Multi-terminal Secrecy in a Linear Non-coherent Packetized Networks

Mahdi Jafari Siavoshani
Ecole Polytechnique Fédérale de Lausanne
Email: mahdi.jafarisiavoshani@epfl.ch

Christina Fragouli
Ecole Polytechnique Fédérale de Lausanne
Email: christina.fragouli@epfl.ch

Abstract—We consider a group of $m+1$ **trusted nodes that aim to create a shared secret key $\mathcal{K}$ over a network in the presence of a passive eavesdropper, Eve. We assume a linear non-coherent network coding broadcast channel (over a finite field $\mathbb{F}_q$) from one of the honest nodes (i.e., Alice) to the rest of them including Eve. All of the trusted nodes can also discuss over a cost-free public channel which is also overheard by Eve.**

For this setup, we propose upper and lower bounds for the secret key generation capacity assuming that the field size q is very large. For the case of two trusted terminals ($m = 1$) our upper and lower bounds match and we have complete characterization for the secrecy capacity in the large field size regime.

I. Introduction

For communication over a network performing linear network coding, Cai and Yeung [1] introduced the problem of securing a multicast transmission against an eavesdropper. In particular, consider a network implementing linear network coding over a finite field $\mathbb{F}_q$. Let us assume that the min-cut value from the source to each receiver is c. From the main theorem of network coding [2], [3] we know that a source can send information at rate equal to the min-cut c to the destinations, in the absence of any malicious eavesdropper. Now, suppose there is a passive eavesdropper, Eve, who overhears ρ arbitrary edges in the network. The *secure network coding* problem is to design a coding scheme such that Eve does not obtain any information about the messages transmitted from the source to destinations. Cai and Yeung [1] showed that the secrecy capacity for this problem is $c - \rho$ and can be achieved if the field size q is sufficiently large. Later this problem formulation has been investigated in many other works. Feldman *et al.* [4] showed that by sacrificing a small amount of rate, one might find a secure scheme that requires much smaller field size. Rouayheb *et al.* [5] observed that this problem can be considered as a generalization of the Ozarow-Wyner wiretap channel of type II. Silva *et al.* [6] proposed a universal coding scheme that only employs encoding at the source.

In contrast to the previous work, in this paper we study the problem of secret key sharing among multiple terminals when nodes can send feedback over a public channel. We consider a source multicasting information over a network at rate equal to the min-cut c to the destinations. We also assume that the relay nodes in the network perform linear randomized network coding which is modeled by a non-coherent transmission scheme. Motivated by [7], [8], we model a non-coherent network coding scenario by a multiplicative matrix channel over a finite field $\mathbb{F}_q$ with uniform and i.i.d. distribution over transfer matrices in every time-slot.

The problem of key agreement between a set of terminals with access to noisy broadcast channel and public discussion channel (visible to the eavesdropper) was studied in [9], where some achievable secrecy rates were established, assuming Eve does not have access to the noisy broadcast transmissions. This was generalized in [10], [11] by developing (non-computable) outer bounds for secrecy rates. However, to the best of our knowledge, ours is the first work to consider multi-terminal secret key agreement over networks employing randomized network coding, when a passive eavesdropper has access to the broadcast transmissions.

Our contributions in this paper are as follows. For the secret key sharing problem introduced above, we propose an asymptotic achievability scheme assuming that the field size q is large. This scheme is based on *subspace coding* and can be extended for arbitrary number of terminals. Using the result of [9], we derive an upper bound for this problem. For $m = 1$, the proposed lower bound matches the upper bound and the *secret key generation capacity* is characterized. However, for $m \geq 2$, depending on the channel parameters, the upper and lower bound might match or not.

The paper is organized as follows. In §II we introduce our notation and the problem formulation and present some preliminaries. In §III, we state a general upper bound for the key generation capacity and evaluate it for the non-coherent network coding broadcast channel. The main results of the paper are presented in §IV.

II. Notation and Setup

A. Notation

We use $\langle X \rangle$ to denote the row span of a matrix X. We use also $[i : j]$ to denote $\{i, i + 1, \ldots, j\}$ where $i, j \in \mathbb{Z}$.

Let Π be an arbitrary vector space of finite dimension defined over a finite field $\mathbb{F}_q$. Suppose Π_1 and Π_2 are two subspaces of Π, i.e., $\Pi_1 \sqsubseteq \Pi$ and $\Pi_2 \sqsubseteq \Pi$. We use $\Pi_1 \cap \Pi_2$ to denote the common subspaces of both Π_1 and Π_2 and $\Pi_1 + \Pi_2$ as the smallest subspace that contains both Π_1 and Π_2. Two subspaces Π_1 and Π_2 are called *orthogonal* if $\Pi_1 \cap \Pi_2 = \{\mathbf{0}\}$.

Two subspaces Π_1 and Π_2 of Π are called *complementary* if they are orthogonal and $\Pi_1 + \Pi_2 = \Pi$.

Now, consider two subspaces Π_1 and Π_2. We define the subtraction of Π_2 from Π_1 by $U = \Pi_1 \setminus_s \Pi_2$ where U is any subspace of Π_1 which is complementary with $\Pi_1 \cap \Pi_2$. Note that, given Π_1 and Π_2, U is not uniquely defined.

For notational convenience, when $\mathcal{J}$ is a set, by $\Pi_{\mathcal{J}}$ we mean $\Pi_{\mathcal{J}} \triangleq \cap_{i \in \mathcal{J}} \Pi_i$.

