A Game Theoretic Treatment for Pair-wise Secret-Key Generation in Many-to-One Networks

Remi A. Chou and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
The School of Electrical Engineering and Computer Science
The Pennsylvania State University, University Park, PA 16802.
remi.chou@psu.edu *yener@engr.psu.edu*

***Abstract*—We consider secret-key generation between several agents and a base station that observe independent and identically distributed (i.i.d.) 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. We do not require them to be kept secret among the agents. 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 all the 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. We study this tension between cooperation and self-interest with a game-theoretic treatment. We establish that cooperation is in the best interest of all agents and that there exists individual secret-key rate allocations that incentivize the agents to follow the protocol. Additionally, we propose an explicit and low-complexity coding scheme based on polar codes and hash functions that achieves such allocations.**

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

I. Introduction

Multiuser communication settings subject to limited total resources bring about issues pertaining to conflict of interests, competition, and fairness among users. Such issues are typically studied by means of game theory - we refer to [1] and references therein for a comprehensive survey.

In this paper, we study a multiterminal secret-key generation problem that involves conflict of interests between users, and propose a solution based on cooperative game theory, more specifically, based on forming coalitions. We refer to [2] for an introduction to coalitional game theory, and to [3] 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 – by means of 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, however, they are not required to be kept secret among agents, i.e, we consider a setting where it is not critical for any agent to learn about the information reported by the other agents. We consider a source model for secret-key generation, i.e., the agents and the base station observe i.i.d. realizations of correlated random variables, and can communicate over a public noiseless channel. It can be shown that the agents increase the sum of all key lengths by agreeing to participate in a joint protocol, in contrast to operating separately on their own. However, each agent is interested in maximizing its own key length only. Consequently, 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.

Note that when the agents are not assumed selfish and when fairness issues are ignored, the secret-key generation model we consider is similar to the one studied in [4] and related to multiple-key generation in a network with trusted helpers [5].

Our contributions are three-fold. (i) In Section II, we formally define the problem and cast it as a coalitional game, for which we derive properties and propose rate allocations as candidates for fair solutions in Section III. (ii) By adding the constraint that the agents are selfish, compared to the model in [4], we are able to derive a secret-key capacity region for an arbitrary number of agents, whereas without this consideration, the secret-key capacity region of the model we consider is unknown, even for two agents [4], [5]. (iii) We provide in Section IV an explicit and low-complexity coding scheme based on polar codes for source coding and hash functions to implement the solutions proposed in Section II.

Proofs are omitted for brevity. We provide concluding remarks in Section V.

II. Problem Statement

We define in Section II-A a secret-key generation model, and in Section II-B a coalitional game associated with this model when the agents are selfish. In the following, for reals a, b, we define $[\![a,b]\!] \triangleq [a,b] \cap \mathbb{N}$.

A. Secret-key generation model

Define $\mathcal{X}_{\mathcal{L}}$ as the Cartesian product of L finite alphabets $\mathcal{X}_l$, $l \in \mathcal{L} \triangleq [\![1,L]\!]$. Consider a discrete memoryless source (DMS) $(\mathcal{X}_{\mathcal{L}} \times \mathcal{X}_0, p_{X_{\mathcal{L}}X_0})$, where $\mathcal{X}_0$ is a finite alphabet and

This work was supported in part by NSF grant CNS-1314719.

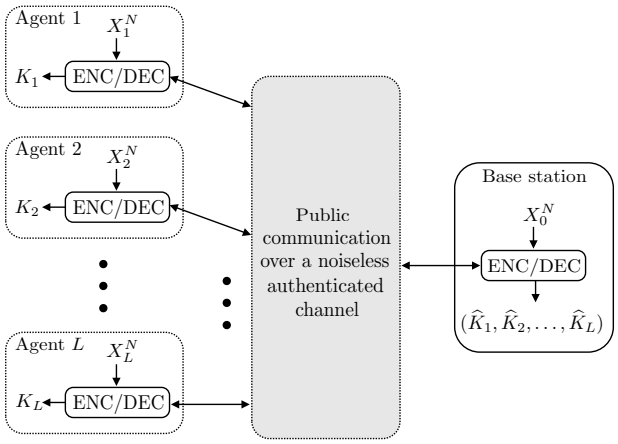

Fig. 1. Many-to-one secret-key generation setting.

$X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$. For $l \in \mathcal{L}$, Agent l observes the component X_l of the DMS, and the base station observes the component X_0. In this paper, the source is assumed to follow the following Markov chain: for any $\mathcal{S}, \mathcal{T} \subset \mathcal{L}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$,

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

Assuming all 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.

