On Secure Network Coding for Multiple Unicast Traffic

Gaurav Kumar Agarwal, Martina Cardone, and Christina Fragouli, *Fellow, IEEE*

***Abstract*— This paper investigates the problem of secure communication in a wireline noiseless scenario where a source wishes to communicate to a number of destinations in the presence of a passive external adversary. Different from the multicast scenario, where all destinations are interested in receiving the same message, in this setting different destinations are interested in different messages. The main focus of this paper is on characterizing the secure capacity region, when the adversary has unbounded computational capabilities, but limited network presence. Towards this end, an outer bound on the secure capacity region is derived, and secure transmission schemes are designed and analyzed in terms of achieved rate performance. It is first shown that, for the case of two destinations, the designed scheme matches the outer bound, hence characterizing the secure capacity region. Then, a particular class of networks referred to as *two-layer* networks is considered, where the source communicates with the destinations by hopping information through one layer of relays. It is shown that the designed scheme is indeed capacity achieving for any two-layer network for which one of the following three conditions is satisfied: (i) the number of destinations is three, (ii) the number of edges eavesdropped by the adversary is one, (iii) the min-cut capacities assume specific values. It is also shown that two-layer networks can be used to model and study a more general class of networks, referred to as *separable*. The key feature of separable networks is that they can be partitioned into edge disjoint networks that satisfy specific min-cut properties. In particular, it is proved that the secure capacity region of any separable network can be characterized from the secure capacity region of the corresponding two-layer network. Finally, for an arbitrary network topology, a two-phase scheme is designed and its rate performance is compared with the capacity-achieving scheme for networks with two destinations.**

***Index Terms*— Network coding, physical layer, information security.**

Manuscript received July 26, 2018; revised December 28, 2019; accepted March 6, 2020. Date of publication March 17, 2020; date of current version July 14, 2020. This work was supported in part by NSF Award under Grant 1740047 and Grant 1954800, and in part by UC-NL under Grant LFR-18-548554. This article was presented in part at the 10th International Conference on Information Theoretic Security. *(Corresponding author: Gaurav Kumar Agarwal.)*

Gaurav Kumar Agarwal was with the Electrical and Computer Engineering Department, University of California, Los Angeles (UCLA), Los Angeles, CA 90095 USA. He is now with Google, Mountain View, CA 94043 USA (e-mail: gauravagarwal@ucla.edu).

Martina Cardone is with the Electrical and Computer Engineering Department, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: cardo089@umn.edu).

Christina Fragouli is with the Electrical and Computer Engineering Department, University of California, Los Angeles (UCLA), Los Angeles, CA 90095 USA (e-mail: christina.fragouli@ucla.edu).

Communicated by P. Mitran, Associate Editor for Communications.

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

Digital Object Identifier 10.1109/TIT.2020.2981325

I. Introduction

SECURE network coding [1] considers the communication from a source to a number of destinations in the presence of a passive external adversary, with unbounded computational capabilities, but limited network presence. The work in [1] showed that the source can securely multicast to all destinations at a rate of $M-k$, where M is the min-cut capacity between the source and each destination, and k is the number of edges eavesdropped by the adversary. In such a multicast scenario, all destinations are interested in receiving the same message.

In this paper, we focus on multiple unicast traffic, where a source wishes to securely communicate to a number of destinations, each interested in an independent message. Our primal objective lies in characterizing the secure capacity region, by means of derivation of novel outer bounds as well as design of polynomial-time transmission schemes.

A. Related Work

Network coding was pioneered by the seminal work of Ahlswede *et al.* [2]. The authors proved that, if M is the min-cut capacity from the source to each destination, then the source can multicast at a rate M to all the destinations. This result implies that, even if a single destination with min-cut capacity M has access to the entire network resources, this destination can only receive at most at a rate equal to M. Moreover, this result shows that multiple destinations sharing some of the network resources, can still receive at a rate M if they are interested in the exact same information. Later, Li *et al.* [3] proved that it suffices to use random linear coding operations to characterize the multicast capacity. Jaggi *et al.* [4] designed polynomial time deterministic algorithms aimed to achieve the multicast capacity. While for the case of single unicast and multicast traffic the capacity is well-known, the same is not true for the case of networks where multiple unicast sessions take place simultaneously and share some of the network resources. For instance, even though the cut-set bound was proved to be tight for some special cases, such as single source with non-overlapping demands and single source with non-overlapping demands and a multicast demand [5], in general it is not tight [6]. It was also recently showed by Kamath *et al.* [7] that characterizing the capacity region of a general network where two unicast sessions take place simultaneously is as hard as characterizing the capacity region of a network with an arbitrary number

of unicast sessions. For the case of single source and two destinations with a non-overlapping demand and a multicast demand, Ramamoorthy and Wesel [8] proposed a nice graph theoretical approach to characterize the capacity region.

Information theoretic security, pioneered by Shannon [9], aims at ensuring a reliable and secure communication among trusted parties inside a network such that a passive external eavesdropper does not learn anything about the content of the information exchanged. For point-to-point channels, information theoretic security can be achieved provided that the communicating trusted parties have a pre-shared key of entropy at least equal to the length of the message [9]. Wyner [10] showed that, if the adversary's channel is a degraded version of the channel to the legitimate destination, then an information theoretic secure communication can be guaranteed even without the pre-shared keys. Moreover, if public feedback is available, Czap *et al.* [11] showed that secure communication can be ensured over erasure networks even when the adversary has a channel of better quality than the legitimate receiver. In [1], Cai et al. characterized the information theoretic secure capacity of a noiseless network with unit capacity edges and with multicast traffic. In this work, which was followed by several others [12], [13], a source wishes to multicast the same information to a number of destinations in the presence of a passive external adversary eavesdropping any k edges of her choice. In [14], Cui et al. studied networks with non-uniform edge capacities when the adversary is allowed to eavesdrop only some specific subsets of edges. For a given linear network code, the notion of generalized Network Hamming weights (GNHW) was defined in [15]. It was shown that the GNHM characterize the information that the adversary has about the messages, as a function of the number of edges eavesdropped. The GNHW are extension of generalized Hamming weights (GHW) for linear codes proposed in [16]. Over the past few years, other notions of information theoretic security have been analyzed, such as the case of weak information theoretic security [17]–[19]. Moreover, several different scenarios have been studied, that include: (i) the case of an active adversary, who can indeed corrupt the communication rather than just passively eavesdropping it [20]–[22]; (ii) erasure networks where a public feedback is available [23]–[25]; (iii) wireless networks [26], [27].

To the best of our knowledge, our work is the first to consider securing private messages over networks. In [28], we considered sending private messages over butterfly-like erasure networks; in [29], we considered noiseless networks with two sources and two destinations where the network topology was derived from the butterfly network; in [30], we considered arbitrary networks for two destinations, and also designed suboptimal schemes for arbitrary network configurations. These results are in part included and extended in this paper. Independently from our work, in [31], the authors studied adaptive and active attacks and also considered multiple multicast traffic over a layered network structure, with arbitrary number of layers. However, different to this paper, every node in one layer is connected to every node in the next layer.

B. Contributions

In this paper, we study the problem of characterizing the secure capacity region of a wireline noiseless multiple unicast scenario with uniform edge capacities. In particular, we focus on networks where a source wishes to securely communicate to a number of destinations, each interested in a different message. Our main contributions can be summarized as follows:

1) We derive an outer bound on the secure capacity region for networks with arbitrary topology and arbitrary number of destinations. Similar to the multicast scenario [1], this outer bound depends on the number of edges that the adversary eavesdrops and on the min-cut capacities between the source and different subsets of destinations.
2) We characterize the secure capacity region for networks with arbitrary topology and with two destinations. Towards this end, we design a secure transmission scheme whose achieved rate region is proved to match the derived outer bound. In particular, we leverage a key property, referred to as *separability* [8], in order to select the parts of the network over which: (i) common keys should be multicast, and (ii) encrypted private messages should be communicated. Our analysis shows that coding across different unicast sessions helps in characterizing the secure capacity even in scenarios where coding was not required in the absence of an adversary.
3) We design a secure polynomial-time transmission scheme for two-layer networks, where the source communicates with the destinations by hopping information through a layer of relays. A key feature of such networks is that they satisfy the separability property over graphs. Our scheme is proved to achieve the secure capacity region when any one of the three following conditions is satisfied: (i) the number of destinations is three, (ii) the adversary eavesdrops any one edge of the network, (iii) the min-cut capacities assume certain values. Moreover, we verify through numerical simulations of 100 randomly constructed two-layer networks that the designed scheme matches the outer bound for networks with arbitrary number of destinations and eavesdropped edges. Thus, the scheme is conjectured to be capacity achieving for any two-layer network.
4) We prove that any network satisfying the separability property can be modeled as a two-layer network. More importantly, we show that the secure capacity region of any separable network can be characterized from the secure capacity region of the corresponding two-layer network, which we refer to as the child two-layer network. In particular, to prove this result, we propose a deterministic mapping from a secure scheme for the child two-layer network to a secure scheme for the corresponding separable network.
5) We design a secure polynomial-time transmission scheme for networks with arbitrary topology and arbitrary number of destinations. In particular, our scheme works in two phases: in the first phase, we multicast keys using the entire network resources, and in the

second phase we communicate encrypted private message packets using again the entire network resources. We also compare the rate region achieved by this scheme with the secure capacity region of networks with two destinations. This scheme is suboptimal, but it offers a yardstick for the secure rate performance that can be attained over multiple unicast networks with single source, but arbitrary topology. Moreover, in both phases, the scheme obliviously uses all the network resources, i.e., it does not try to optimally "separate" the information and key flows by leveraging the specific structure of the network (which is indeed the case for the capacity achieving scheme for two destinations). Although this characteristic causes the scheme to be suboptimal, it also makes it easy to implement.

6) We draw several observations on the derived secure capacity results. For instance, we show that, although the source conveys a private message to each receiver, we may need to re-use the same keys across several receivers to achieve the secure capacity. We also show that the secure capacity region for two destinations is non-reversible, which is a key difference with respect to the case when there is no adversary. Specifically, we show that, if we switch the role of the source and destinations and we reverse the directions of the edges, then the new secure capacity region differs from the original one. Moreover, for the case of two destinations, we compare the secure capacity region with the capacity region when the adversary is absent. The goal of this analysis is to quantify the rate loss that is incurred to guarantee security.

C. Paper Organization

Section II formally defines the setup, that is the multiple unicast wireline noiseless network with single source and arbitrary number of destinations, and formulates the problem. Section III derives an outer bound on the secure capacity region. Section IV provides a capacity-achieving secure transmission scheme for networks with two destinations and arbitrary topology. Section V designs a secure transmission scheme for networks with a two-layer topology and arbitrary number of destinations. Section V also derives some secure capacity results, and it shows connections between two-layer networks and separable networks. Section VI provides a two-phase achievable scheme for networks with arbitrary number of destinations and arbitrary topology. Section VII compares the derived results with the unsecure rate region, and discusses the *reversibility* property of secure multiple unicast traffic. Finally, Section VIII concludes the paper and highlights some future research directions that are object of current investigation.

II. Setup and Problem Formulation

Throughout the paper we adopt the following notation convention. Calligraphic letters indicate sets and subspaces; $\emptyset$ is the empty set and $|\mathcal{A}|$ is the cardinality of $\mathcal{A}$; for two sets $\mathcal{A}_1, \mathcal{A}_2$, $\mathcal{A}_1 \subseteq \mathcal{A}_2$ indicates that $\mathcal{A}_1$ is a subset of $\mathcal{A}_2$, $\mathcal{A}_1 \cup \mathcal{A}_2$ indicates the union of $\mathcal{A}_1$ and $\mathcal{A}_2$, $\mathcal{A}_1 \sqcup \mathcal{A}_2$ indicates the disjoint union of $\mathcal{A}_1$ and $\mathcal{A}_2$, $\mathcal{A}_1 \cap \mathcal{A}_2$ is the intersection of $\mathcal{A}_1$ and $\mathcal{A}_2$ and $\mathcal{A}_1 \backslash \mathcal{A}_2$ is the set of elements that belong to $\mathcal{A}_1$ but not to $\mathcal{A}_2$; $[n_1 : n_2]$ is the set of integers from n_1 to $n_2 \geq n_1$; $[n]$ is the set of integers from 1 to $n \geq 1$; $[x]^+ := \max\{0, x\}$ for $x \in \mathbb{R}$; for a vector a, a^T is its transpose vector; $\dim(\mathcal{N})$ is the dimension of the subspace $\mathcal{N}$; for two subspaces $\mathcal{N}_1$ and $\mathcal{N}_2$, their intersection, union and sum are defined as $\mathcal{N}_1 \cap \mathcal{N}_2 := \{\mathbf{x} : \ \mathbf{x} \in \mathcal{N}_1, \mathbf{x} \in \mathcal{N}_2\}$, $\mathcal{N}_1 \cup \mathcal{N}_2 := \{\mathbf{x} : \ \mathbf{x} \in \mathcal{N}_1 \text{ or } \mathbf{x} \in \mathcal{N}_2\}$, and $\mathcal{N}_1 + \mathcal{N}_2 := \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in \mathcal{N}_1, \mathbf{y} \in \mathcal{N}_2\}$, respectively; $0_{i \times j}$ is the all-zero matrix of dimension $i \times j$; I_j is the identity matrix of dimension j; for a matrix A of dimension $m \times n$, $rk(A)$ is the rank of A, and $A|_{\mathcal{S}}$ denotes the submatrix of A of dimension $|\mathcal{S}| \times n$ where only the rows indexed by the set $\mathcal{S} \subseteq [m]$ are retained.