B. Preliminaries

Definition 1. *We define $\mathcal{S}(\ell, k)$ to be the set of all subspaces of dimension at most k in the ℓ-dimensional space $\mathbb{F}_q^\ell$.*

Definition 2 (see [7]). *We denote by $\xi(n, d)$ the number of different $n \times \ell$ matrices with elements from a finite field $\mathbb{F}_q$, such that their rows span a specific subspace $\pi_d \sqsubseteq \mathbb{F}_q^\ell$ of dimension d where $0 \le d \le \min[n, \ell]$. By using [7, Lemma 2], $\xi(n, d)$ does not depend on ℓ and depends on π_d only through its dimension d.*

Lemma 1. *Suppose that k subspaces $\Pi_1, \ldots, \Pi_k$, with dimensions $d_1, \ldots, d_k$, are chosen uniformly at random from $\mathbb{F}_q^n$. Then w.h.p. (with high probability)[1] we have*

$$\dim(\Pi_1 + \cdots + \Pi_k) = \min[d_1 + \cdots + d_k, n], \quad and$$
$$\dim(\Pi_1 \cap \cdots \cap \Pi_k) = [d_1 + \cdots + d_k - (k-1)n]^+.$$

Note that even if one of the subspaces, for example Π_1, is a fixed subspace, then the above results are still valid.

Proof: These results follow from [12, Corollary 1] by using induction on the number of subspaces. ∎

C. Problem Statement

We consider a set of $m + 1 \ge 2$ honest nodes, $\mathsf{T}_0, \ldots, \mathsf{T}_m$, ($\mathsf{T}$ stands for "terminal") that aim to share a secret key $\mathcal{K}$ among themselves while keeping it concealed from a passive adversary, Eve. Eve does not perform any transmissions, but is trying to eavesdrop on (overhear) the communications between the honest nodes. For convenience, sometimes we will refer to node $\mathsf{T}_0, \mathsf{T}_1, \mathsf{T}_2, \ldots$, as "Alice," "Bob," "Calvin," and so on.

We assume that there exists a non-coherent network coding broadcast channel (which is going to be defined more precisely in the following) from Alice to the other terminals (including Eve). Also assume that the legitimate terminals can publicly discuss over a noiseless rate unlimited public channel.

Consider a non-coherent linear network coding communication scenario where at every time-slot t Alice (terminal T_0) injects a set of n_A vectors (packets) of length ℓ (over some finite field $\mathbb{F}_q$) into the network, denoted by the row vectors of the matrix $X_\mathsf{A}[t] \in \mathbb{F}_q^{n_A \times \ell}$. Each terminal T_i receives n_i randomly chosen linear combinations of the transmitted vectors, namely for $r \in \{1, \ldots, m, \mathsf{E}\}$, we have[2]

$$X_r[t] = F_r[t] X_\mathsf{A}[t], \tag{1}$$

[1]During the paper by "high probability" we mean probability of order $1 - O(q^{-1})$ unless otherwise stated.

[2]As subscript, we use i to denote for T_i for all $i \in [0 : m]$. At some points, we also use $X_\mathsf{A}, X_\mathsf{B}, X_\mathsf{C}$, etc., to denote for X_0, X_1, X_2, etc.

where $F_r[t] \in \mathbb{F}_q^{n_r \times n_\mathsf{A}}$ is chosen uniformly at random among all possible matrices and independently for each receiver and every time-slot. So for the channel transition probability we can write

$$P_{X_1 \cdots X_m X_\mathsf{E} | X_\mathsf{A}}(x_1, \ldots, x_m, x_\mathsf{E} | x_\mathsf{A}) =$$
$$P_{X_\mathsf{E} | X_\mathsf{A}}(x_\mathsf{E} | x_\mathsf{A}) \prod_{i=1}^{m} P_{X_i | X_\mathsf{A}}(x_i | x_\mathsf{A}), \tag{2}$$

where for each $r \in \{1, \ldots, m, \mathsf{E}\}$ we have (see [7, Sec IV-A])

$$P_{X_r | X_\mathsf{A}}(x_r | x_\mathsf{A}) \triangleq \begin{cases} q^{-n_r \dim(x_\mathsf{A})} & \text{if } \langle x_r \rangle \sqsubseteq \langle x_\mathsf{A} \rangle, \\ 0 & \text{otherwise.} \end{cases}$$

Note that in this setup we do not assume any CSI[3] at the transmitter or receivers.

In order to define the secrecy capacity, we use [13, Definition 1] and [13, Definition 2] (see also [14], [15], [9], [11]).

III. UPPER BOUND

A. Secrecy Upper Bound for Independent Broadcast Channels

The secret key generation capacity among multiple terminals (without eavesdropper having access to the broadcast channel) is completely characterized in [9]. By using this result, it is possible to state an upper bound for the secrecy capacity of the key generation problem among multiple terminals where the eavesdropper has also access to the broadcast channel. This can be done by adding a dummy terminal to the first problem and giving all the eavesdropper's information to this dummy node and let it to participate in the key generation protocol. By doing so, the secret key generation rate does not decrease. Hence by combining [9, Theorem 4.1] and [9, Lemma 5.1], the following result can be stated.

Theorem 1. *The secret key generation capacity is upper bounded as follows*

$$C_s \le$$
$$\max_{P_{X_0}} \min_{\lambda \in \Lambda([0:m])} \left[H(X_{[0:m]} | X_\mathsf{E}) - \sum_{B \subsetneq [0:m]} \lambda_B H(X_B | X_{B^c}, X_\mathsf{E}) \right],$$

where $\Lambda([0 : m])$ is the set of all collections $\lambda = \{\lambda_B : B \subsetneq [0 : m], B \ne \emptyset\}$ of weights $0 \le \lambda_B \le 1$, satisfying

$$\sum_{B \subsetneq [0:m], i \in B} \lambda_B = 1, \qquad \forall i \in [0 : m].$$

Note that in the above expression for the upper bound, it is possible to change the order of maximization and minimization [9, Theorem 4.1].

Now, for our problem where the channel from Alice to the other terminals are assumed to be independent, we can further simplify the upper bound given in Theorem 1, as stated in Corollary 1.