Definition 1. *For $i \in \mathcal{L}$, let $\mathcal{K}_i$ be a key alphabet of size 2^{NR_i} and define $\mathcal{K}_{\mathcal{L}}$ as the Cartesian product of $\mathcal{K}_i$, $i \in \mathcal{L}$. A $((2^{NR_i})_{i\in\mathcal{L}}, N)$ secret-key generation strategy 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 is denoted by $A_{\mathcal{L}} \in \mathcal{A}_{\mathcal{L}}$, for some discrete alphabet $\mathcal{A}_{\mathcal{L}}$.*
3) *Agent i, $i \in \mathcal{L}$, computes $K_i(X_i^N, A_{\mathcal{L}}) \in \mathcal{K}_i$.*
4) *The base station computes $\widehat{K}_i(X_0^N, A_{\mathcal{L}}) \in \mathcal{K}_i$, $i \in \mathcal{L}$.*

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

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

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

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

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

The secrecy constraint (3) ensures that the keys generated by the agents are independent from the public communication. By (4), the keys generated are almost jointly independent [4], so that the simultaneous use of the keys by the agents is secure.

B. Game definition

We consider a coalitional game [2] for the secret-key generation problem of Section II-A where the agents are the players. The players are selfish, i.e., solely interested in maximizing their payoffs, which we define as their individual secret-key rates. The base station is not a player but is merely a passive entity. The agents can potentially form coalitions to maximize their payoffs, in the sense that subsets of agents can agree on a collective protocol to follow before the actual secret-key generation protocol occurs. 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 can only use the public channel. We define our coalitional game by associating with each coalition of cooperating agents $\mathcal{S} \subseteq \mathcal{L}$ a certain worth $v(\mathcal{S})$, which we define as the *maximal secret-key sum-rate* that coalition $\mathcal{S}$ can obtain *regardless of the strategies adopted by the member of $\mathcal{S}^c$*. 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?

This game formulation follows a framework analogous to the one for the Gaussian multiple access channel problem studied in [6], and the Gaussian multiple access wiretap channel problem studied in [7]. This framework is generically termed as alpha theory [8].

III. Game analysis

We study the properties of v in Section III-A and propose candidates for secret-key rate allocations in Section III-B.

A. Properties of the game and characterization of its core

We start by giving the following characterization of $v(\mathcal{S})$ defined in Section II-B.

Theorem 1. *For $\mathcal{S} \subseteq \mathcal{L}$, we have $v(\mathcal{S}) = I(X_{\mathcal{S}}; X_0|X_{\mathcal{S}^c})$.*

We readily observe that the game defined in Section II-B is superadditive in the sense that 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 $\mathcal{S} \cup \mathcal{T}$. One can indeed show that the secrecy constraints for coalitions $\mathcal{S}$ and $\mathcal{T}$, with $\mathcal{S} \cap \mathcal{T} = \emptyset$, implies a secrecy constraint for the coalition $\mathcal{S} \cup \mathcal{T}$; we omit details for brevity. 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. A useful concept to overcome this complication is the core of the game.

Definition 3 (e.g. [2])**.** *The core $\mathcal{C}(v)$ of a superadditive game $(\mathcal{L}, v)$ is defined by*

$$\left\{ (R_l)_{l\in\mathcal{L}} : \sum_{l\in\mathcal{L}} R_l = v(\mathcal{L}) \text{ and } \sum_{i\in\mathcal{S}} R_i \geqslant v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L} \right\}. \tag{5}$$

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 (5) 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.

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

Definition 4 ([9])**.** *A game $(\mathcal{L}, v)$ is convex if v is supermodular, i.e., $\forall \mathcal{U}, \mathcal{V} \subseteq \mathcal{L}, v(\mathcal{U}) + v(\mathcal{V}) \leqslant v(\mathcal{U} \cup \mathcal{V}) + v(\mathcal{U} \cap \mathcal{V})$.*

The intuition behind this definition is that supermodularity provides a stronger incentive to form coalition than superadditity. Indeed, supermodularity of a function can equivalently be defined as follows [9]

$$\forall l \in \mathcal{L}, \forall \mathcal{T} \subseteq \mathcal{L} \backslash \{l\}, \forall \mathcal{S} \subseteq \mathcal{T}, \\ v(\mathcal{S} \cup \{l\}) - v(\mathcal{S}) \leqslant v(\mathcal{T} \cup \{l\}) - v(\mathcal{T}), \quad (6)$$

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.