We represent a wireline noiseless network with a directed acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of directed edges. The edges represent orthogonal communication links, which are interference-free. In particular, these links are discrete noiseless memoryless channels of unit capacity over a common alphabet. If an edge $e \in \mathcal{E}$ connects a node i to a node j, we refer to node i as the tail and to node j as the head of e, i.e., $\text{tail}(e) = i$ and $\text{head}(e) = j$. For each node $v \in \mathcal{V}$, we define $\mathcal{I}(v)$ as the set of all incoming edges of node v and $\mathcal{O}(v)$ as the set of all outgoing edges of node v.

In this network, there is one source node S and m destination nodes $D_i, i \in [m]$. The source node does not have any incoming edges, i.e., $\mathcal{I}(S) = \emptyset$, and each destination node does not have any outgoing edges, i.e., $\mathcal{O}(D_i) = \emptyset, \forall i \in [m]$. Source S has a message W_i for destination $D_i, i \in [m]$. These m messages are assumed to be independent. Thus, the network consists of multiple unicast traffic, where m unicast sessions take place simultaneously and share the network resources. A passive eavesdropper/adversary Eve is also present in the network and can eavesdrop any k edges of her choice. Note that this assumption implies that Eve has limited network presence; this is equivalent to a scenario where there are several *non-collaborating* adversaries, each observing a different subset of k edges. We also highlight that Eve is an external eavesdropper, i.e., she is not one of the destinations.

The symbol transmitted over n channel uses on edge $e \in \mathcal{E}$ is denoted as X_e^n. In addition, for $\mathcal{E}_t \subseteq \mathcal{E}$ we define $X_{\mathcal{E}_t}^n = \{X_e^n : e \in \mathcal{E}_t\}$. We assume that the source node S has infinite sources of randomness Θ, while the other nodes in the network do not have any randomness.

Over this network, we are interested in finding all possible feasible m-tuples $(R_1, R_2, \ldots, R_m)$ such that each destination $D_i, i \in [m]$, reliably decodes the message W_i (with zero error) and Eve receives no information about the content of the messages. In particular, we are interested in ensuring perfect information theoretic secure communication, and hence we aim at characterizing the secure capacity region, which is next formally defined.

Definition 1 (*Secure Capacity Region):* A rate m-tuple $(R_1, R_2, \ldots, R_m)$ is said to be securely achievable if there

exist a block length n with $R_i = \frac{H(W_i)}{n}$, $\forall i \in [m]$ and a set of encoding functions f_e, $\forall e \in \mathcal{E}$, with

$$X_e^n = \begin{cases} f_e\left(W_{[m]}, \theta\right) & \text{if tail}(e) = S, \\ f_e\left(\{X_\ell^n : \ell \in \mathcal{I}(tail(e))\}\right) & \text{otherwise,} \end{cases}$$

such that each destination D_i can reliably decode the message W_i i.e.,

$$H\left(W_i | \{X_e^n : e \in \mathcal{I}(D_i)\}\right) = 0, \ \forall i \in [m].$$

Moreover, we also require perfect secrecy, i.e.,

$$I\left(W_{[m]}; X_{\mathcal{E}_\mathcal{Z}}^n\right) = 0, \ \forall \ \mathcal{E}_\mathcal{Z} \subseteq \mathcal{E} \text{ such that } |\mathcal{E}_\mathcal{Z}| \leq k.$$

The **secure capacity region** is the closure of all such feasible rate m-tuples.

Definition 2 (Min-Cut): A **cut** is an edge set $\mathcal{E}_\mathcal{A} \subseteq \mathcal{E}$, which separates the source S from a set of destinations $D_\mathcal{A} := \{D_i, \ i \in \mathcal{A}\}$. In a network with unit capacity edges, the minimum cut or **min-cut** is a cut that has the minimum number of edges. Throughout the paper, we denote by $M_\mathcal{A}$ the capacity of the min-cut between the source S and the set of destinations $D_\mathcal{A} := \{D_i, \ i \in \mathcal{A}\}, \mathcal{A} \subseteq [m]$, and we refer to $M_\mathcal{A}$ as the min-cut capacity.

In Definition 1, we require perfect secrecy, i.e., no matter which (at most) k edges Eve eavesdrops, she does not learn anything about the content of the messages. In particular, throughout the paper, we will use the following condition on perfect secrecy proved in [32, Lemma 3.1].

Lemma 1: Let W be the message vector that has to be transmitted, and K be a vector of size k of uniform i.i.d. symbols independent of W. Then, the vector X representing the symbols transmitted over the edges of the network can be represented in matrix form as

$$X = \begin{bmatrix} A & B \end{bmatrix} \begin{bmatrix} W \\ K \end{bmatrix},$$

where A and B are the encoding matrices. This transmission scheme is perfectly secure if and only if

$$rk\left(\begin{bmatrix} A & B \end{bmatrix}\big|_\mathcal{Z}\right) = rk\left(B|_\mathcal{Z}\right), \ \forall |\mathcal{Z}| \leq k, \tag{1}$$

where, for a matrix H of size $m \times n$ and a set $\mathcal{Z} \subseteq [m]$, we denote by $H|_\mathcal{Z}$ the submatrix of H of dimension $|\mathcal{Z}| \times n$ where only the rows indexed by the set $\mathcal{Z} \subseteq [m]$ are retained.

Remark 1: The condition in (1) ensures that any set of (at most) k linear combinations of message symbols W and random symbols K received on the edges indexed by $\mathcal{Z}$ are independent from the message symbols W. This follows since, according to (1), the columns of $A|_\mathcal{Z}$ do not provide any additional rank over the column rank provided by $B|_\mathcal{Z}$, and hence the random symbols from K can not be 'canceled out' from the linear combinations received by the eavesdropper without 'canceling out' the message symbols W. This intuitively explains why the condition in (1) implies perfect secrecy.

III. Outer Bound

In this section, we derive an outer bound on the secure capacity region of a multiple unicast wireline noiseless network with a single source and m destinations. In particular, as stated in Theorem 2, this region depends on the min-cut capacities between the source and different subsets of destinations, and on the number of edges that the adversary eavesdrops. The next theorem provides the outer bound region.

Theorem 2: An outer bound on the secure capacity region for the multiple unicast traffic over networks with a single source and m destinations is given by

$$R_\mathcal{A} \leq [M_\mathcal{A} - k]^+, \quad \forall \mathcal{A} \subseteq [m] \ , \tag{2}$$

where $R_\mathcal{A} := \sum_{i \in \mathcal{A}} R_i$, and where $M_\mathcal{A}$ is defined in Definition 2.

Proof: Let $\mathcal{E}_\mathcal{A}$ be a min-cut between the source S and $D_\mathcal{A}$ and $\mathcal{E}_\mathcal{Z} \subseteq \mathcal{E}_\mathcal{A}$ be the set of k edges eavesdropped by Eve, and define $\mathcal{I}(D_\mathcal{A}) := \bigcup_{i \in \mathcal{A}} \mathcal{I}(D_i)$. If $|\mathcal{E}_\mathcal{A}| < k$, let $\mathcal{E}_\mathcal{Z} = \mathcal{E}_\mathcal{A}$. We have

$$\begin{aligned} nR_\mathcal{A} &= H(W_\mathcal{A}) \\ &\overset{(a)}{=} H(W_\mathcal{A}) - H(W_\mathcal{A}|X_{\mathcal{I}(D_\mathcal{A})}^n) \\ &\overset{(b)}{\leq} H(W_\mathcal{A}) - H(W_\mathcal{A}|X_{\mathcal{E}_\mathcal{A}}^n) \\ &\overset{(c)}{=} I(W_\mathcal{A}; X_{\mathcal{E}_\mathcal{Z}}^n, X_{\mathcal{E}_\mathcal{A} \setminus \mathcal{E}_\mathcal{Z}}^n) \\ &= I(W_\mathcal{A}; X_{\mathcal{E}_\mathcal{Z}}^n) + I(W_\mathcal{A}; X_{\mathcal{E}_\mathcal{A} \setminus \mathcal{E}_\mathcal{Z}}^n | X_{\mathcal{E}_\mathcal{Z}}^n) \\ &\overset{(d)}{=} I(W_\mathcal{A}; X_{\mathcal{E}_\mathcal{A} \setminus \mathcal{E}_\mathcal{Z}}^n | X_{\mathcal{E}_\mathcal{Z}}^n) \\ &\overset{(e)}{\leq} H(X_{\mathcal{E}_\mathcal{A} \setminus \mathcal{E}_\mathcal{Z}}^n) \\ &\overset{(f)}{\leq} n[M_\mathcal{A} - k]^+ \ , \end{aligned}$$

where $W_\mathcal{A} = \{W_i, i \in \mathcal{A}\}$ and: (i) the equality in (a) follows because of the decodability constraint (see Definition 1); (ii) the inequality in (b) follows because of the 'conditioning reduces the entropy' principle and since $X_{\mathcal{I}(D_\mathcal{A})}^n$ is a deterministic function of $X_{\mathcal{E}_\mathcal{A}}^n$; (iii) the equality in (c) follows from the definition of mutual information and since $\mathcal{E}_\mathcal{A} = \mathcal{E}_\mathcal{Z} \cup \mathcal{E}_{\mathcal{A} \setminus \mathcal{Z}}$; (iv) the equality in (d) follows because of the perfect secrecy requirement (see Definition 1); (v) the inequality in (e) follows since the entropy of a discrete random variable is a non-negative quantity and because of the 'conditioning reduces the entropy' principle; (vi) finally, the inequality in (f) follows since each link is of unit capacity and since $|\mathcal{E}_\mathcal{A} \setminus \mathcal{E}_\mathcal{Z}| = [M_\mathcal{A} - k]^+$. By dividing both sides of the above inequality by n we obtain that $R_\mathcal{A}$ in (2) is an outer bound on the secure capacity region of the multiple unicast traffic over networks with single source and m destinations. This concludes the proof of Theorem 2. □

Remark 2: Since the passive adversary Eve eavesdrops any k edges of her choice, intuitively Theorem 2 states that, if she eavesdrops k edges of a cut with capacity M, we can at most hope to reliably transmit at rate $M - k$. However, this holds only for the case of a single source; indeed, as we will see in Section VII-B through an example, higher rates can be achieved for networks having a single destination and multiple sources.

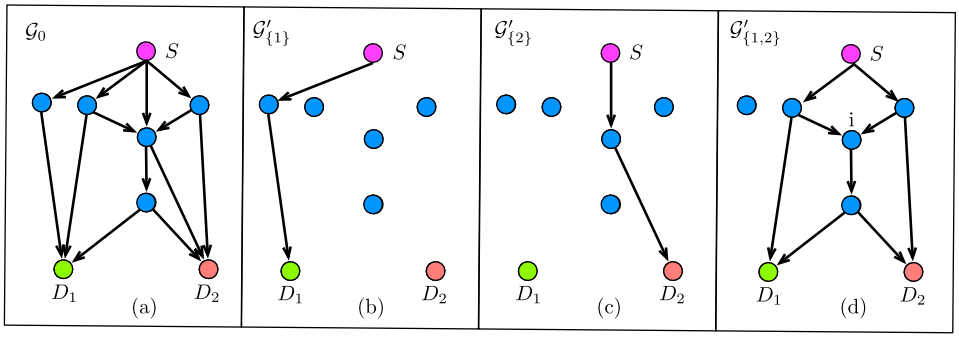


Fig. 1. A 2-destination separable network $\mathcal{G}_0$ in (a) and its partition into 3 edge disjoint graphs $\mathcal{G}'_{\mathcal{J}}, \mathcal{J} \subseteq \{1,2\}, \mathcal{J} \neq \emptyset$ in (b)-(d). Here, $M'_{\{1\}} = M'_{\{2\}} = 1$, and $M'_{\{1,2\}} = 2$.