Corollary 1. *If the channels from Alice to the other terminals are independent, as described in (2), then the upper bound*

[3]Channel state information.

stated in Theorem 1, for the secret key generation capacity is simplified to

$$C_s \leq \max_{P_{X_0}} \min_{j \in [1:m]} I(X_0; X_j | X_\mathsf{E}) \tag{3}$$

$$\leq \min_{j \in [1:m]} \max_{P_{X_0}} I(X_0; X_j | X_\mathsf{E}). \tag{4}$$

Proof: For the proof please refer to [16]. ∎

Remark: Note that (3) is the best upper bound one might hope for an independent broadcast channel using results of [9].

Remark: Using [14, Theorem 7] or [15, Theorem 2], we observe that the bound given in (4) is indeed tight for the two terminals problem where we have the Markov chains $X_\mathsf{B} \leftrightarrow X_\mathsf{A} \leftrightarrow X_\mathsf{E}$ (when the channels are independent) or $X_\mathsf{A} \leftrightarrow X_\mathsf{B} \leftrightarrow X_\mathsf{E}$ (when the channels are degraded).

B. Upper Bound for Non-coherent Channel

In the previous section, we have shown that the secret key generation rate for our problem can be upper bounded by (4). Now, we need to evaluate the above upper bound for the non-coherent network coding channel defined in §II-C.

Lemma 2. *For the joint distribution of the form*

$$P_{X_\mathsf{A} X_i X_\mathsf{E}}(x_\mathsf{A}, x_i, x_\mathsf{E}) = P_{X_\mathsf{A}}(x_\mathsf{A}) P_{X_i | X_\mathsf{A}}(x_i | x_\mathsf{A}) P_{X_\mathsf{E} | X_\mathsf{A}}(x_\mathsf{E} | x_\mathsf{A})$$

the mutual information $I(X_\mathsf{A}; X_i | X_\mathsf{E})$ is a concave function of $P_{X_\mathsf{A}}(x_\mathsf{A})$ for fixed $P_{X_i | X_\mathsf{A}}(x_i | x_\mathsf{A})$ and $P_{X_\mathsf{E} | X_\mathsf{A}}(x_\mathsf{E} | x_\mathsf{A})$.

Proof: For the proof please refer to [16]. ∎

Similar to [7, Definition 5], here we define an equivalent subspace broadcast channel from Alice (terminal T_0) to the rest of terminals as follows. We assume that Alice sends a subspace $\Pi_\mathsf{A} \in \mathcal{S}(\ell, n_\mathsf{A})$ where $\Pi_\mathsf{A} = \langle X_\mathsf{A} \rangle$ and each of the legitimate terminals receives $\Pi_i \in \mathcal{S}(\ell, n_i)$ and Eve receives $\Pi_\mathsf{E} \in \mathcal{S}(\ell, n_\mathsf{E})$ where $\Pi_i = \langle X_i \rangle$ and $\Pi_\mathsf{E} = \langle X_\mathsf{E} \rangle$, respectively. The channel transition probabilities are independent and for each receiver i is defined as follows

$$P_{\Pi_i | \Pi_\mathsf{A}}(\pi_i | \pi_\mathsf{A}) \triangleq \begin{cases} \xi(n_i, \dim(\pi_i)) q^{-n_i \dim(\pi_\mathsf{A})} & \text{if } \pi_i \sqsubseteq \pi_\mathsf{A}, \\ 0 & \text{otherwise,} \end{cases}$$

where the function ξ is defined in Definition 2.

Lemma 3. *For every input distribution P_{X_A} there exists an input distribution P_{Π_A} such that $I(X_\mathsf{A}; X_i | X_\mathsf{E}) = I(\Pi_\mathsf{A}; \Pi_i | \Pi_\mathsf{E})$ and vice-versa.*

Proof: For the proof please refer to [16]. ∎

So by Lemma 3, in order to maximize $I(X_\mathsf{A}; X_i | X_\mathsf{E})$ with respect to P_{X_A} it is sufficient to solve an equivalent problem, i.e., maximize $I(\Pi_\mathsf{A}; \Pi_i | \Pi_\mathsf{E})$ with respect to P_{Π_A}; which is seemingly a simpler optimization problem.

Lemma 4. *The input distribution that maximizes $I(\Pi_\mathsf{A}; \Pi_i | \Pi_\mathsf{E})$ is the one which is uniform over all subspaces having the same dimension.*

Proof: By the concavity of $I(\Pi_\mathsf{A}; \Pi_i | \Pi_\mathsf{E})$ with respect to P_{Π_A}, that is stated in Lemma 2, the proof follows by an argument very similar to [7, Lemma 8]. ∎

Lemma 5. *Asymptotically in the field size, we have*

$$\max_{P_{X_\mathsf{A}}} I(X_\mathsf{A}; X_i | X_\mathsf{E}) = \max_{P_{\Pi_\mathsf{A}}} I(\Pi_\mathsf{A}; \Pi_i | \Pi_\mathsf{E}) =$$
$$(\min[n_\mathsf{A}, n_i + n_\mathsf{E}] - n_\mathsf{E}) (\ell - \min[n_\mathsf{A}, n_i + n_\mathsf{E}]) \log q.$$

Proof: For the proof refer to [16]. ∎

Thus, by using the upper bound given in (4) and Lemma 5 we have the following result for the upper bound on the secret key generation rate, as stated in Theorem 2.

Theorem 2. *The secret key generation rate in a non-coherent network coding scenario, which is defined in §II-C, is asymptotically (in the field size) upper bounded by*

$$C_s \leq$$
$$\min_{i \in [1:m]} \left[(\min[n_\mathsf{A}, n_i + n_\mathsf{E}] - n_\mathsf{E}) (\ell - \min[n_\mathsf{A}, n_i + n_\mathsf{E}]) \right] \log q.$$

Remark: Note that if $n_\mathsf{E} = n_\mathsf{A}$ then the secret key generation rate is zero because Eve is so powerful that she overhears all of the transmitted information.

IV. ASYMPTOTIC ACHIEVABILITY SCHEME

Here in this section, we describe our achievability scheme for the secret key sharing problem among multiple terminals in a non-coherent network coding setup.