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

Corollary 1. *By [9] any convex game has non-empty core. Hence, by Proposition 1, the game defined in Sectoin II-B has a non-empty core $\mathcal{C}(v)$.*

We provide an alternative characterization of the core that will turn out to be useful to show that any point of the core can be achieved. 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 Section II-B is given by*

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

B. Candidates for secret-key rate allocations

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*: The secret-key sum-rate capacity for the grand coalition $\mathcal{L}$ is achieved. (ii) *Symmetry*: 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*: 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*: 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. In our setting, the later axiom could correspond to several key generation protocols performed by the same agents with the source statistics varying for each protocol. Moreover, it would mean that even if the agents do not know in advance the number P of secret-key generation protocols they are going to be involved in and which particular source statistics will be associated with each protocol, they are going to obtain the same individual key lengths as if they had to perform the P protocols simultaneously, in the sense of performing one protocol whose value function is the sum of P value functions.

The unique secret-rate tuple that satisfies the previous four axioms is called the Shapley value.

Proposition 2. *The Shapley value of $(\mathcal{L}, v)$ defined in Section II-B is in $\mathcal{C}(v)$ and is given by $(R_l^{\text{Shap}})_{l \in \mathcal{L}}$, where for $l \in \mathcal{L}$*

$$R_l^{\text{Shap}} = I(X_l; X_0) - \frac{1}{L} \sum_{\mathcal{S} \subseteq \mathcal{L} \backslash \{l\}} \binom{L-1}{|\mathcal{S}|}^{-1} I(X_l; X_{\mathcal{S}}). \quad (7)$$

The fact that the Shapley value belongs to the core follows by [9] from the convexity of $(\mathcal{L}, v)$ proved in Proposition 1. Observe that (7) quantifies the difference of key length obtained for Agent l, $l \in \mathcal{L}$, between the case $L = 1$ and the case $L > 1$.

Other *solution concepts* than the Shapley value can be considered to choose a "*fair*" point in the core. In particular, the additivity axiom might not always be relevant in our problem, for instance, if the agents only perform a unique secret-key generation protocol. We do not intend to provide an exhaustive list of such concepts, we will, however, describe a solution concept that has attracted a certain interest in many studies, the nucleolus.

Definition 5 (e.g. [2])**.** *Define the set of preimputation $\mathcal{Y} \triangleq \{\mathbf{y} = (y_i)_{i \in \mathcal{L}} \in \mathbb{R}_+^L : \sum_{i \in \mathcal{L}} y_i = v(\mathcal{L})\}$. 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 $i, j \in [\![1, 2^L]\!], i < j \implies \theta_i(\mathbf{y}) \geqslant \theta_j(\mathbf{y})$. The nucleolus is defined as $\{\mathbf{y}_0 \in \mathcal{Y} : \theta(\mathbf{y}_0) \preceq \theta(\mathbf{y}), \forall y \in \mathcal{Y}\}$, where " $\preceq$ " denote the lexicographic order, i.e., for $\mathbf{y}^{(1)}, \mathbf{y}^{(2)} \in \mathcal{Y}$, $\left(\mathbf{y}^{(1)} \preceq \mathbf{y}^{(2)}\right) \iff \left(\mathbf{y}^{(1)} = \mathbf{y}^{(2)}\right.$ or , $\left.\exists i_0, \left(\forall j < i_0, y_j^{(1)} = y_j^{(2)} \text{ and } y_{i_0}^{(1)} < y_{i_0}^{(2)}\right)\right)$.*

A possible interpretation of the nucleolus is to see the excess $e(\mathbf{y}, \mathcal{S})$ for some $\mathbf{y} \in \mathcal{Y}$, $\mathcal{S} \in 2^{\mathcal{L}}$, as an indicator of dissatisfaction of coalition $\mathcal{S}$ associated with the preimputation $\mathbf{y}$. One thus might want to choose the preimputation $\mathbf{y}$ 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 one obtains a unique choice for $\mathbf{y}$ as stated in Proposition 3.