IV. Capacity Achieving Scheme for Networks With Two Destinations

In this section, we prove that the outer bound in Theorem 2 is tight for the case of $m = 2$ destinations and arbitrary k. Towards this end, we design a secure transmission scheme whose achievable rate region matches the outer bound in Theorem 2. Our scheme follows the works of [1] and [9], where the source shares k keys (i.e., uniformly at random generated packets) with each destination, as well as information packets encoded with the k keys. As a result, by observing any k edges, the eavesdropper cannot extract any information about the messages. The main novel observation in our scheme is that, although the source transmits a private message to each receiver, we do not need to necessarily use a private key to encrypt each private message, but instead we can re-use the same key for multiple destinations. Thus, in some cases, we need to multicast keys to the destinations, although we never need to multicast encoded messages. Moreover, this scheme has the special property that we can isolate the key and encrypted message transmissions: we use some part of the network to convey (potentially multicast) the keys, and the remaining part to communicate the encrypted messages (i.e., the messages encoded with the keys). Our main result is stated in the following theorem.

Theorem 3: The outer bound in (2) is tight for the case $m = 2$, i.e., the secure capacity region of the multiple unicast traffic over networks with single source and $m = 2$ destinations is

$$R_1 \leq [M_{\{1\}} - k]^+ , \tag{3a}$$
$$R_2 \leq [M_{\{2\}} - k]^+ , \tag{3b}$$
$$R_1 + R_2 \leq [M_{\{1,2\}} - k]^+ . \tag{3c}$$

Clearly, from the result in Theorem 2, the rate region in (3) is an outer bound on the secure capacity region. Hence, we now need to prove that the rate region in (3) is also achievable. Towards this end, we start by providing the following definition of *separable* graphs, which we will leverage in the design of our scheme.

Definition 3 (Separable Graph): A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a single source and m destinations is said to be **separable** if it can be partitioned into $2^m - 1$ edge disjoint graphs (graphs with empty edge sets are also allowed). These graphs are denoted as $\mathcal{G}'_{\mathcal{J}} = (\mathcal{V}, \mathcal{E}'_{\mathcal{J}}), \mathcal{J} \subseteq [m], \mathcal{J} \neq \emptyset$ and are such that $\mathcal{E}'_{\mathcal{J}} \subseteq \mathcal{E}$, $\bigcup_{\mathcal{J}} \mathcal{E}'_{\mathcal{J}} = \mathcal{E}$ and $\mathcal{E}'_{\mathcal{J}} \cap \mathcal{E}'_{\mathcal{L}} = \emptyset$, $\forall \mathcal{J} \neq \mathcal{L} \subseteq [m]$. The three following properties must be satisfied:

1) For each of the graphs $\mathcal{G}'_{\mathcal{J}}$, all the min-cut capacities between the source S and any nonempty subset of destinations in $\{D_i : i \in \mathcal{J}\}$ are identical with value denoted by $M'_{\mathcal{J}}$;
2) For each of the graphs $\mathcal{G}'_{\mathcal{J}}$, no paths exist from the source S to each destination D_i, $i \in [m] \setminus \mathcal{J}$.
3) The min-cut capacities $M'_{\mathcal{J}}$ are such that

$$M_{\mathcal{A}} = \sum_{\substack{\mathcal{J} \subseteq [m] \\ \mathcal{J} \cap \mathcal{A} \neq \emptyset}} M'_{\mathcal{J}}, \ \forall \mathcal{A} \subseteq [m], \tag{4}$$

where $M_{\mathcal{A}}$ is the min-cut capacity for the graph $\mathcal{G}$ as defined in Definition 2.

To better understand the above definition, consider a graph $\mathcal{G}$ with $m = 2$ destinations. Then, the graph $\mathcal{G}$ is separable if it can be partitioned into 3 edge disjoint graphs such that:

- $\mathcal{G}'_{\{1\}}$ has the following min-cut capacities: $M'_{\{1\}}$ from S to D_1 and zero from S to D_2,
- $\mathcal{G}'_{\{2\}}$ has the following min-cut capacities: zero from S to D_1 and $M'_{\{2\}}$ from S to D_2,
- $\mathcal{G}'_{\{1,2\}}$ has the following min-cut capacities: $M'_{\{1,2\}}$ from S to D_1, $M'_{\{1,2\}}$ from S to D_2 and $M'_{\{1,2\}}$ from S to $\{D_1, D_2\}$,

where the quantities $M'_{\{1\}}, M'_{\{2\}}$ and $M'_{\{1,2\}}$ can be computed using the following set of equations:

$$M_{\{1\}} = M'_{\{1\}} + M'_{\{1,2\}}, \tag{5a}$$
$$M_{\{2\}} = M'_{\{2\}} + M'_{\{1,2\}}, \tag{5b}$$
$$M_{\{1,2\}} = M'_{\{1\}} + M'_{\{2\}} + M'_{\{1,2\}}. \tag{5c}$$

An example of separable graph for $m = 2$ and its partition into 3 edge disjoint graphs is shown in Fig. 1. We now state the following lemma, which is a consequence of [8, Theorem 1] and which we will use to prove the achievability of the rate region in (3). For completeness, we provide a self-contained proof of this lemma in Appendix A.

Lemma 4 [8, Theorem 1]: Any graph with a single source and $m = 2$ destinations is separable.

Proof of Theorem 3: By leveraging the result in Lemma 4, we are now ready to prove Theorem 3. In particular, we consider two cases depending on the value of k (i.e., the number of edges that the eavesdropper eavesdrops).

Without loss of generality, we assume that $k < \min_{i\in[2]} M_{\{i\}}$, as otherwise secure communication to the set of destinations $\{D_i : k \geq M_{\{i\}}, i \in [2]\}$ is not possible at any positive rate, and hence we can just remove this set of destinations from the network. To secure our messages from the adversary, we use uniform random packets generated at the source, which we refer to as *keys*. We will transmit these keys as well as the messages encoded with these keys over the network. The security of our schemes relies on two aspects: (i) a message encoded with a uniform random key is independent of the message and is distributed uniformly, and (ii) the amount of keys that we use is such that the eavesdropper cannot collect a sufficient number of keys and encoded messages to be able to extract any information on the messages.

1) **Case 1:** $k \geq M'_{\{1,2\}}$. In this case, by substituting the quantities in (5) into (3), we obtain that the constraint in (3c) is redundant. Thus, we will now prove that the rate pair $(R_1, R_2) = (M_{\{1\}} - k, M_{\{2\}} - k)$ is securely achievable, which along with the time-sharing argument proves the achievability of the entire rate region in (3). We denote with $K_1, K_2, \ldots, K_k$ the k key packets and with $W_i^{(1)}, W_i^{(2)}, \ldots, W_i^{(R_i)}$ (with $i \in [2]$) the R_i message packets for D_i. With this, our scheme is as follows:
   - We multicast the key packets $K_i, \forall i \in [M'_{\{1,2\}}]$, to both D_1 and D_2 using $\mathcal{G}'_{\{1,2\}}$, which has edges denoted by $\mathcal{E}'_{\{1,2\}}$. This is possible since $\mathcal{G}'_{\{1,2\}}$ has a min-cut capacity $M'_{\{1,2\}}$ to both D_1 and D_2 (see Definition 3).
   - We unicast the key packets $K_\ell, \forall \ell \in [M'_{\{1,2\}} + 1 : k]$, to $D_i, \forall i \in [2]$, using $k - M'_{\{1,2\}}$ paths out of the $M'_{\{i\}}$ disjoint paths in $\mathcal{G}'_{\{i\}}$. We denote by $\hat{\mathcal{E}}_{\{i\}}$ the set that contains all the first edges of these paths. Clearly, $|\hat{\mathcal{E}}_{\{i\}}| = k - M'_{\{1,2\}}, \forall i \in [2]$. Notice that $\hat{\mathcal{E}}_{\{i\}} \subseteq \mathcal{E}'_{\{i\}}, \forall i \in [2]$ (see Definition 3).
   - We send the $R_i, \forall i \in [2]$, encrypted message packets (i.e., encoded with the keys) of D_i on the remaining $M'_{\{i\}} - k + M'_{\{1,2\}}$ disjoint paths in $\mathcal{G}'_{\{i\}}$. We denote by $\bar{\mathcal{E}}_{\{i\}}$ the set that contains all the first edges of these paths in $\mathcal{G}'_{\{i\}}$. Clearly, $|\bar{\mathcal{E}}_{\{i\}}| = R_i, \forall i \in [2]$, $\bar{\mathcal{E}}_{\{i\}} \subseteq \mathcal{E}'_{\{i\}}$ and $\bar{\mathcal{E}}_{\{i\}} \cap \hat{\mathcal{E}}_{\{i\}} = \emptyset$ (see Definition 3).

This scheme achieves $R_i = M'_{\{i\}} - k + M'_{\{1,2\}} = M_{\{i\}} - k, \forall i \in [1:2]$, where the second equality follows by using the definitions in (5). Now we prove that this scheme is also secure. We start by noticing that, thanks to Definition 3, the edge sets $\mathcal{E}'_{\{1,2\}}$, $\hat{\mathcal{E}}_{\{i\}}$ and $\bar{\mathcal{E}}_{\{i\}}$, with $i \in [2]$, are disjoint. We write these transmissions in a matrix form (with G and U being the encoding matrices of size $\ell \times k$ and $(R_1 + R_2) \times k$, respectively) and we obtain (6) and (7), shown at the bottom of the page.

We here highlight that on the remaining edges $\mathcal{E} \backslash \{\mathcal{E}'_{\{1,2\}} \cup \hat{\mathcal{E}}_{\{1\}} \cup \bar{\mathcal{E}}_{\{1\}} \cup \hat{\mathcal{E}}_{\{2\}} \cup \bar{\mathcal{E}}_{\{2\}}\}$ of the network, we either do not transmit any symbol or simply route the symbols from $\{X_{\bar{\mathcal{E}}_{\{1\}}}, X_{\bar{\mathcal{E}}_{\{2\}}}, X_{\hat{\mathcal{E}}_{\{1\}}}, X_{\hat{\mathcal{E}}_{\{2\}}}\}$ (corresponding to the symbols transmitted on disjoint paths). Thus, without loss of generality, we can assume that Eve eavesdrops at most k edges from $\{\mathcal{E}'_{\{1,2\}} \cup \hat{\mathcal{E}}_{\{1\}} \cup \bar{\mathcal{E}}_{\{1\}} \cup \hat{\mathcal{E}}_{\{2\}} \cup \bar{\mathcal{E}}_{\{2\}}\}$. In what follows, we let: (i) X denote the vector of the symbols transmitted over these edges, (ii) K be the vector of the k random key packets, and (iii) W be the vector of the message packets for both destinations. More formally,

$$X = \begin{bmatrix} X_{\mathcal{E}'_{\{1,2\}}} \\ X_{\hat{\mathcal{E}}_{\{1\}}} \\ X_{\hat{\mathcal{E}}_{\{2\}}} \\ X_{\bar{\mathcal{E}}_{\{1\}}} \\ X_{\bar{\mathcal{E}}_{\{2\}}} \end{bmatrix}, \; W = \begin{bmatrix} W_1^{(1)} \\ \vdots \\ W_1^{(R_1)} \\ W_2^{(1)} \\ \vdots \\ W_2^{(R_2)} \end{bmatrix}, \; K = \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_k \end{bmatrix}.$$

$$\begin{bmatrix} X_{\mathcal{E}'_{\{1,2\}}} \\ X_{\hat{\mathcal{E}}_{\{1\}}} \\ X_{\hat{\mathcal{E}}_{\{2\}}} \end{bmatrix} = \underbrace{\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{\ell 1} & g_{\ell 2} & \cdots & g_{\ell k} \end{bmatrix}}_{G} \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_k \end{bmatrix}, \; \ell = |\mathcal{E}'_{\{1,2\}}| + 2\left(k - M'_{\{1,2\}}\right), \tag{6}$$

$$\begin{bmatrix} X_{\bar{\mathcal{E}}_{\{1\}}} \\ X_{\bar{\mathcal{E}}_{\{2\}}} \end{bmatrix} = \underbrace{\begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1k} \\ u_{21} & u_{22} & \cdots & u_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ u_{r1} & u_{r2} & \cdots & u_{rk} \end{bmatrix}}_{U} \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_k \end{bmatrix} + \begin{bmatrix} W_1^{(1)} \\ \vdots \\ W_1^{(R_1)} \\ W_2^{(1)} \\ \vdots \\ W_2^{(R_2)} \end{bmatrix}, \; r = R_1 + R_2. \tag{7}$$

With this, X can be represented in a matrix form as

$$X = \begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{bmatrix} \begin{bmatrix} W \\ K \end{bmatrix}, \tag{9}$$

with G and U being defined in (6) and (7), respectively, at the bottom of the previous page. We highlight that the first $|\mathcal{E}'_{\{1,2\}}|$ rows of G (i.e., those that correspond to multicasting the keys) are determined by the network coding scheme for multicasting [2]. As such, they can be constructed in $\mathcal{O}\left(|\mathcal{E}|^3\right)$ by using the multicasting scheme of [4], which requires a finite field of size $m = 2$. Thus, the security follows if we can show that for any choice of G, there exists a U such that (9) satisfies the condition in Lemma 1. This is proved in Appendix B where we show that, over a sufficiently large finite field, a random choice of U in (9) satisfies the condition in Lemma 1 with high probability. Thus, the rate pair $(R_1, R_2) = (M_{\{1\}}-k, M_{\{2\}}-k)$ is securely achievable.