Without loss of generality, let us assume that[4] $n_\mathsf{A} < \ell$. Moreover, in this work we focus on the asymptotic regime where the field size is large. Suppose that Alice broadcasts a message $X_\mathsf{A}[t]$ at time-slot t of the following form

$$X_\mathsf{A}[t] = \begin{bmatrix} I_{n_\mathsf{A} \times n_\mathsf{A}} & M[t] \end{bmatrix}, \tag{5}$$

where $M[t] \in \mathbb{F}_q^{n_\mathsf{A} \times (\ell - n_\mathsf{A})}$ is a uniformly at random distributed matrix. The rest of legitimate terminals and Eve receive a linear transformed version of $X_\mathsf{A}[t]$ according to the channel introduced in (1).

For each terminal $r \in \{\mathsf{A}, 1, \ldots, m, \mathsf{E}\}$, we define the subspace $\Pi_r \triangleq \langle X_r \rangle$. Then, for every $r \neq \mathsf{A}$ we have $\Pi_r \sqsubseteq \Pi_\mathsf{A}$. Because of (5), after broadcasting $X_\mathsf{A}[t]$, the legitimate terminals learn the channel state and reveal the channel transfer matrices $F_r[t]$, $r \in [1 : m]$, publicly over the public channel. Thus Alice can also recover the subspaces Π_r for all of the legitimate terminals.

Now, for each non-empty subset $\mathcal{J} \subseteq [1 : m]$ of legitimate receivers, let us define the subspace $U_\mathcal{J}$ as follows

$$U_\mathcal{J} \triangleq \Pi_\mathcal{J} \setminus_s \left(\sum_{i \in \mathcal{J}^c} \Pi_{i\mathcal{J}} + \Pi_{\mathsf{E}\mathcal{J}} \right), \tag{6}$$

where $\Pi_\mathcal{J} = \cap_{i \in \mathcal{J}} \Pi_i$, $\Pi_{i\mathcal{J}} = \Pi_i \cap \Pi_\mathcal{J}$, and $\Pi_{\mathsf{E}\mathcal{J}} = \Pi_\mathsf{E} \cap \Pi_\mathcal{J}$. By definition, $U_\mathcal{J}$ is the common subspace among the receivers in $\mathcal{J}$ which is orthogonal to all of the subspaces of other terminals, i.e., it is orthogonal to Π_i, $i \in \mathcal{J}^c$, and Π_E (see also Fig. 1). Note that the subspaces $U_\mathcal{J}$'s are not uniquely defined. However, from the definition of the operator "$\setminus_s$", it

---

[4]If $n_\mathsf{A} \geq \ell$ then Alice can reduce the number of injected packets into the network from n_A to some smaller number n'_A where $n'_\mathsf{A} < \ell$.

can be easily shown that the dimension of each $U_{\mathcal{J}}$ is uniquely determined and equal to

$$\dim(U_{\mathcal{J}}) = \dim(\Pi_{\mathcal{J}}) - \dim\left(\sum_{i \in \mathcal{J}^c} \Pi_{i\mathcal{J}} + \Pi_{\mathsf{E}\mathcal{J}}\right). \quad (7)$$

If Alice had the subspace Π_{E} observed by Eve, she would be able to construct subspaces $U_{\mathcal{J}}$'s; but she does not have Π_{E}. However, because the subspaces Π_i's and Π_{E} are chosen independently and uniformly at random from Π_{A}, and because the field size q is large, Alice, by applying Lemma 1, can find the dimension of each $U_{\mathcal{J}}$ w.h.p. Then it can be easily observed that (e.g., see [12, Lemma 3]) if Alice chooses a uniformly at random subspace of $\Pi_{\mathcal{J}}$ with dimension $\dim(U_{\mathcal{J}})$ then it satisfies (6) w.h.p., so it can be a possible candidate for $U_{\mathcal{J}}$.

Now, consider $2^m - 1$ different non-empty subsets of $[1 : m]$. To each subset $\emptyset \neq \mathcal{J} \subseteq [1 : m]$, we assign a parameter $\theta_{\mathcal{J}} \geq 0$ such that the following set of inequalities hold,

$$\theta_{\mathcal{J}_1} + \cdots + \theta_{\mathcal{J}_k} \leq \dim(U_{\mathcal{J}_1} + \cdots + U_{\mathcal{J}_k} + \Pi_{\mathsf{E}}) - \dim(\Pi_{\mathsf{E}}), \quad (8)$$

for any $k \in [1 : 2^{(2^m - 1)} - 1]$ and any different selection of subsets $\mathcal{J}_1, \ldots, \mathcal{J}_k$. Note that the right hand side of the inequalities defined in (8) depend on the actual choice of subspaces $U_{\mathcal{J}}$'s. But, as described above, in the following we assume that $U_{\mathcal{J}}$'s are chosen uniformly at random from $\Pi_{\mathcal{J}}$.

If Alice knows the subspace Π_{E}, then we can state the following result.

Lemma 6. *There exists subspaces $U'_{\mathcal{J}} \sqsubseteq U_{\mathcal{J}}$ such that $\dim(U'_{\mathcal{J}}) = \theta_{\mathcal{J}}$ for all $\emptyset \neq \mathcal{J} \subseteq [1 : m]$, and $U'_{\mathcal{J}}$'s and Π_{E} are orthogonal subspaces (i.e., $\dim(\Pi_{\mathsf{E}} + \sum_i U'_{\mathcal{J}_i}) = \dim(\Pi_{\mathsf{E}}) + \sum_i \theta_{\mathcal{J}_i}$) if and only if $\theta_{\mathcal{J}}$'s are non-negative integers and satisfy (8).*

Proof: The proof of this lemma is based on [17, Lemma 4] and can be found in [16]. ■

Fig.1 depicts pictorially the relation between subspaces introduced in the above discussions.
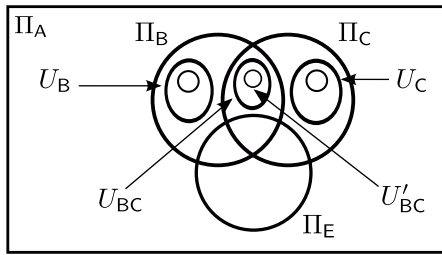

Fig. 1. The relations between subspaces Π's, U's, and U''s for the case of $m = 2$.

