B. Myerson, *Game Theory: Analysis of Conflict*. Cambridge, MA, USA: Harvard Univ. Press, 1991.

[14] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Process. Mag.*, vol. 26, no. 5, pp. 77–97, May 2009.

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

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

[17] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[18] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

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

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

[21] L. Lai and L. Huie, "Simultaneously generating multiple keys in many to one networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2394–2398.

[22] L. Lai and S.-W. Ho, "Key generation algorithms for pairwise independent networks based on graphical models," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4828–4837, Sep. 2015.

[23] H. Zhang, Y. Liang, L. Lai, and S. Shamai (Shitz), "Multi-key generation over a cellular model with a helper," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3804–3822, Jun. 2017.

[24] P. Xu, Z. Ding, X. Dai, and G. K. Karagiannidis, "Simultaneously generating secret and private keys in a cooperative pairwise-independent network," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1139–1150, Jun. 2016.

[25] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[26] E. Arikan, "Source polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 899–903.

[27] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010.

[28] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 639–651, Feb. 2012.

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

[30] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[31] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, pp. 40–47, Jan./Mar. 1996.

[32] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 1981.

[33] R. J. Aumann and B. Peleg, "Von Neumann–Morgenstern solutions to cooperative games without side payments," *Bull. Amer. Math. Soc.*, vol. 66, no. 3, pp. 173–179, 1960.

[34] G. Jentzsch, "Some thoughts on the theory of cooperative games," *Adv. Game Theory, Ann. Math. Stud.*, vol. 52, no. 52, pp. 407–442, 1964.

[35] L. Shapley and M. Shubik, "Game theory in economics—Chapter 6: Characteristic function, core, and stable set," Santa Monica, CA, USA, RAND, Tech. Rep. RAND R904/6-NSF, 1973.

[36] M. Maschler, B. Peleg, and L. S. Shapley, "Geometric properties of the kernel, nucleolus, and related solution concepts," *Math. Oper. Res.*, vol. 4, no. 4, pp. 303–338, 1979.

[37] R. A. Chou and A. Yener, "The degraded Gaussian multiple access wiretap channel with selfish transmitters: A coalitional game theory perspective," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 1703–1707.

[38] L. S. Shapley, "Cores of convex games," *Int. J. Game Theory*, vol. 1, no. 1, pp. 11–26, Dec. 1971.

[39] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," in *Combinatorial Structures and Their Applications*. Berlin, Germany: Springer-Verlag, 1970, pp. 69–87.

[40] M. Maschler, B. Peleg, and L. S. Shapley, "The kernel and bargaining set for convex games," *Int. J. Game Theory*, vol. 1, no. 1, pp. 73–93, 1971.

[41] R. J. Aumann and M. Maschler, "The bargaining set for cooperative games," *Adv. Game Theory*, vol. 52, pp. 443–476, 1964.

[42] T. Ichiishi, *Game Theory for Economic Analysis*. New York, NY, USA: Academic, 1983.
[43] D. Schmeidler, "The nucleolus of a characteristic function game," *SIAM J. Appl. Math.*, vol. 17, no. 6, pp. 1163–1170, 1969.
[44] F. A. Behringer, "A simplex based algorithm for the lexicographically extended linear maxmin problem," *Eur. J. Oper. Res.*, vol. 7, no. 3, pp. 274–283, 1981.
[45] B. Fromen, "Reducing the number of linear programs needed for solving the nucleolus problem of n-person game theory," *Eur. J. Oper. Res.*, vol. 98, no. 3, pp. 626–636, 1997.
[46] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.
[47] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *J. Cryptol.*, vol. 10, no. 2, pp. 97–110, 1997.
[48] 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.
[49] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[50] G. Kramer, "Topics in multi-user information theory," *Found. Trends Commun. Inf. Theory*, vol. 4, nos. 4–5, pp. 265–444, 2007.
[51] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2000, pp. 351–368.
[52] 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.
[53] J. HÅstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, 1999.
[54] 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, 2008.
[55] J. Wullschleger, "Oblivious-transfer amplification," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer-Verlag, 2007, pp. 555–572.
[56] H. Zhang, L. Lai, Y. Liang, and H. Wang, "The capacity region of the source-type model for secret key and private key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6389–6398, Oct. 2014.
[57] C. Ye and P. Narayan, "The secret key~private key capacity region for three terminals," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2005, pp. 2142–2146.
[58] E. Şaşoğlu, "Polar coding theorems for discrete systems," EPFL Thesis, EPFL, Switzerland, 2011.
[59] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2009, pp. 1493–1495.
[60] M. Madiman, "Cores of cooperative games in information theory," *EURASIP J. Wireless Commun. Netw.*, vol. 2008, no. 1, Apr. 2008, Art. no. 318704.

Rémi A. Chou (M'17) 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, in 2015. From 2015 to 2017, he was a postdoctoral scholar at The Pennsylvania State University, University Park, PA. He is now an Assistant Professor in the Electrical Engineering and Computer Science Department at Wichita State University, Wichita, KS.

Aylin Yener (S'91–M'01–SM'14–F'15) received the B.Sc. degree in electrical and electronics engineering and the B.Sc. degree in physics from Boğaziçi University, Istanbul, Turkey, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA. She is a Distinguished Professor of Electrical Engineering at The Pennsylvania State University, University Park, PA, USA, where she joined the faculty as an assistant professor in 2002. Since 2017, she is also a Dean's Fellow in the College of Engineering at The Pennsylvania State University. She was a visiting professor of Electrical Engineering at Stanford University in 2016–2018 and a visiting associate professor in the same department in 2008–2009. Her current research interests are in information security, green communications, caching systems, and more generally in the fields of information theory, communication theory and networked systems. She received the NSF CAREER Award in 2003, the Best Paper Award in Communication Theory from the IEEE International Conference on Communications in 2010, the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award in 2010, the IEEE Marconi Prize Paper Award in 2014, the PSEAS Premier Research Award in 2014, the Leonard A. Doggett Award for Outstanding Writing in Electrical Engineering at Penn State in 2014, and the IEEE Women in Communications Engineering Outstanding Achievement Award in 2018. She is a distinguished lecturer for the IEEE Information Theory Society (2019–2020), the IEEE Communications Society (2018–2020) and the IEEE Vehicular Technology Society (2017–2019).

Dr. Yener is serving as the vice president of the IEEE Information Theory Society in 2019. Previously she was the second vice president (2018), member of the Board of Governors (2015–2018) and the treasurer (2012–2014) of the IEEE Information Theory Society. She served as the Student Committee Chair for the IEEE Information Theory Society (2007–2011), and was the co-Founder of the Annual School of Information Theory in North America in 2008. She was a Technical (Co)-Chair for various symposia/tracks at the IEEE ICC, PIMRC, VTC, WCNC, and Asilomar in 2005, 2008–2014 and 2018. Previously, she served as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS (2009–2012), an Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING (2017–2018), and an Editor and an Editorial Advisory Board Member for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (2001–2012). She also served a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY in 2011, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS in 2015. Currently, she serves as a Senior Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.