2) **Case 2:** $k < M'_{\{1,2\}}$. By substituting the quantities in (5), the rate region in (3) becomes

$$\begin{aligned} R_i &\le M_{\{i\}} - k \\ &= M'_{\{i\}} + M'_{\{1,2\}} - k, \ \forall i \in [2] \ , \qquad \text{(10a)} \\ R_1 + R_2 &\le M_{\{1,2\}} - k \\ &= M'_{\{1\}} + M'_{\{2\}} + M'_{\{1,2\}} - k \ . \qquad \text{(10b)} \end{aligned}$$

We now show that we can achieve the two corner points i.e., the rate pair in (8), shown at the bottom of the page, for $\alpha \in \{0, 1\}$, where the equality in (a) follows by using the definitions in (5). This, along with the time-sharing argument, proves the achievability of the entire rate region in (10). We recall that we denote with $K_1, K_2, \ldots, K_k$ the k key packets and with $W_i^{(1)}, W_i^{(2)}, \ldots, W_i^{(R_i)}$ (with $i \in [2]$) the R_i message packets for D_i. With this, our scheme is as follows:

- Using the graph $\mathcal{G}'_{\{1,2\}}$ we multicast to both destinations D_1 and D_2: (i) $K_i, \forall i \in [k]$, (ii) $\alpha(M'_{\{1,2\}}-k)$ encrypted message packets (i.e., formed by encoding W_1 and the keys K) for D_1 and (iii) $(1-\alpha)$ $(M'_{\{1,2\}} - k)$ encrypted message packets (i.e., formed by encoding W_2 and the keys K) for D_2. Recall that the edges of the graph $\mathcal{G}'_{\{1,2\}}$ are denoted by $\mathcal{E}'_{\{1,2\}}$ (see Definition 3). Note that, since all these packets are multicast, then D_1 might also receive packets that are for D_2, and vice versa. However, note that, since the eavesdropper is external, i.e., it is not one of the destinations, then this does not violate the security condition, as long as the adversary, who eavesdrops any k edges of her choice, does not learn anything about the content of the messages. We also highlight that the message packets multicast to the two destinations are encoded using the key packets, where the encoding is based on the secure network coding result on multicasting [1], which ensures perfect security from an adversary eavesdropping any k edges.
- We send $M'_{\{i\}}$ encrypted message packets of D_i (i.e., encoded by using the k key packets) on the $M'_{\{i\}}$ disjoint paths to D_i in the graph $\mathcal{G}'_{\{i\}}$, and denote by $\hat{\mathcal{E}}_{\{i\}}$ the set that contains all the first edges of these paths for $i \in [2]$.

This scheme achieves the rate pair in (8) at the bottom of this page. Now we prove that this scheme is also secure. For ease of representation, in what follows we let $R'_1 = \alpha(M'_{\{1,2\}} - k)$ and $R'_2 = (1-\alpha)(M'_{\{1,2\}} - k)$. We again notice that, thanks to Definition 3, the edge sets $\mathcal{E}'_{\{1,2\}}$, $\hat{\mathcal{E}}_{\{1\}}$ and $\hat{\mathcal{E}}_{\{2\}}$ are disjoint. We write these transmissions in a matrix form (with G, S and U being the encoding matrices of sizes $\ell \times k$, $\ell \times t$ and $r \times k$ respectively) and we obtain (11) and (12) at the bottom of the next page.

In what follows, we let: (i) X denote the vector of the symbols transmitted over the edges $\mathcal{E}'_{\{1,2\}}$, $\hat{\mathcal{E}}_{\{1\}}$ and $\hat{\mathcal{E}}_{\{2\}}$, (ii) K be the vector of the k random key packets, and (iii)

$$W' := \begin{bmatrix} W_1^{(1)} \\ \vdots \\ W_1^{(R'_1)} \\ W_2^{(1)} \\ \vdots \\ W_2^{(R'_2)} \end{bmatrix}, \ W'' := \begin{bmatrix} W_1^{(R'_1+1)} \\ \vdots \\ W_1^{(R_1)} \\ W_2^{(R'_2+1)} \\ \vdots \\ W_2^{(R_2)} \end{bmatrix}.$$

With this, X can be represented in a matrix form as

$$\begin{aligned} X &= \begin{bmatrix} X_{\mathcal{E}'_{\{1,2\}}} \\ X_{\hat{\mathcal{E}}_{\{1\}}} \\ X_{\hat{\mathcal{E}}_{\{2\}}} \end{bmatrix} \\ &= \begin{bmatrix} S & 0_{\ell\times r} & G \\ 0_{r\times t} & I_r & U \end{bmatrix} \begin{bmatrix} W' \\ W'' \\ K \end{bmatrix}, \qquad \text{(13)} \end{aligned}$$

where G and S are defined in (11), shown at the bottom of the next page, and U is defined in (12), shown at the bottom of the next page. Similar to Case 1, on the remaining edges $\mathcal{E}\backslash\{\mathcal{E}'_{\{1,2\}} \cup \hat{\mathcal{E}}_{\{1\}} \cup \hat{\mathcal{E}}_{\{2\}}\}$ of the network, we either do not transmit any symbol or simply route the symbols from $\{X_{\hat{\mathcal{E}}_{\{1\}}}, X_{\hat{\mathcal{E}}_{\{2\}}}\}$ (corresponding to the symbols transmitted on disjoint paths). Thus, without loss of generality, we can assume that

$$\begin{aligned} (R_1, R_2) = \big((1-\alpha)(M_{\{1,2\}} - M_{\{2\}}) + \alpha(M_{\{1\}} - k), \\ (1-\alpha)(M_{\{2\}} - k) + \alpha(M_{\{1,2\}} - M_{\{1\}})\big) \\ \overset{(a)}{=} (M'_{\{1\}} + \alpha(M'_{\{1,2\}} - k), M'_{\{2\}} + (1-\alpha)(M'_{\{1,2\}} - k)) \ . \end{aligned} \tag{8}$$

the eavesdropper eavesdrops at most k edges from $\{\mathcal{E}'_{\{1,2\}} \cup \hat{\mathcal{E}}_{\{1\}} \cup \hat{\mathcal{E}}_{\{2\}}\}$. We highlight that the matrices G and S are determined by the secure network coding scheme for multicasting [1]. As such, they can be constructed in $\mathcal{O}\left(k^2|\mathcal{E}|^{k+2}\right)$ by using the scheme of [33], which requires a finite field of size $|\mathcal{E}|^k$. Thus, security follows if we can show that for any choice of S and G satisfying the security condition in Lemma 1, i.e., $rk\left(\left[\begin{array}{cc} S & G \end{array}\right]|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]|_{\mathcal{Z}}\right), \forall |\mathcal{Z}| \leq k$, there exists a choice of U such that the security condition in Lemma 1 is satisfied for (13). This is proved in Appendix C where we show that, over a sufficiently large finite field, a random choice of U in (13) satisfies the condition in Lemma 1 with high probability.

This concludes the proof of Theorem 3. □

Example 1: We here illustrate the above described scheme for the network $\mathcal{G}_0$ in Fig. 1(a). We first note that $\mathcal{G}_0$ has min-cut capacities $M_{\{1\}} = M_{\{2\}} = 3$ and $M_{\{1,2\}} = 4$, and it can be partitioned into three edge disjoint graphs $\mathcal{G}'_{\mathcal{J}}, \mathcal{J} \subseteq \{1,2\}, \mathcal{J} \neq \emptyset$ as shown in Figs. 1(b)-(d), with min-cut capacities equal to $M'_{\{1\}} = M'_{\{2\}} = 1$ and $M'_{\{1,2\}} = 2$, respectively. We assume that the adversary eavesdrops any $k = 2$ edges of her choice. For this case, the source should be able to securely communicate at a rate $(R_1, R_2) = (1, 1)$ towards the $m = 2$ destinations. This rate pair can be achieved using two key packets K_1 and K_2 and operations over $\mathbb{F}_4$ as follows:

1) Over the set of edges in $\mathcal{G}'_{\{1\}}$, the source transmits $W_1 + K_1 + 2\ K_2$; the intermediate node simply routes this transmission to D_1;
2) Over the set of edges in $\mathcal{G}'_{\{2\}}$, the source transmits $W_2 + K_1 + 3\ K_2$; the intermediate node simply routes this transmission to D_2;
3) Over the set of edges in $\mathcal{G}'_{\{1,2\}}$, the source multicasts K_1 and K_2 to the receivers. It transmits K_1 to one intermediate node and K_2 to the other intermediate node. The intermediate node denoted as i in Fig. 1(d) receives K_1 and K_2 and transmits $K_1 + K_2$ on its outgoing edges. Thus D_1 and D_2 receive both K_1 and K_2. It therefore follows that $D_i, i \in [2]$, can successfully recover W_i. ■

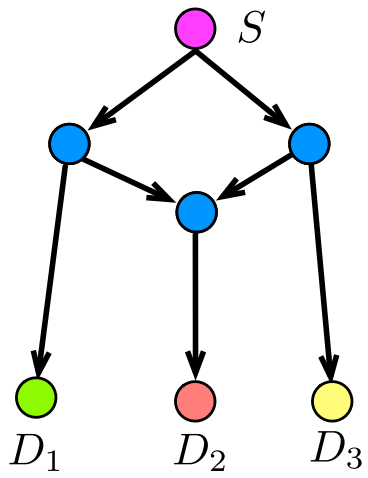


Fig. 2. Example of a non-separable graph.

We conclude this section with some observations on separable graphs. As highlighted in the proof of Theorem 3, given the separation of a graph into subgraphs, our capacity achieving scheme is polynomial-time. However, identifying the subgraphs with the required min-cut properties is not an easy problem [8], and it is not clear if it can be performed in polynomial-time. Moreover, although for the case of $m = 2$ destinations any graph is separable (see [8, Theorem 1]), in general the same does not hold for $m \geq 3$, as the following example illustrates.