Proposition 3 ([10])**.** *For a convex game, the nucleolus is a singleton and belongs to the core.*

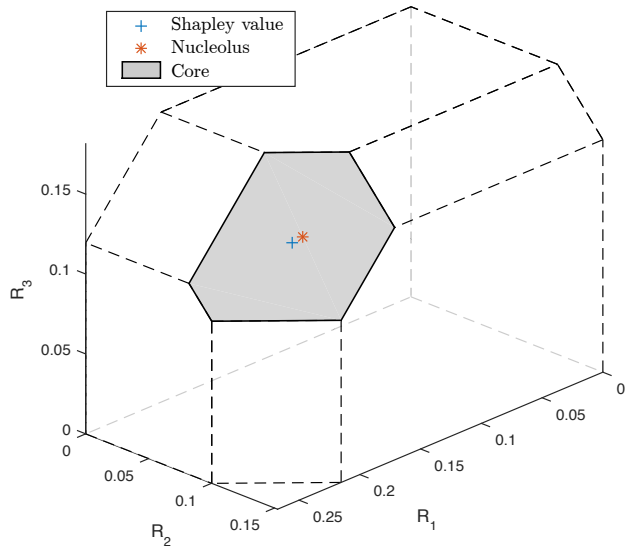

Fig. 2. Core, Shapley value, and nucleolus of the game described in Example 1.

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

Example 1. *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 $x \in [0, 1]$, $\bar{x} = 1 - x$. One can show that, when $L = 3$ and $(q\ p_1\ p_2\ p_3) = (0.40\ 0.20\ 0.27\ 0.25)$, we have $v(\{1\}) \approx 0.17134$, $v(\{2\}) \approx 0.08205$, $v(\{3\}) \approx 0.10142$, $v(\{1, 2\}) \approx 0.28771$, $v(\{1, 3\}) \approx 0.31679$, $v(\{2, 3\}) \approx 0.20155$, $v(\{1, 2, 3\}) \approx 0.46921$. Using Proposition 2, we obtain the following secret-key rates*

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

The core of the game, as well as the Shapley value and the nucleolus are depicted in Figure 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. In Theorem 3, we claim that the coding scheme presented in Section IV-A achieves for the grand coalition, i.e., the coalition $\mathcal{L}$, a region that contains the core $\mathcal{C}(v)$. The proof is briefly sketched in Section IV-B.

Theorem 3. *Consider a DMS $(\mathcal{X}_\mathcal{L} \times \mathcal{X}_0, p_{X_\mathcal{L} X_0})$ such that $\forall l \in \mathcal{L}, |\mathcal{X}_l| = 2$. Any rate tuple in $\mathcal{R}_\mathcal{L} \triangleq \left\{(R_l)_{l\in\mathcal{L}} : 0 \leqslant \sum_{i\in\mathcal{S}} R_i \leqslant I(X_\mathcal{S}; X_0), \forall \mathcal{S} \subseteq \mathcal{L}\right\}$ 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 $\mathcal{R}_\mathcal{L} \supseteq \mathcal{C}(v)$.*

Note that Theorem 3 can be extended so as to not require the Markov chain (1).

Remark 1. *For $L = 2$, [4, Theorem 3] provides a coding scheme to achieve the region $\mathcal{R}_\mathcal{L}$ in Theorem 3. For arbitrary L, [4, Theorem 1] provides a coding scheme that achieves the sum-rate $v(\mathcal{L})$. However, in contrast to our solution, these coding schemes, which rely on existence results from [11], are neither explicit nor low-complexity, require time-sharing (for [4, Theorem 3]), and only provide weak-secrecy.*

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 [12], 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.

Our coding scheme operates over B blocks of length N, where N is a power 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 1, 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 [13]. For any $l \in \mathcal{L}$, we define the polar transform of X_l^N by $U_l^N \triangleq X_l^N G_n$, moreover, for any set $\mathcal{I} \subseteq [\![1, N]\!]$, we define $U_l^N[\mathcal{I}] \triangleq ((U_l)_i)_{i\in\mathcal{I}}$. For any $l \in \mathcal{L}$, for any $\mathcal{S} \subseteq \mathcal{L}$, for $\delta_N \triangleq 2^{-N^\beta}$ with $\beta \in]0, 1/2[$, we also define the following sets

$$\mathcal{H}_{X_l|X_0} \triangleq \left\{i \in [\![1, N]\!] \colon H\left((U_l)_i | (U_l)^{i-1} X_0^N\right) \geqslant \delta_N\right\}.$$

The privacy amplification step, described in Algorithm 2, relies on two-universal hash functions. 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.