Although in practice Alice only knows the dimension of Π_{E} (w.h.p.), but still she can find subspaces $U'_{\mathcal{J}} \sqsubseteq U_{\mathcal{J}}$ such that the result of Lemma 6 holds w.h.p., as stated in Lemma 7.

Lemma 7. *Alice can find subspaces $U'_{\mathcal{J}} \sqsubseteq U_{\mathcal{J}}$ such that $\dim(U'_{\mathcal{J}}) = \theta_{\mathcal{J}}$ for all $\emptyset \neq \mathcal{J} \subseteq [1 : m]$, and $U'_{\mathcal{J}}$'s are orthogonal subspaces and $U'_{\mathcal{J}}$'s and Π_{E} are orthogonal*

subspaces w.h.p., if and only if $\theta_{\mathcal{J}}$'s are non-negative integers and satisfy (8).

Proof: For the proof refer to [16]. ■

Then, we have the following result.

Theorem 3. *The secret key sharing rate given by the solution of the following convex optimization problem can be asymptotically (in the field size) achieved*

maximize $\quad \left[\min_{r \in [1:m]} \sum_{\mathcal{J} \ni r} \theta_{\mathcal{J}}\right] (\ell - n_{\mathsf{A}}) \log q$
subject to $\quad \theta_{\mathcal{J}} \geq 0, \quad \forall \mathcal{J} \subseteq [1 : m], \ \mathcal{J} \neq \emptyset, \quad$ and
$\quad\quad\quad \theta_{\mathcal{J}_1} + \cdots + \theta_{\mathcal{J}_k} \leq$
$\quad\quad\quad\quad \dim(U_{\mathcal{J}_1} + \cdots + U_{\mathcal{J}_k} + \Pi_{\mathsf{E}}) - \dim(\Pi_{\mathsf{E}})$
$\quad\quad\quad \forall k, \ \forall \mathcal{J}_1, \ldots, \mathcal{J}_k : \ \emptyset \neq \mathcal{J}_i \subseteq [1 : m],$
$\quad\quad\quad \mathcal{J}_i \neq \mathcal{J}_j \text{ if } i \neq j,$

where for every $\mathcal{J}$, $U_{\mathcal{J}}$ is chosen uniformly at random from $\Pi_{\mathcal{J}}$ with the dimension calculated by (7) under the assumption that $\Pi_1, \ldots, \Pi_m$, and Π_{E} are selected independently and uniformly at random from Π_{A} with dimensions $n_1, \ldots, n_m, n_{\mathsf{E}}$.

Proof of Theorem 3: Let Alice use the broadcast channel N times by sending matrices $X_{\mathsf{A}}[1], \ldots, X_{\mathsf{A}}[N]$ of the form (5). As mentioned before, in every time-slot t, each of the legitimate terminals sends publicly the channel transfer matrix it has received.

Then, let us define $\hat{\theta}_{\mathcal{J}} \triangleq \lfloor N\theta_{\mathcal{J}} \rfloor$ for all $\mathcal{J}$ and consider the following set of inequalities

$$\hat{\theta}_{\mathcal{J}_1} + \cdots + \hat{\theta}_{\mathcal{J}_k} + N\dim(\Pi_{\mathsf{E}}) \leq$$
$$\dim\left(\bigoplus_{t=1}^{N} U_{\mathcal{J}_1}[t] + \cdots + \bigoplus_{t=1}^{N} U_{\mathcal{J}_k}[t] + \bigoplus_{t=1}^{N} \Pi_{\mathsf{E}}[t]\right), \quad (9)$$

where "$\oplus$" is the direct sum operator. Each of $\hat{U}_{\mathcal{J}_i} \triangleq \bigoplus_{t=1}^{N} U_{\mathcal{J}_i}[t]$ is a subspace of an $N \times n_{\mathsf{A}}$ dimensional space $\bigoplus_{t=1}^{N} \Pi_{\mathsf{A}}[t]$. Similarly, we have $\hat{\Pi}_{\mathsf{E}} \sqsubseteq \bigoplus_{t=1}^{N} \Pi_{\mathsf{A}}[t]$ where $\hat{\Pi}_{\mathsf{E}} \triangleq \bigoplus_{t=1}^{N} \Pi_{\mathsf{E}}[t]$. It can be easily seen that if the set of inequalities (8) are satisfied then the set of inequalities (9) are also satisfied.

Now, by using Lemma 7, Alice can find a set of orthogonal subspaces $\hat{U}'_{\mathcal{J}}$ with dimension $\hat{\theta}_{\mathcal{J}}$ (that are also orthogonal to $\hat{\Pi}_{\mathsf{E}}$ w.h.p.). By applying Lemma 8 (appeared after this theorem), one would observe that if Alice uses a basis of $\hat{U}'_{\mathcal{J}}$ ($\hat{\theta}_{\mathcal{J}}$ linear independent vectors from $\hat{U}'_{\mathcal{J}}$) to share a secret key $\mathcal{K}_{\mathcal{J}}$ with all terminals in $\mathcal{J}$, then this key is secure from Eve and all other legitimate terminals in $\mathcal{J}^c$ w.h.p. Using each key $\mathcal{K}_{\mathcal{J}}$, Alice can send a message of size $\hat{\theta}_{\mathcal{J}}(\ell - n_{\mathsf{A}}) \log q$ secretly to the terminals in $\mathcal{J}$. In order to share the key $\mathcal{K}_{\mathcal{J}}$, Alice sends publicly a set of coefficients for each terminal in $\mathcal{J}$ so that each of them can construct the subspace $\hat{U}_{\mathcal{J}}$ from their own received subspace. Note that even having these coefficients, Eve cannot recover any information regarding $\mathcal{K}_{\mathcal{J}}$ (for more discussion see [13]).