Example 2: Consider the network in Fig. 2, which consists of $m = 3$ destinations and has the following min-cut capacities: $M_{\{1\}} = 1$, $M_{\{2\}} = 1$, $M_{\{3\}} = 1$, $M_{\{1,2\}} = 2$,

$$X_{\mathcal{E}'_{\{1,2\}}} = \underbrace{\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{\ell 1} & g_{\ell 2} & \cdots & g_{\ell k} \end{bmatrix}}_{G} \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_k \end{bmatrix} + \underbrace{\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1t} \\ s_{21} & s_{22} & \cdots & s_{1t} \\ \vdots & \vdots & \ddots & \vdots \\ s_{\ell 1} & s_{\ell 2} & \cdots & s_{\ell t} \end{bmatrix}}_{S} \begin{bmatrix} W_1^{(1)} \\ \vdots \\ W_1^{(R'_1)} \\ W_2^{(1)} \\ \vdots \\ W_2^{(R'_2)} \end{bmatrix}, \tag{11}$$

where $\ell = |\mathcal{E}'_{\{1,2\}}|$ and $t = R'_1 + R'_2$, and

$$\begin{bmatrix} X_{\hat{\mathcal{E}}_{\{1\}}} \\ X_{\hat{\mathcal{E}}_{\{2\}}} \end{bmatrix} = \underbrace{\begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1k} \\ u_{21} & u_{22} & \cdots & u_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ u_{r1} & u_{r2} & \cdots & u_{rk} \end{bmatrix}}_{U} \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_k \end{bmatrix} + \begin{bmatrix} W_1^{(R'_1+1)} \\ \vdots \\ W_1^{(R_1)} \\ W_2^{(R'_2+1)} \\ \vdots \\ W_2^{(R_2)} \end{bmatrix}, \quad r = R_1 + R_2 - (M'_{\{1,2\}} - k)\ . \tag{12}$$

$M_{\{2,3\}} = 2$, $M_{\{1,3\}} = 2$ and $M_{\{1,2,3\}} = 2$. With this, we can find $M'_{\mathcal{J}}$, $\mathcal{J} \subseteq [3]$, by solving (4). In particular, we obtain: $M'_{\{1\}} = M'_{\{2\}} = M'_{\{3\}} = 0$, $M'_{\{1,2\}} = M'_{\{2,3\}} = M'_{\{1,3\}} = 1$ and $M'_{\{1,2,3\}} = -1$. Since a graph can not have a negative min-cut capacity, we readily conclude that a separation of the form defined in Definition 3 is not possible. ■

V. Secure Scheme for Two-Layer Networks

In Section IV, we characterized the secure capacity region of networks with $m = 2$ destinations, by leveraging the separability property. In this section, we discuss separable networks with arbitrary number of destinations and characterize the capacity region of networks with: (i) arbitrary number m of destinations, where the adversary eavesdrops any $k = 1$ edge of her choice, (ii) networks with $m = 3$ destinations, where the adversary eavesdrops any arbitrary k edges of her choice, and (iii) networks with arbitrary values of k and m for which the min-cut capacities satisfy certain properties. Towards this end, we will first consider a special class of separable networks, namely networks having a two-layer topology, and design a secure scheme for this class of networks. We will then show that, in order to characterize the secure capacity region of any separable network, it is sufficient to study two-layer networks. In particular, we will prove that any separable network can be modeled as a two-layer network with the same min-cut capacities, and that a secure scheme for a two-layer network can be transformed into a secure scheme for its corresponding separable network. We now proceed by formally defining the two-layer network topology.

Definition 4: A two-layer network consists of one source S that wishes to communicate with m destinations, by hopping information through one layer of t relays. As such, a two-layer network is parameterized by: (i) the integer t, which denotes the number of relays in the first layer; (ii) the integer m, which indicates the number of destinations in the second layer; (iii) m sets $\mathcal{M}_i$, $i \in [m]$, such that $\mathcal{M}_i \subseteq [t]$, where $\mathcal{M}_i$ contains the indexes of the relays connected to destination D_i.

An example of a two-layer network is shown in Fig. 3, for which $t = 6$, $m = 3$, $\mathcal{M}_1 = \{1, 2, 3, 4\}$, $\mathcal{M}_2 = \{1, 2, 5, 6\}$ and $\mathcal{M}_3 = \{3, 4, 5, 6\}$.

Before delving into the study of such two-layer networks, recall that the capacity-achieving scheme for $m = 2$ destinations described in Section IV uses some parts of the network to convey (potentially multicasting) the keys and the remaining part to communicate the encrypted messages. Therefore, we now ask the following question: can we extend this idea to get a capacity-achieving scheme for separable networks with arbitrary number of destinations? In other words, can we spatially isolate the key from the message transmission? The next example shows that this is not possible through an example.

Example 3: Consider the two-layer network shown in Fig. 3, which consists of $m = 3$ destinations, and where the adversary can eavesdrop any $k = 3$ edges of her choice. For this network we have the following min-cut capacities: $M_{\{1\}} = M_{\{2\}} = M_{\{3\}} = 4$, $M_{\{1,2\}} = M_{\{1,3\}} = M_{\{2,3\}} = M_{\{1,2,3\}} = 6$. We would like to show that the triple $(R_1, R_2, R_3) = (1, 1, 1)$ – obtained from the outer bound in Theorem 2 – can not be achieved when the key packets and the encrypted messages are transmitted over different parts of the network. It is not difficult to see that, out of the 6 outgoing edges from the source, multicasting 3 keys[1] requires a number of edges strictly greater than 4. Thus, we would be left with strictly less than 2 edges, which are not sufficient to transmit 3 message packets, i.e., one for each destination. It therefore follows that, with this strategy, the rate triple $(R_1, R_2, R_3) = (1, 1, 1)$ can not be securely achieved.

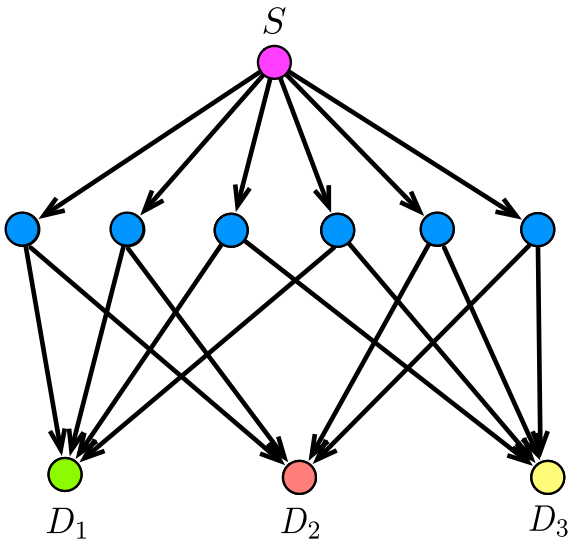


Fig. 3. Two-layer network example which illustrates that using different parts of the network to transmit the keys and the encrypted messages is not optimal. In this network $\mathcal{M}_1 = \{1, 2, 3, 4\}$, $\mathcal{M}_2 = \{1, 2, 5, 6\}$ and $\mathcal{M}_3 = \{3, 4, 5, 6\}$.

However, let the source transmits the following symbols on its outgoing edges

$$\begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 \\ 1 & 0 & 0 & 1 & 3 & 2 \\ 4 & 6 & 4 & 1 & 4 & 2 \\ 2 & 4 & 2 & 1 & 5 & 4 \end{bmatrix}}_{B} \begin{bmatrix} W_1 \\ W_2 \\ W_3 \\ K_1 \\ K_2 \\ K_3 \end{bmatrix}, \tag{14}$$

where $B \in \mathbb{F}_7^{6\times 6}$ is the encoding matrix. If the intermediate nodes simply route the received symbols, then we can achieve the rate tuple $(1, 1, 1)$. This is because, the encoding matrix B can be written as

$$B = \begin{bmatrix} B' & B'' \end{bmatrix},$$

where B' contains the first three columns of B in (14), and B'' contains the last three columns of B in (14). Thus, it follows that

$$rk\left(\begin{bmatrix} B' & B'' \end{bmatrix}\Big|_{\mathcal{Z}}\right) = rk\left(B''\Big|_{\mathcal{Z}}\right), \ \forall |\mathcal{Z}| \leq 3,$$

which, from Lemma 1, implies that the encoding in (14) is secure.

[1] Note that 3 keys are required since the adversary eavesdrops $k = 3$ edges of her choice.

Moreover, each destination can decode its respective message as follows:

- Destination 1: $W_1 = 6\ X_1 + 3\ X_2 + 4\ X_3 + X_4$,
- Destination 2: $W_2 = 6\ X_1 + 4\ X_2 + 3\ X_5 + X_6$,
- Destination 3: $W_3 = 5\ X_3 + 6\ X_4 + X_5 + 2\ X_6$.

Thus, the rate triple $(R_1, R_2, R_3) = (1, 1, 1)$ can be securely achieved. This example shows that using different parts of the network to transmit the keys and the encrypted messages, in general is not optimal. This is partially due to the fact that destinations do not need to decode each key individually, as long as they can successfully recover their message. ■

A. Secure Transmissions Scheme

For two-layer networks, we have $M_{\mathcal{A}} = |\cup_{i\in\mathcal{A}}\mathcal{M}_i|$. For notational convenience, we let $M_{\cap\{i,j\}} = |\mathcal{M}_i \cap \mathcal{M}_j|$ and $M_{\cap\{i,\mathcal{A}\}} = |\mathcal{M}_i \cap (\cup_{j\in\mathcal{A}}\mathcal{M}_j)|$. Moreover, we also assume that $M_{\{i\}} \geq k, \forall i \in [m]$ (otherwise secure communication is not possible) with $M_{\emptyset} := k$ for consistency.

We here propose a polynomial-time (see Lemma 6) secure transmission scheme for two-layer networks. In Section V-B, we will then derive its achieved rate region. The source S encodes the message packets with k random packets and transmits these packets on its outgoing edges to the t relays. We can write the received symbols at the t relays as

$$\begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_t \end{bmatrix} = \begin{bmatrix} & H & | & V & \end{bmatrix} \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_m \\ K \end{bmatrix}, \qquad (15)$$

where: (i) $W_i, i \in [m]$ is a column vector of R_i message packets for destination D_i, (ii) K is a column vector which contains the k random packets, (iii) H is an encoding matrix of dimension $t\times(\sum_{i=1}^{m} R_i)$ (as we will show below such a matrix can always be constructed so that all the destinations correctly decode their intended message), and (iv) V is a Vandermonde matrix of dimension $t\times k$. The matrix V is chosen for *security purposes*, i.e., any set of k rows of V are linearly independent and hence Lemma 1 ensures that, no matter which k rows (i.e., edges) Eve eavesdrops, she will learn nothing about the messages $W_{[m]}$.

Remark 3: The only property of V that we require in our scheme is the Maximum Distance Separable (MDS) property (i.e., any k rows of V are linearly independent). This implies that, even if we select a random matrix $\tilde{V}$ instead of V, with high probability (close to 1 for large field size) we will have a secure scheme for the two-layer network. This also implies that a finite field of size $\mathcal{O}(|\mathcal{E}|)$ can deterministically provide such a matrix $\tilde{V}$.

Each relay $i \in [t]$ will then forward the received symbol X_i in (15) to the destinations to which it is connected. As such, each destination will observe a subset of symbols from $\{X_1, X_2, \ldots, X_t\}$ (depending on which of the t relays it is connected to). Finally, destination $D_i, i \in [m]$ selects a decoding vector and performs the inner product with $[X_1, X_2, \ldots, X_t]$. In particular, this decoding vector is chosen such that it has two characteristics: (1) it is in the left null space of V, i.e., in the right null space of V^T; this ensures that each destination is able to cancel out the random packets (encoded with the message packets); (2) it has zeros in the positions corresponding to the relays it is not connected to; this ensures that each destination uses only the symbols that it actually observes. In other words, all the decoding vectors that D_i can choose belong to the right null space $\mathcal{N}_i$ of the matrix V_i defined

$$V_i = \begin{bmatrix} V^T \\ C_i \end{bmatrix}, \qquad (16)$$

where C_i is a matrix of dimension $\bar{t}_i \times t$, with $\bar{t}_i$ being the number of relays to which D_i is not connected to, i.e., $\bar{t}_i = t - M_i$. In this section, we will use the notion $\mathcal{V}_i$ to denote the row-space of the matrix V_i. In particular, each row of C_i has all zeros except a one in the position corresponding to a relay to which D_i is not connected to.