B. Coding Scheme Analysis

The proof of Theorem 3 relies on [14, Lemma 1.1], [13], [15, Lemma 7], and [16] combined with the following version of the leftover hash lemma. One of the additional challenges

Algorithm 1 Reconciliation protocol

for Agent $l \in \mathcal{L}$ **do**
  for Block $b \in \mathcal{B}$ **do**
    Compute $U_l^N \triangleq X_l^N G_n$
    Transmit $A_l \triangleq U_l^N[\mathcal{H}_{X_l|X_0}]$ to the base station over the public channel
  end for
end for
Let $A_{\mathcal{L}} \triangleq (A_l)_{l\in\mathcal{L}}$ denote the public communication in a Block $b \in \mathcal{B}$.
for Block $b \in \mathcal{B}$ **do**
  Given $A_{\mathcal{L}}^b$ and X_0^N observed in Block b, the base station reconstructs $X_{\mathcal{L}}^N$ for Block b using the successive cancellation algorithm for source coding with side information of [13].
end for

Algorithm 2 Privacy amplification protocol

for Block $b \in \mathcal{B}$ **do**
  for Agent $l \in \mathcal{L}$ **do**
    Compute $K_l \triangleq F_l(X_l^N)$
    Publicly transmit the choice of F_l to the base station
  end for
  for $l \in \mathcal{L}$ **do**
    The base station computes $K_l \triangleq F_l(X_l^N)$
  end for
end for

introduced by a distributed setting, compared to [12], is the evaluation of the min-entropies appearing in Lemma 1.

Lemma 1 (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 $F_{\mathcal{L}}(X_{\mathcal{L}}) \triangleq (F_1(X_1)||F_2(X_2)||\dots||F_L(X_L))$, where $||$ denotes concatenation. Then, for any $z \in \mathcal{Z}$, we have*

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

where H_∞ denotes the min-entropy, $\mathbb{V}$ denotes the variational distance, $p_{U_{\mathcal{K}}}$ and $p_{U_{\mathcal{F}}}$ are the uniform distribution over $[\![1, 2^{r_{\mathcal{L}}}]\!]$, and $[\![1, s_{\mathcal{L}}]\!]$, respectively.

V. Concluding Remarks

We have studied a pairwise secret-key generation source model between L 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 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 can adopt. We have showed that the game associated with our problem is convex, and characterized its core, which is interpreted as a converse for our setting. We have concluded that the grand coalition is in the best interest of all agents and stable, in the sense that no coalition of agents has any incentive to leave the grand coalition. We have also characterized the Shapley value, and identified it as a possible solution concept to ensure fairness among agents. Finally, we have proposed an explicit and low-complexity coding scheme relying on polar codes for source coding and hash functions to achieve *any point of the core*. Under the proposed coalitional game theory framework, we thus obtain the secret-key capacity region for our problem. It contrasts with the fact that no tight outer bound is known for the model we consider when the selfishness constraints are removed, even when $L = 2$.

The alpha theory framework for coalitional games is general and could be applied to other security problems involving a tension between cooperation and self-interest. The difficulty is to characterize a value function for this framework. Our problem without the degradation property (1) remains open for this reason and is, unfortunately, at least as difficult as determining the secret-key capacity for the two-user secret generation model in [12].

References

[1] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.

[2] B. Peleg and P. Sudhölter, *Introduction to the theory of cooperative games*. Springer Science & Business Media, 2007, vol. 34.

[3] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Başar, "Coalitional game theory for communication networks," *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp. 77–97, 2009.

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

[5] H. Zhang, Y. Liang, L. Lai, and S. Shamai, "Multi-key generation over a cellular model with a helper," *Subm. to IEEE Trans. Inf. Theory*, 2015.

[6] R. La and V. Anantharam, "A game-theoretic look at the Gaussian multiaccess channel," *DIMACS series in discrete mathematics and theoretical computer science*, vol. 66, pp. 87–106, 2004.

[7] R. Chou and A. Yener, "The degraded gaussian multiple access wiretap channel with selfish transmitters: A coalitional game theory perspective," in *IEEE Int. Symp. Inf. Theory*, 2017.

[8] L. Shapley and M. Shubik, "Game theory in economics - Chapter 6: Characteristic function, core, and stable set," *RAND R904/6-NSF*, 1973.

[9] L. Shapley, "Cores of convex games," *International journal of game theory*, vol. 1, no. 1, pp. 11–26, 1971.

[10] D. Schmeidler, "The nucleolus of a characteristic function game," *SIAM Journal on applied mathematics*, vol. 17, no. 6, pp. 1163–1170, 1969.

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

[12] C. Cachin and U. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, 1997.

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

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

[15] R. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages: A random bining analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.

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