Up until now, the problem of sharing a key $\mathcal{K}$ among legitimate terminals have been reduced to a multicast problem where Alice would like to transmit a message (i.e., the shared key $\mathcal{K}$) to a set of terminal where the rth one has a min-cut

$\sum_{\mathcal{J} \ni r} \hat{\theta}_{\mathcal{J}}$. From the main theorem of network coding (e.g., see [2], [3], [18], [19]), we know that this problem can be solved by performing linear network coding where the achievable rate is as follows

$$R_s \leq \left[\frac{1}{N} \min_{r \in [1:m]} \sum_{\mathcal{J} \ni r} \hat{\theta}_{\mathcal{J}} \right] (\ell - n_{\mathsf{A}}) \log q.$$

By increasing N, the achievable secrecy rate will be arbitrarily close to $R_s \leq \left[\min_{r \in [1:m]} \sum_{\mathcal{J} \ni r} \theta_{\mathcal{J}} \right] (\ell - n_{\mathsf{A}}) \log q$, and we are done. ∎

Lemma 8. *Consider a set of n_{A} packets denoted by the rows of a matrix $X_{\mathsf{A}} \in \mathbb{F}_q^{n_{\mathsf{A}} \times \ell}$ of the form $X_{\mathsf{A}} = [I \quad M]$, where $M \sim \mathsf{Uni} \left(\mathbb{F}_q^{n_{\mathsf{A}} \times (\ell - n_{\mathsf{A}})} \right)$. Assume that Eve has overheard n_{E} independent linear combinations of these packets, represented by the rows of a matrix $X_{\mathsf{E}} \in \mathbb{F}_q^{n_{\mathsf{E}} \times \ell}$. Then for every k packets $y_1, \ldots, y_k$ that are linear combinations of the rows of X_{A}, if the subspace $\Pi_Y = \langle y_1, \ldots, y_k \rangle$ is orthogonal to $\langle X_{\mathsf{E}} \rangle$ we have $I(y_1, \ldots, y_k; X_{\mathsf{E}}) = 0$.*

Proof: The proof is stated in [16, Appendix B]. ∎

A. Special Case: Achievability Scheme for Two Terminals

For simplicity and without loss of generality we assume that $n_{\mathsf{B}} \leq n_{\mathsf{A}}$ and $n_{\mathsf{E}} \leq n_{\mathsf{A}}$. The key generation scheme starts by Alice broadcasting a message $X_{\mathsf{A}}[t]$ at time t of the form of (5). Then, Theorem 3 states that the secrecy rate R_s is achievable if

$$R_s \leq [\dim(U_{\mathsf{B}} + \Pi_{\mathsf{E}}) - \dim(\Pi_{\mathsf{E}})] (\ell - n_{\mathsf{A}}) \log q,$$

where $U_{\mathsf{B}} = \Pi_{\mathsf{B}} \setminus_s \Pi_{\mathsf{E}}$ (for convenience we have replaced $U_{\{\mathsf{B}\}}$ with U_{B}). Because $U_{\mathsf{B}} \cap \Pi_{\mathsf{E}} = \{\mathbf{0}\}$, we have

$$\begin{aligned} R_s &\leq [\dim(U_{\mathsf{B}})] (\ell - n_{\mathsf{A}}) \log q \\ &= [\dim(\Pi_{\mathsf{B}}) - \dim(\Pi_{\mathsf{B}} \cap \Pi_{\mathsf{E}})] (\ell - n_{\mathsf{A}}) \log q \\ &= \left[n_{\mathsf{B}} - (n_{\mathsf{B}} + n_{\mathsf{E}} - n_{\mathsf{A}})^+ \right] (\ell - n_{\mathsf{A}}) \log q \\ &= [\min[n_{\mathsf{A}}, n_{\mathsf{B}} + n_{\mathsf{E}}] - n_{\mathsf{E}}] (\ell - n_{\mathsf{A}}) \log q, \end{aligned}$$

where this is the same as the upper bound given in Theorem 2. This is obvious when $n_{\mathsf{A}} \leq n_{\mathsf{B}} + n_{\mathsf{E}}$. On the other hand, if $n_{\mathsf{A}} > n_{\mathsf{B}} + n_{\mathsf{E}}$, then Alice can reduce the number of injected packets in every time-slot from n_{A} to $n_{\mathsf{B}} + n_{\mathsf{E}}$ (there is no need to use more than $n_{\mathsf{B}} + n_{\mathsf{E}}$ degrees of freedom).

Remark: Note that in the above scheme, as long as $n_{\mathsf{E}} < n_{\mathsf{A}}$, the secrecy rate is non-zero.

Now, we compare the derived secrecy rate with the case where no feedback is allowed. First let us assume that $n_{\mathsf{B}} \geq n_{\mathsf{E}}$. Then, in the non-coherent network coding scenario introduced in §II-C, it can be easily verified that the channel from Alice to Eve is a *stochastically degraded* (for the definition refer to [20, p. 373]) version of the channel from Alice to Bob.

So by applying the result of [21] or [22, Theorem 3], for the secret key sharing capacity we can write

$$\begin{aligned} C_s &= \max_{P_{X_{\mathsf{A}}}} [I(X_{\mathsf{A}}; X_{\mathsf{B}}) - I(X_{\mathsf{A}}; X_{\mathsf{E}})] \\ &= \max_{P_{\Pi_{\mathsf{A}}}} [I(\Pi_{\mathsf{A}}; \Pi_{\mathsf{B}}) - I(\Pi_{\mathsf{A}}; \Pi_{\mathsf{E}})], \end{aligned}$$

where the sufficiency of optimization over subspaces follows from a similar argument to [7, Theorem 1]. Similar to the proof of Lemma 5, one can show that

$$C_s = [n_{\mathsf{B}} - n_{\mathsf{E}}]^+ (\ell - n_{\mathsf{B}}) \log q,$$

which is positive only if $n_{\mathsf{B}} > n_{\mathsf{E}}$. ∎

The above comparison demonstrates the amount of improvement of the secret key generation rate we might gain by using feedback.