For instance, for the network in Fig. 3, we have

$$C_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$
$$C_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$
$$C_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We let T be a matrix of dimension $(\sum_{i=1}^{m} R_i) \times t$ that, for each destination $D_i, i \in [m]$, contains R_i decoding vectors that belong to the right null space of the matrix V_i in (16), denoted as $\mathcal{N}_i$. Mathematically, we have

$$T = \begin{bmatrix} ---- d_1^{(1)} ---- \\ ---- d_2^{(1)} ---- \\ \vdots \\ ---- d_{R_1}^{(1)} ---- \\ ---- d_1^{(2)} ---- \\ \vdots \\ ---- d_{R_m}^{(m)} ---- \end{bmatrix}, \qquad (17)$$

where $d_j^{(i)}$ denotes the j-th decoding vector (of length t) selected from the null space $\mathcal{N}_i$, with $i \in [m], j \in [R_i]$. Note that, if for all $i \in [m]$, we can select R_i decoding vectors from $\mathcal{N}_i$ such that all the $d_j^{(i)}$ in (17) are linearly independent (i.e., such that T has a full row rank), then it is possible to construct the matrix H in (15) such that

$$TH = I_{(\sum_{i=1}^{m} R_i)}, \qquad (18)$$

which ensures that all the destinations are able to correctly decode their intended message as

$$\begin{bmatrix} \hat{W}_1 \\ \vdots \\ \hat{W}_m \end{bmatrix} = T \begin{bmatrix} X_1 \\ \vdots \\ X_t \end{bmatrix} \overset{(15)}{=} \begin{bmatrix} TH & TV \end{bmatrix} \begin{bmatrix} W_1 \\ \vdots \\ W_m \\ K \end{bmatrix}$$
$$= TH \begin{bmatrix} W_1 \\ \vdots \\ W_m \end{bmatrix} + TVK = \begin{bmatrix} W_1 \\ \vdots \\ W_m \end{bmatrix}.$$

In Appendix D, we propose an iterative algorithm (of polynomial-complexity as formally proved in Lemma 6) to select $R_i, i \in [m]$ decoding vectors from $\mathcal{N}_i$ such that T in (17) has indeed a full row rank. The performance of the proposed algorithm is provided in the following lemma, which is also proved in Appendix D.

Lemma 5: For any given permutation $\pi = \{\pi(1), \ldots, \pi(m)\}$ of $[m]$, it is possible to select

$$R_{\pi(i)} = \dim\left(\sum_{j=1}^{i} \mathcal{N}_{\pi(j)}\right) - \dim\left(\sum_{j=1}^{i-1} \mathcal{N}_{\pi(j)}\right), \quad i \in [m], \tag{19}$$

vectors from $\mathcal{N}_{\pi(i)}$ so that all the $\sum_{i=1}^{m} R_i$ selected vectors are linearly independent.

Remark 4: Note that, since there are $m!$ possible permutations of $[m]$, then Lemma 5 offers $m!$ possible choices for selecting $R_i, i \in [m]$ vectors from $\mathcal{N}_i$ so that all the $\sum_{i=1}^{m} R_i$ selected vectors are linearly independent. We prove in Lemma 7 that these choices form the corner points of the secure rate region achieved by our scheme.

Remark 5: The result in Lemma 5 implies that rate m-tuple $(R_1, R_2, \ldots, R_m)$, with $R_i, i \in [m]$ being defined in (19), can be securely achieved by our proposed scheme.

The following lemma analyzes the complexity of designing our proposed secure scheme.

Lemma 6: The complexity of designing the secure transmission scheme in (15) equals $\mathcal{O}(m|\mathcal{E}|^4)$. Moreover, a field size of dimension $q \geq |\mathcal{E}|$ is sufficient.

Proof: To achieve any rate m-tuple $(R_1, R_2, \ldots, R_m)$ using our scheme, we need to find a basis of null spaces $\mathcal{N}_i, \ \forall i \in [m]$ and then use the iterative algorithm proposed in Appendix D to form the decoding matrix T in (17). A basis of the null space $\mathcal{N}_i$ can be found using the Gaussian elimination algorithm, which has a complexity of $\mathcal{O}(|\mathcal{E}|^3)$ [34]. The iterative algorithm in Appendix D for selecting decoding vectors in these null spaces requires discarding dependent vectors, which has a complexity of $\mathcal{O}(m|\mathcal{E}||\mathcal{E}|^3)$. This follows since: (i) there are at most $m|\mathcal{E}|$ vectors in the basis of these null spaces, and (ii) to check if each vector is dependent on the previously selected vectors, we require $\mathcal{O}(|\mathcal{E}|^3)$ computations using the Gaussian elimination algorithm. Finally, given the decoding matrix T, we require the computation of the encoding matrix H which, as highlighted in (18), is the right inverse of T. Thus, computing H requires $\mathcal{O}(|\mathcal{E}|^3)$ operations by again using the Gaussian elimination algorithm. It therefore follows that the overall complexity of our secure transmission scheme is $\mathcal{O}(m|\mathcal{E}|^4)$.

As discussed in Remark 3, to ensure security we are using only the MDS property of the Vandermonde matrix V in (15). The size of this matrix is $t \times k$, and $t \leq |\mathcal{E}|$. Thus, a field size of dimension $|\mathcal{E}|$ is sufficient. This concludes the proof of Lemma 6. □

In the next section, we will leverage the result in Lemma 5 and Remark 4 to derive the secure rate region achieved by our proposed scheme.

B. Achieved Secure Rate Region

In this section, we derive the rate region achieved by the secure scheme described in Section V-A. In particular, we have the following lemma, whose proof is in Appendix E.

Lemma 7: The secure rate region achieved by the proposed scheme is given by

$$0 \leq \sum_{i \in \mathcal{A}} R_i \leq \dim\left(\sum_{i \in \mathcal{A}} \mathcal{N}_i\right), \ \forall \mathcal{A} \subseteq [m], \tag{20}$$

where $\mathcal{N}_i$ is the right null space of the matrix V_i in (16).

In the remainder of this section, we prove that the secure rate region in (20) is indeed the secure *capacity* region when: (i) the adversary eavesdrops any $k = 1$ edge of her choice (and arbitrary m); (ii) there are $m = 3$ destinations (and arbitrary k); (iii) k and m are arbitrary, but the network has some special structure in terms of minimum cut.

C. Secure Capacity for $k = 1$, m Arbitrary

In this section, we consider the case where Eve eavesdrops any $k = 1$ edge of her choice, and characterize the secure capacity region. In particular, we prove the following theorem.

Theorem 8: For the two-layer network when Eve eavesdrops any $k = 1$ edge of her choice, the secure capacity region is

$$\sum_{i \in \mathcal{A}} R_i \leq M_{\mathcal{A}} - C_{\mathcal{A}}, \ \forall \mathcal{A} \subseteq [m], \tag{21}$$

with $C_{\mathcal{A}}$ being the number of connected components in an undirected graph where: (i) there are $|\mathcal{A}|$ nodes, i.e., one for each $i \in \mathcal{A}$; (ii) an edge between node i and node j, $\{i, j\} \in \mathcal{A}$, $i \neq j$, exists if $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$.

1) Outer Bound: We show that the outer bound in Theorem 2 can be equivalently written as in (21). Let $\mathcal{A}_i, i \in [C_{\mathcal{A}}]$, represent the set of nodes in the i-th component of the graph constructed as explained in Theorem 8. Then, clearly $\mathcal{A} = \bigsqcup_{i=1}^{C_{\mathcal{A}}} \mathcal{A}_i$ and we can write

$$\begin{aligned}
\sum_{i \in \mathcal{A}} R_i &= \sum_{i \in \mathcal{A}_1} R_i + \sum_{i \in \mathcal{A}_2} R_i + \ldots + \sum_{i \in \mathcal{A}_{C_{\mathcal{A}}}} R_i \\
&\overset{(a)}{\leq} (M_{\mathcal{A}_1} - k) + (M_{\mathcal{A}_2} - k) + \ldots \\
&\quad + \left(M_{\mathcal{A}_{C_{\mathcal{A}}}} - k\right) \\
&\overset{(b)}{=} M_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \ldots \cup \mathcal{A}_{C_{\mathcal{A}}}} - kC_{\mathcal{A}} \\
&\overset{(c)}{=} M_{\mathcal{A}} - kC_{\mathcal{A}} \\
&\overset{k=1}{=} M_{\mathcal{A}} - C_{\mathcal{A}},
\end{aligned}$$

where: (i) the inequality in (a) follows by applying (2) for each set $\mathcal{A}_i, i \in [C_{\mathcal{A}}]$, (ii) the equality in (b) follows since, by construction, $\mathcal{M}_i \cap \mathcal{M}_j = \emptyset$ for all $i \in \mathcal{A}_x$ and $j \in \mathcal{A}_y$ with $x \neq y$, and (iii) the equality in (c) follows since $\mathcal{A} = \bigsqcup_{i=1}^{C_{\mathcal{A}}} \mathcal{A}_i$. Thus, (2) implies (21). Moreover, since $C_{\mathcal{A}} \geq 1$, (21) implies (2). This shows that the rate region in Theorem 8 is an outer bound on the secure capacity region when $k = 1$.

We now consider an example of a two-layer network and show how the upper bound derived above applies to it.

Example 4: Let $\mathcal{A} = \{2,3,4\}$, and assume that $\mathcal{M}_1 = \{1,2\}$, $\mathcal{M}_2 = \{3,4\}$, $\mathcal{M}_3 = \{4,5,6\}$ and $\mathcal{M}_4 = \{7,8\}$. Then, we construct an undirected graph such that: (i) it has 3 nodes since $|\mathcal{A}| = 3$ and (ii) it has an edge between node 2 and node 3 since $\mathcal{M}_2 \cap \mathcal{M}_3 = \{4\} \neq \emptyset$. It therefore follows that this graph has $C_{\mathcal{A}} = 2$ components. In particular, we have

$$\sum_{i\in\mathcal{A}} R_i = \sum_{i\in\mathcal{A}_1} R_i + \sum_{i\in\mathcal{A}_2} R_i \leq M_{\{2,3,4\}} - 2k \overset{k=1}{=} 4, \quad (22)$$

where $\mathcal{A}_1 = \{2,3\}$ and $\mathcal{A}_2 = \{4\}$. ■

2) Achievable Rate Region: We here show that the rate region in Theorem 8 is achieved by the scheme described in Section V-A. In particular, we show that

$$\dim\left(\sum_{i\in\mathcal{A}} \mathcal{N}_i\right) \geq M_{\mathcal{A}} - C_{\mathcal{A}}, \ \forall \mathcal{A} \subseteq [m], \quad (23)$$

where recall that $\dim\left(\sum_{i\in\mathcal{A}} \mathcal{N}_i\right)$ is the secure rate performance of our proposed scheme in Section V-A (see Lemma 7). The condition in (23) can be equivalently written as $\forall \mathcal{A} \subseteq [m]$,

$$\begin{aligned} M_{\mathcal{A}} - C_{\mathcal{A}} \leq \dim\left(\textstyle\sum_{i\in\mathcal{A}} \mathcal{N}_i\right) &\overset{(a)}{=} \dim\left(\left(\cap_{i\in\mathcal{A}} \mathcal{V}_i\right)^{\perp}\right) \\ &= t - \dim\left(\cap_{i\in\mathcal{A}} \mathcal{V}_i\right), \end{aligned}$$

where the equality in (a) follows by using the property of the dual space and rank nullity theorem, and $V_i, i \in \mathcal{A}$ is defined in (16) with $\mathcal{V}_i$ being the row space of the matrix V_i. In other words, we next show that

$$\forall \mathcal{A} \subseteq [m], \ \dim\left(\cap_{i\in\mathcal{A}} \mathcal{V}_i\right) \leq t - M_{\mathcal{A}} + C_{\mathcal{A}}. \quad (24)$$

Towards this end, we would like to count the number of linearly independent vectors $x \in \mathbb{F}_q^t$ that belong to $(\cap_{i\in\mathcal{A}} \mathcal{V}_i)$.

We note that, by our construction: (i) V^T consists of one row (since $k = 1$) of t ones, and (ii) C_i has zeros in the positions indexed by $\mathcal{M}_i$. Hence, if a vector belongs to $\mathcal{V}_i$, then all its components indexed by $\mathcal{M}_i$ have to be the same, i.e., either they are all zeros, or they are all equal to a multiple of one. Thus, we have q choices to fill such positions indexed by $\mathcal{M}_i$.

Now, consider V_j with $j \in \mathcal{A}$ and $j \neq i$. By using the same logic as above, if a vector belongs to $\mathcal{V}_j$, then all its components indexed by $\mathcal{M}_j$ have to be the same and we have q choices to fill these. We now need to count the number of such choices that are consistent with the choices made to fill the positions indexed by $\mathcal{M}_i$. Towards this end, we consider two cases:

1) **Case 1:** $\mathcal{M}_i \cap \mathcal{M}_j = \emptyset$. In this case, there is no overlap in the elements indexed by $\mathcal{M}_i$ and $\mathcal{M}_j$ and hence we can select all the available q choices for the positions indexed by $\mathcal{M}_j$;
2) **Case 2:** $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$. In this case, there is some overlap in the elements indexed by $\mathcal{M}_i$ and $\mathcal{M}_j$. Thus, since we have already fixed the elements indexed by $\mathcal{M}_i$, we do not have any choice for the elements indexed by $\mathcal{M}_j$ (since all the elements have to be the same).

By iterating the same reasoning as above for all $i \in \mathcal{A}$, we conclude that we can fill all the positions indexed by $\cup_{i\in\mathcal{A}} \mathcal{M}_i$ of a vector $x \in \mathbb{F}_q^t$ and make sure that $x \in (\cap_{i\in\mathcal{A}} \mathcal{V}_i)$ in $q^{C_{\mathcal{A}}}$ ways. This is because, there are $C_{\mathcal{A}}$ connected components, and for each of these components we have only q choices to fill the corresponding positions in the vector x (i.e., the positions that correspond to the relays to which at least one of the destinations inside that component is connected). Once we fix any position inside a component, in fact all the other positions inside that component have to be the same, and thus we have no more freedom in choosing the other positions. Moreover, the remaining $t - M_{\mathcal{A}}$ positions of x can be filled with any value in $\mathbb{F}_q$ and for this we have $q^{t-M_{\mathcal{A}}}$ possible choices. Therefore, the number of vectors $x \in \mathbb{F}_q^t$ that belong to $(\cap_{i\in\mathcal{A}} \mathcal{V}_i)$ is at most $q^{C_{\mathcal{A}}+t-M_{\mathcal{A}}}$, which implies

$$\forall \mathcal{A} \subseteq [m], \ \dim\left(\cap_{i\in\mathcal{A}} \mathcal{V}_i\right) \leq t - M_{\mathcal{A}} + C_{\mathcal{A}}.$$

This proves that the secure scheme in Section V-A achieves the rate region in Theorem 8. We now illustrate our method of identifying vectors that belong to $\cap_{i\in\mathcal{A}} \mathcal{V}_i$ through an example.

Example 5: Let $t = 8$, $m = 4$, $\mathcal{M}_1 = \{1,2\}$, $\mathcal{M}_2 = \{3,4\}$, $\mathcal{M}_3 = \{4,5,6\}$ and $\mathcal{M}_4 = \{7,8\}$. Let $\mathcal{A} = \{2,3,4\}$. With this, we can construct $V_i, i \in [4]$, as described in (16), where V^T consists of one row of 8 ones. We now want to count the number of vectors $x \in \mathbb{F}_q^8$ such that $x \in \mathcal{V}_2 \cap \mathcal{V}_3 \cap \mathcal{V}_4$. We use the following iterative procedure:

1) For x to belong to $\mathcal{V}_2$ its elements in the 3rd and 4th positions have to be the same since $\mathcal{M}_2 = \{3,4\}$. Thus, we have q choices to fill the 3rd and 4th position.
2) For x to belong to $\mathcal{V}_3$, its elements in the 4th, 5th and 6th positions have to be the same since $\mathcal{M}_3 = \{4,5,6\}$. However, the element in the 4th position has already been fixed in selecting vectors that belong to $\mathcal{V}_2$. Thus, there is no further choice in filling the 5th and 6th positions.
3) For x to belong to $\mathcal{V}_4$, its elements in the 7th and 8th positions have to be the same since $\mathcal{M}_4 = \{7,8\}$. Since in the previous two steps, we have not filled yet the elements in these positions, then we have q possible ways to fill the elements in the 7th and 8th positions.
4) Moreover, we can fill the elements in the 1st and 2nd positions of x in q^2 possible ways.

With the above procedure we get that $\dim\left(\cap_{i\in\{2,3,4\}} \mathcal{V}_i\right) = 4$, which is equal to the upper bound that we computed in (22) for the same example. ■

D. Secure Capacity for $m = 3$, k Arbitrary

In this section, we consider the case $m = 3$, and prove the following theorem.

Theorem 9: For a two-layer network with $m = 3$ destinations, the secure capacity region is given by

$$\sum_{i\in\mathcal{A}} R_i \leq M_{\mathcal{A}} - k, \ \forall \mathcal{A} \subseteq [m]. \quad (25)$$

Clearly, from our result in Theorem 2, the rate region in (25) is an outer bound on the secure capacity region and can be

equivalently written as

$$\sum_{i\in\mathcal{A}} R_i \leq \min_{\mathcal{P}\,:\,\bigsqcup_{\mathcal{Q}\in\mathcal{P}}\mathcal{Q}=\mathcal{A}} \left\{\sum_{\mathcal{Q}\in\mathcal{P}} M_{\mathcal{Q}} - |\mathcal{P}|k\right\}, \quad \forall \mathcal{A}\subseteq[m],$$

where $\mathcal{P}$ is a disjoint partition of $\mathcal{A}$. We will now show that for every $\mathcal{A}\subseteq[m]$,

$$\dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i\right) \geq \min_{\mathcal{P}\,:\,\bigsqcup_{\mathcal{Q}\in\mathcal{P}}\mathcal{Q}=\mathcal{A}} \left\{\sum_{\mathcal{Q}\in\mathcal{P}} M_{\mathcal{Q}} - |\mathcal{P}|k\right\}. \quad (26)$$

We prove (26) by considering three different cases.

Case 1: $|\mathcal{A}|=1$, i.e., $\mathcal{A}=\{i\}$. For this case, V_i in (16) has $k+t-M_{\{i\}}$ rows. In particular, all these rows are linearly independent since: (i) the rows of V^T are linearly independent as V is a Vandermonde matrix, (ii) C_i is full row rank by construction, and (iii) any linear combination of the rows of V^T will have a weight of at least $t-k+1$ (from the Vandermonde property), whereas any linear combination of the rows of C_i will have a weight of at most $t-M_{\{i\}}\leq t-k$. It therefore follows that, $\forall i\in[3]$, we have that

$$\begin{aligned}\dim(\mathcal{N}_i) &= t-\dim(\mathcal{V}_i)\\ &= t-(k+t-M_{\{i\}})\\ &= M_{\{i\}}-k,\end{aligned}$$

where the first equality follows by using the rank-nullity theorem. Thus, (26) is satisfied.

Case 2: $|\mathcal{A}|=2$, i.e., $\mathcal{A}=\{i,j\}$. For this case, $\forall (i,j)\in[3]^2, i\neq j$, we have that

$$\begin{aligned}\dim(\mathcal{N}_i+\mathcal{N}_j) &= \dim(\mathcal{N}_i)+\dim(\mathcal{N}_j)\\ &\quad -\dim(\mathcal{N}_i\cap\mathcal{N}_j)\\ &= M_{\{i\}}+M_{\{j\}}-2k-\dim(\mathcal{N}_i\cap\mathcal{N}_j), \quad (27)\end{aligned}$$

where the second equality follows by using $\dim(\mathcal{N}_i)$ derived in Case 1. Thus, we need to compute $\dim(\mathcal{N}_i\cap\mathcal{N}_j)$. Note that, by definition, $\mathcal{N}_i\cap\mathcal{N}_j$ is the right null space of

$$V_{ij}^{\star}=\begin{bmatrix}V_i\\V_j\end{bmatrix}\overset{(16)}{=}\begin{bmatrix}V^T\\C_i\\C_j\end{bmatrix}=\begin{bmatrix}V^T\\C_{ij}\end{bmatrix},$$

where the last equality follows by removing one copy of the common rows in C_i and C_j, i.e., C_{ij} is a matrix of dimension $(t-M_{\cap\{i,j\}})\times t$, with all unique rows. Using a similar argument as in Case 1 (i.e., any vector in the span of V^T has a minimum weight of $t-k+1$ and any linear combination of the rows of C_{ij} will have a weight of at most $t-M_{\cap\{i,j\}}$), the number of linearly independent rows of $V_{ij}^{\star}$ is $\min\{t,t-M_{\cap\{i,j\}}+k\}$. Thus,

$$\begin{aligned}\dim(\mathcal{N}_i\cap\mathcal{N}_j) &= t-\min\{t,t-M_{\cap\{i,j\}}+k\}\\ &= \max\{0,M_{\cap\{i,j\}}-k\}\\ &= [M_{\cap\{i,j\}}-k]^+,\end{aligned}$$

where the first equality follows from the rank-nullity theorem. We can now write $\dim(\mathcal{N}_i+\mathcal{N}_j)$ from (27) as

$$\dim(\mathcal{N}_i+\mathcal{N}_j) = \min\left\{M_{\{i\}}+M_{\{i\}}-2k, M_{\{i,j\}}-k\right\}.$$

Thus, the condition in (26) is satisfied.

Case 3: $\mathcal{A}=\{1,2,3\}$. For this case, we will compute $\dim(\mathcal{N}_1+\mathcal{N}_2+\mathcal{N}_3)$ as

$$\dim(\mathcal{N}_1+\mathcal{N}_2+\mathcal{N}_3) = t-\dim(\mathcal{V}_1\cap\mathcal{V}_2\cap\mathcal{V}_3). \quad (28)$$

Towards this end, we would like to compute the number of linearly independent vectors $x\in\mathbb{F}_q^t$ that belong to $\mathcal{V}_1\cap\mathcal{V}_2\cap\mathcal{V}_3$. We start by noting that, similar to the case $k=1$, the positions of x corresponding to $[t]\setminus\cup_{i\in[3]}\mathcal{M}_i$ can be filled with any value in $\mathbb{F}_q$ and for this we have $q^{t-M_{\{1,2,3\}}}$ possible choices. We now select a permutation (i,j,ℓ) of $(1,2,3)$.

In order for x to belong to $\mathcal{V}_i$, the positions of x corresponding to $\mathcal{M}_i$ can be filled in q^k possible ways. This is because: (i) C_i in (16) has zeros in the positions specified by $\mathcal{M}_i$, and (ii) V^T has k rows. In other words, let $x_{\mathcal{M}_i}$ be the subvector of $x\in\mathbb{F}_q^t$ where only the components indexed by the set $\mathcal{M}_i$ are retained. Then, in order for x to belong to $\mathcal{V}_i$ we would need

$$x_{\mathcal{M}_i}=\sum_{y=1}^{k}\alpha_y V_{y,\mathcal{M}_i}^T,$$

where $\alpha_y\in\mathbb{F}_q, \forall y\in[k]$ and $V_{y,\mathcal{M}_i}^T$ is the y-th row of V^T where only the columns indexed by $\mathcal{M}_i$ are retained. Thus, we have q^k possible values that the coefficients α's can assume.

Then, to fill the positions of x specified by $\mathcal{M}_j$ so that $x\in\mathcal{V}_j$, we have *at most* $q^{[k-M_{\cap\{i,j\}}]^+}$ possible choices. This is because the positions of x corresponding to $\mathcal{M}_i\cap\mathcal{M}_j$ have already been fixed (when filling $x_{\mathcal{M}_i}$, i.e., the vector x in the positions specified by $\mathcal{M}_i$).

Finally, to fill the positions of x corresponding to $\mathcal{M}_\ell$ such that $x\in\mathcal{V}_\ell$, we have *at most* $q^{[k-M_{\cap\{\ell,\{i,j\}\}}]^+}$ possible choices. This is because, the positions of x corresponding to $\mathcal{M}_\ell\cap(\mathcal{M}_i\cup\mathcal{M}_j)$ have already been fixed (when filling $x_{\mathcal{M}_i\cup\mathcal{M}_j}$, i.e., the vector x in the positions specified by $\mathcal{M}_i\cup\mathcal{M}_j$). Thus, we obtain the following upper bound

$$\begin{aligned}\dim(\mathcal{V}_1\cap\mathcal{V}_2\cap\mathcal{V}_3)\leq\ & k+[k-M_{\cap\{i,j\}}]^+ +\\ & [k-M_{\cap\{\ell,\{i,j\}\}}]^+ +\\ & t-M_{\{1,2,3\}}.\end{aligned}$$

We observe that the upper bound above, in general, is not tight and it varies depending on the choice of the permutation of $(1,2,3)$. However, in Appendix F, we further tighten the upper bound for the quantity $\dim(\mathcal{V}_1\cap\mathcal{V}_2\cap\mathcal{V}_3)$, and we show that this new bound is invariant of the choice of the permutation of $(1,2,3)$. Moreover, we show that, when substituted in (28), this new bound satisfies the condition in (26). This proves that the scheme described in Section V-A securely achieves the rate region in Theorem 9.