B. Special Case: Achievability Scheme for Three Terminals

As an another example, here we consider the three trusted terminals problem (i.e., $m = 2$). As before, we assume that $n_{\mathsf{A}} < \ell$ and for the convenience we suppose that $n_{\mathsf{B}} = n_{\mathsf{C}} \leq n_{\mathsf{A}}$ and $n_{\mathsf{E}} \leq n_{\mathsf{A}}$.

In order to characterize the achievable secrecy rate, we need to find the dimension of subspaces U_{B}, U_{C}, and U_{BC} and their sums (including Π_{E} as well). We assume that the field size q is large and we know that Π_{B}, Π_{C}, and Π_{E} are chosen uniformly at random from Π_{A}. Subspaces Π_{BC} and Π_{BE} are also distributed independently and uniformly at random in Π_{B}. Similarly, the same is true for Π_{BC} and Π_{CE} in Π_{C}. We have

$$\begin{cases} U_{\mathsf{B}} \triangleq \Pi_{\mathsf{B}} \setminus_s (\Pi_{\mathsf{BC}} + \Pi_{\mathsf{BE}}) \\ U_{\mathsf{C}} \triangleq \Pi_{\mathsf{C}} \setminus_s (\Pi_{\mathsf{BC}} + \Pi_{\mathsf{CE}}) \\ U_{\mathsf{BC}} \triangleq \Pi_{\mathsf{BC}} \setminus_s (\Pi_{\mathsf{BCE}}), \end{cases}$$

so we can write

$$\begin{aligned} \dim(U_{\mathsf{B}}) &= \dim(\Pi_{\mathsf{B}}) - \dim(\Pi_{\mathsf{BC}} + \Pi_{\mathsf{BE}}) \\ &\overset{(a)}{=} \dim(\Pi_{\mathsf{B}}) - \min\left[\dim(\Pi_{\mathsf{BC}}) + \dim(\Pi_{\mathsf{BE}}), \dim(\Pi_{\mathsf{B}})\right] \\ &\overset{(b)}{=} n_{\mathsf{B}} - \min\left[\dim(\Pi_{\mathsf{BC}}) + \dim(\Pi_{\mathsf{BE}}), n_{\mathsf{B}}\right] \\ &= [n_{\mathsf{B}} - \dim(\Pi_{\mathsf{BC}}) - \dim(\Pi_{\mathsf{BE}})]^+ \\ &\overset{(c)}{=} \left[n_{\mathsf{B}} - (2n_{\mathsf{B}} - n_{\mathsf{A}})^+ - (n_{\mathsf{B}} + n_{\mathsf{E}} - n_{\mathsf{A}})^+ \right]^+, \end{aligned}$$

where (a) follows from Lemma 1 because Π_{BC} and Π_{BE} are chosen independently and uniformly at random from Π_{B}, (b) is true because q is large, and (c) follows from Lemma 1. Note that because we have assumed $n_{\mathsf{B}} = n_{\mathsf{C}}$ it follows that $\dim(U_{\mathsf{C}}) = \dim(U_{\mathsf{B}})$.

Similarly, for the dimension of U_{BC} we can write

$$\begin{aligned} \dim(U_{\mathsf{BC}}) &= \dim(\Pi_{\mathsf{BC}}) - \dim(\Pi_{\mathsf{BCE}}) \\ &= \dim(\Pi_{\mathsf{BC}}) - [\dim(\Pi_{\mathsf{BC}}) + n_{\mathsf{E}} - n_{\mathsf{A}}]^+ \\ &= \min \left[n_{\mathsf{A}} - n_{\mathsf{E}}, (2n_{\mathsf{B}} - n_{\mathsf{A}})^+ \right]. \end{aligned}$$

Proposition 1. *From the construction, the subspaces U_{B}, U_{C}, and U_{BC} are orthogonal and similarly the same holds for U_{B}, U_{BC}, and Π_{E}. Also U_{C}, U_{BC}, and Π_{E} are orthogonal w.h.p.*

Now we may write the linear program stated in Theorem 3 as follows

$$\begin{array}{ll} \text{maximize} & \min\left[\theta_{\mathsf{B}} + \theta_{\mathsf{BC}}, \theta_{\mathsf{C}} + \theta_{\mathsf{BC}}\right] (\ell - n_{\mathsf{A}}) \log q \\ \text{subject to} & \theta_{\mathsf{B}} \leq \dim(U_{\mathsf{B}} + \Pi_{\mathsf{E}}) - n_{\mathsf{E}} \\ & \theta_{\mathsf{C}} \leq \dim(U_{\mathsf{C}} + \Pi_{\mathsf{E}}) - n_{\mathsf{E}} \\ & \theta_{\mathsf{BC}} \leq \dim(U_{\mathsf{BC}} + \Pi_{\mathsf{E}}) - n_{\mathsf{E}} \\ & \theta_{\mathsf{B}} + \theta_{\mathsf{C}} \leq \dim(U_{\mathsf{B}} + U_{\mathsf{C}} + \Pi_{\mathsf{E}}) - n_{\mathsf{E}} \\ & \theta_{\mathsf{B}} + \theta_{\mathsf{C}} + \theta_{\mathsf{BC}} \leq \dim(U_{\mathsf{B}} + U_{\mathsf{C}} + U_{\mathsf{BC}} + \Pi_{\mathsf{E}}) - n_{\mathsf{E}}. \end{array}$$

Because of the symmetry in the problem ($n_B = n_C$), for the optimal solution we should have $\theta_B = \theta_C$. Knowing this and using Proposition 1, we may further simplify the above linear program as follows

maximize $\quad [\theta_B + \theta_{BC}] (\ell - n_A) \log q$
subject to $\quad \theta_B \le \frac{1}{2} [\dim(U_B + U_C + \Pi_E) - n_E] \triangleq \alpha_1$
$\qquad\qquad \theta_{BC} \le \dim(U_{BC}) \triangleq \alpha_2$
$\qquad\qquad 2\theta_B + \theta_{BC} \le \dim(U_B + U_C + U_{BC} + \Pi_E) - n_E \triangleq \alpha_3.$

From the definitions of α's, we can easily observe that, $\alpha_3 \ge 2\alpha_1$, $\alpha_3 \ge \alpha_2$, and $\alpha_3 \le 2\alpha_1 + \alpha_2$. Hence, $\theta_B + \theta_{BC}$ gets its maximum at the point $(\theta_B, \theta_{BC}) = (\frac{\alpha_3 - \alpha_2}{2}, \alpha_2)$. Thus, for the maximum achievable secrecy rate we have

$$R_s = \left[\frac{\alpha_2 + \alpha_3}{2} \right] (\ell - n_A) \log q.$$

As mentioned before, we assume that subspaces $U_{\mathcal{J}}$'s are chosen uniformly at random from $\Pi_{\mathcal{J}}$. So Π_E and $U_{\mathcal{J}}$'s are independent and for α_3 we can write

$\alpha_3 = \min[\dim(U_B) + \dim(U_C) + \dim(U_{BC}) + \dim(\Pi_E), n_A] - n_E$
$\quad = \min[\dim(U_B) + \dim(U_C) + \dim(U_{BC}), n_A - n_E]$
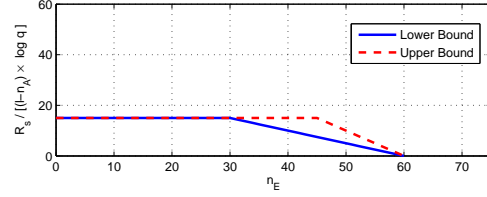$\quad = \min[2\dim(U_B) + \dim(U_{BC}), n_A - n_E].$

So for the secrecy rate (achievable asymptotically when q goes to infinity) we have

$$R_s/(\ell - n_A) \log q =$$
$$\min \left[\dim(U_B) + \dim(U_{BC}), \frac{1}{2} \left(n_A + \dim(U_{BC}) - n_E \right) \right]. \quad (10)$$
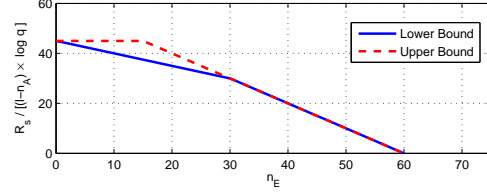
Example 1. *As an example, here we compare the achievable secret key sharing rate among three legitimate terminals (i.e., $m = 2$) as derived in (10) with the upper bound stated in Theorem 2. We consider two symmetric setup where for the first one we have $n_A = 60$, $n_B = n_C = 15$ (see Fig. 2(a)) and for the second one we have $n_A = 60$, $n_B = n_C = 45$ (see Fig. 2(b)). In each of these situations, we depict the upper and lower bounds on the secret key generation rate as a function of the number of packets (degrees of freedom) received by Eve.*

(a) $m = 2$, $n_A = 60$, and $n_B = n_C = 15$.

(b) $m = 2$, $n_A = 60$, and $n_B = n_C = 45$.

Fig. 2. A comparison between the achievable secrecy rate of Theorem 3 and the upper bound given by Theorem 2 for two cases: (a) when $m = 2$, $n_A = 60$, and $n_B = n_C = 15$ and (b) when $m = 2$, $n_A = 60$, and $n_B = n_C = 45$.

REFERENCES

[1] N. Cai and R. W. Yeung, "Secure network coding," *IEEE International Symposium on Information Theory (ISIT)*, p. 323, 2002.
[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, pp. 1204–1216, Jul. 2000.
[3] S.-Y. R. Li, R. W. Yeung, and N. Cai., "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
[4] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," *Allerton Conference on Communication, Control, and Computing*, Sep. 2004.
[5] S. Y. E. Rouayheb and E. Soljanin, "On wiretap networks ii," *IEEE International Symposium on Information Theory (ISIT)*, pp. 551–555, Jun. 2007.
[6] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.
[7] M. Jafari Siavoshani, S. Mohajer, C. Fragouli, and S. N. Diggavi, "On the capacity of non-coherent network coding," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1046–1066, Feb. 2011.
[8] D. Silva, F. R. Kschischang, and R. Koetter, "Communication over finite-field matrix channels," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1296–1305, Mar. 2010.
[9] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.
[10] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - part i," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.
[11] ——, "Information-theoretic key agreement of multiple terminals - part ii: Channel model," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3997–4010, Aug. 2010.
[12] M. Jafari Siavoshani, C. Fragouli, and S. N. Diggavi, "Subspace properties of network coding and their applications," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2599–2619, May 2012.
[13] M. Jafari Siavoshani, C. Fragouli, S. N. Diggavi, U. Pulleti, and K. Argyraki, "Group secret key generation over broadcast erasure channels," *Asilomar Conference on Signals, Systems, and Computers*, pp. 719–723, Nov. 2010.
[14] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[15] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, part i: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[16] M. Jafari Siavoshani and C. Fragouli, "Multi-terminal secrecy in a linear non-coherent packetized networks," *EPFL Technical Report*, 2012, [Online]. Available: http://infoscience.epfl.ch/record/175547.
[17] M. A. Khojastepour and A. Keshavarz-Haddad, "Multicast achievable rate region of deterministic broadcast channel," *IEEE International Conference on Communications (ICC)*, 2011.
[18] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
[19] C. Fragouli and E. Soljanin, "Network coding fundamentals," in *Monograph in Series, Foundations and Trends in Networking*. Now Publishers, Jun. 2007.
[20] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
[21] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
[22] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.