E. Secure Capacity for Arbitrary Values of k and m

We here provide sufficient conditions for which the secure scheme in Section V-A is capacity achieving for arbitrary values of k and m. In particular, we have the following lemma.

Lemma 10: The scheme in Section V-A achieves the secure capacity region of a two-layer network with arbitrary values of k and m whenever $\mathcal{M}_{\cap\{i,j\}} \geq k$ for all $(i,j) \in [m]^2, i \neq j$.

Proof: We can compute $\dim(\cap_{i\in\mathcal{A}}\mathcal{V}_i)$ as follows

$$\begin{aligned}\dim(\cap_{i\in\mathcal{A}}\mathcal{V}_i) &\overset{(a)}{\leq} k + [k - \mathcal{M}_{\cap\{i_1,i_2\}}]^+ \\ &\quad + [k - \mathcal{M}_{\cap\{i_3,\{i_1,i_2\}\}}]^+ + \ldots \\ &\quad + [k - \mathcal{M}_{\cap\{i_{|\mathcal{A}|},\{i_1,i_2,\ldots,i_{|\mathcal{A}|-1}\}\}}]^+ \\ &\quad + t - M_{\mathcal{A}} \\ &\overset{(b)}{=} k + t - M_{\mathcal{A}},\end{aligned}$$

where $(i_1, i_2, \ldots, i_{|\mathcal{A}|})$ represents a permutation of the elements of $\mathcal{A}$ and: (i) the inequality in (a) follows by extending to arbitrary values of m the iterative algorithm proposed for Case 3 in Section V-D to fill the vector x so that $x \in \cap_{i\in\mathcal{A}}\mathcal{V}_i$ and (ii) the equality in (b) follows since

$$\mathcal{M}_{\cap\{i_j,\{i_1,i_2,\ldots,i_{j-1}\}\}} \geq \mathcal{M}_{\cap\{i_j,i_{j-1}\}} \geq k.$$

By using the property of dual spaces and the rank-nullity theorem, we obtain $\dim(\sum_{i\in\mathcal{A}}\mathcal{N}_i) \geq M_{\mathcal{A}} - k$, which satisfies the condition in (26) $\forall\mathcal{A} \subseteq [m]$. This concludes the proof of Lemma 10. □

Example 6: An example of a two-layer network that satisfies the condition in Lemma 10 is characterized by the following parameters (see Definition 4): $t = 10, m = 4, k = 6$, $\mathcal{M}_1 = \{1,2,3,4,5,6,7,8\}$, $\mathcal{M}_2 = \{3,4,5,6,7,8,9,10\}$, $\mathcal{M}_3 = \{1,2,5,6,7,8,9,10\}$ and $\mathcal{M}_4 = \{1,2,3,4,7,8,9,10\}$. ■

The results presented in this section provide the secure capacity region characterization for networks with: (i) arbitrary value m of destinations, and $k = 1$ edge eavesdropped by the adversary; (ii) arbitrary value k of edges eavesdropped and $m = 3$ destinations; (iii) arbitrary values for k and m under certain conditions on the min-cut capacities (see Lemma 10).

For arbitrary values of m and k for which the condition in Lemma 10 is not satisfied, we performed numerical evaluations by randomly constructing two-layer networks and, for all the cases we tried, we could not find any network for which the scheme is not optimal. In particular, in our simulations, we considered up to $m = 8$ destinations and, for different choices of t and k, we connected each destination to a randomly chosen set of relays. We constructed 100 such network instances, and verified that the rate region achieved by our designed scheme given in Lemma 7 equals the outer bound in (2). This suggests that our designed scheme could indeed be optimal for arbitrary values of m and k, and we conjecture this result to hold.

Conjecture 1: Consider a two-layer network with m destinations, where an adversary eavesdrops any k edges of her choice. The secure capacity region is given by

$$\sum_{i\in\mathcal{A}} R_i \leq |\cup_{i\in\mathcal{A}}\mathcal{M}_i| - k, \ \forall\mathcal{A} \subseteq [m],$$

where $\mathcal{M}_i \subseteq [t], \ i \in [m]$ denotes the destination connection sets.

F. Secure Capacity Scheme for Arbitrary Separable Networks

In this section, we will first show that for any separable network, a corresponding two-layer network can be created such that both networks have the same min-cut capacities $M_{\mathcal{A}}$ for all $\mathcal{A} \subseteq [m]$. We will then show that a secure scheme designed for a two-layer network can be converted to a secure scheme for the corresponding separable network.

By Definition 3, a separable network $\mathcal{G}$ with m destinations, can be separated into $2^m - 1$ networks $\mathcal{G}'_{\mathcal{J}}$, $\mathcal{J} \subseteq [m], \mathcal{J} \neq \emptyset$ where $\mathcal{G}'_{\mathcal{J}}$ has min-cut capacity $M'_{\mathcal{J}}$ to every subset of destinations in $\mathcal{J}$. To construct the corresponding two-layer network, we use the following iterative procedure:

1) We place the source node S in layer 0 of our network, and the m destination nodes $D_i, i \in [m]$, in layer 2 of our network;
2) For each $\mathcal{J} \subseteq [m]$, we add $M'_{\mathcal{J}}$ relays in layer 1 of our network;
3) For each $\mathcal{J} \subseteq [m]$, we connect: (i) the source in layer 0 with all the added $M'_{\mathcal{J}}$ relays, and (ii) all the added $M'_{\mathcal{J}}$ relays with the destinations $D_i, i \in \mathcal{J}$ in layer 2.

By following the above procedure, it is not difficult to verify that, for each $\mathcal{A} \subseteq [m]$, the min-cut capacity in the constructed two-layer network is $M_{\mathcal{A}}$ as given in (4). As such, the new constructed two-layer network has the same min-cut capacity $M_{\mathcal{A}}$ of the corresponding separable network. In what follows, we refer to the original separable network as *parent* separable network, and to the corresponding two-layer network as *child* two-layer network.

We now show that a secure scheme designed for the child two-layer network can be leveraged to build a secure scheme for the corresponding parent separable network. Towards this end, we assume that we have a secure scheme for the child two-layer network, i.e., as described in (15) in Section V-A, we have

$$X = \begin{bmatrix} H & V \end{bmatrix} \begin{bmatrix} W \\ K \end{bmatrix}.$$

Recall that, as highlighted in Remark 3, even if we select a random matrix $\tilde{V}$ instead of the Vandermonde matrix V, with a high probability (close to 1 for large field size) we will have a secure scheme for the child two-layer network.

To transform the above secure scheme into a secure scheme for the parent separable network, we proceed as follows. On every graph $\mathcal{G}'_{\mathcal{J}}$ in the parent separable network, we transmit (multicast) the symbols that were transmitted in the child two-layer network from the source node S in layer 0 to the set of $M'_{\mathcal{J}}$ relays in layer 1 that were added when constructing the child two-layer network for $\mathcal{G}'_{\mathcal{J}}$. Note that this multicast towards all destinations $D_i, i \in \mathcal{J}$, is possible since $\mathcal{G}'_J$ has min-cut capacity $M'_{\mathcal{J}}$. With such a strategy, at the end of the transmissions every destination in the parent separable graph still receives the same set of packets as it would have received in the child two-layer network. Thus, all the destinations can still decode their respective messages.

We now prove that this scheme is also secure. Let Y be the collection of the symbols transmitted (multicast) on the parent separable network, as described above. Since multicasting involves network coding, we have

$$Y = \left[\ G\ \right] X, \tag{29}$$

where G is an encoding matrix of dimension $|\mathcal{E}| \times M_{[m]}$, which can be constructed in $\mathcal{O}\left(m|\mathcal{E}|^3\right)$ by using the multicasting scheme of [4], which requires a finite field of dimension m. Thus,

$$\begin{aligned} Y &= \left[\ G\ \right] \left[\ H \quad \tilde{V}\ \right] \begin{bmatrix} W \\ K \end{bmatrix} \\ &= \left[\ GH \quad G\tilde{V}\ \right] \begin{bmatrix} W \\ K \end{bmatrix}. \end{aligned}$$

From the security condition in Lemma 1, it follows that the scheme above is secure if we can show that for any choice of G, there exists a $\tilde{V}$ such that $\tilde{V}$ is an MDS matrix (i.e., any k rows of $\tilde{V}$ are linearly independent) and

$$\begin{aligned} rk\left(\left[\ GHG\tilde{V}\ \right]\big|_{\mathcal{Z}}\right) = rk\left(\left[\ G\tilde{V}\ \right]\big|_{\mathcal{Z}}\right), \\ \forall |\mathcal{Z}| \leq k. \end{aligned} \tag{30}$$

This is shown in Appendix G, where we prove that over a sufficiently large finite field, with high probability a random choice of $\tilde{V}$ is an MDS matrix and satisfies the condition in (30).

VI. Two-Phase Scheme for Networks With Arbitrary Topologies and Arbitrary Number of Destinations

We now propose the design of a secure transmission scheme for networks with arbitrary topologies and arbitrary number of destinations. This scheme consists of two phases, namely the key generation phase (in which secret keys are generated between the source and the m destinations) and the message sending phase (in which the message packets are first encoded using the secret keys and then transmitted to the m destinations). In particular, this scheme is inspired by the work in [11], where it was shown that for multicast and single unicast connections, such a two-phase scheme that separates over time the transmissions of keys and messages indeed achieves the secure capacity. However, it turns out that this is no longer the case for multiple unicast sessions, as we discuss in detail in the following.

The secure rate region of this two-phase scheme is presented in Theorem 11.

Theorem 11: Let $(\hat{R}_1, \hat{R}_2, \ldots, \hat{R}_m)$ be an achievable rate m-tuple in the absence of the eavesdropper. Then, the rate m-tuple $(R_1, R_2, \ldots, R_m)$ with

$$R_i = \hat{R}_i \left[1 - \frac{k}{M}\right]^+, \forall i \in [m]\ , \tag{31}$$

where M is the minimum min-cut capacity between the source and any destination, is securely achievable in the presence of an adversary who eavesdrops any k edges of her choice.

Proof: Let $M_{\{i\}}$ be the min-cut capacity between the source and the destination D_i with $i \in [m]$. We define M as the minimum among all these individual min-cut capacities, i.e., $M = \min_{i\in[m]} M_{\{i\}}$. Let $(\hat{R}_1, \hat{R}_2, \ldots, \hat{R}_m) \in \mathbb{R}^m$ be the rate m-tuple achieved in the absence of the eavesdropper. We start by noting that if $k \geq M$, then (31) would evaluate to a zero rate towards each destination, which can always be achieved. Thus, we focus on the case $k < M$. We approximate the rate m-tuple $(\hat{R}_1, \hat{R}_2, \ldots, \hat{R}_m) \in \mathbb{R}^m$ with rational numbers; notice that this is always possible since the set of rationals $\mathbb{Q}$ is dense in $\mathbb{R}$. Since this rational rate m-tuple might involve fractional flows on the edges, we replace each edge with T parallel edges. We denote this new network as $\mathcal{G}_T$. The number T is chosen such that: (i) we achieve the rate m-tuple $(T\hat{R}_1, T\hat{R}_2, \ldots, T\hat{R}_m)$ over $\mathcal{G}_T$, and (ii) every edge in $\mathcal{G}_T$ carries an integer flow. In what follows, we describe our coding scheme and show that

$$(R_1, R_2, \ldots, R_m) = \left(1 - \frac{k}{M}\right)(\hat{R}_1, \hat{R}_2, \ldots, \hat{R}_m) \tag{32}$$

is securely achievable on $\mathcal{G}$. In particular, our scheme consists of two phases, namely the key generation phase and the message sending phase. Moreover, the key generation phase consists of k subphases, whereas the message sending phase consists of $M - k$ subphases. In each subphase, we use the network $\mathcal{G}_T$ for transmission. We also highlight that we allow the adversary to eavesdrop any Tk edges of $\mathcal{G}_T$. We next describe the two phases of our scheme.

- *Key generation.* This first phase – in which secure keys are established between the source and the destinations – consists of k subphases. In each subphase, the source multicasts $T(M-k)$ random packets securely to all destinations which will be used as secret keys in the message sending phase. This is possible thanks to the secure network coding result of [1], since the minimum min-cut capacity of $\mathcal{G}_T$ is TM and Eve has access to Tk edges. Thus, at the end of this phase, by transmitting TM random packets in each of the k subphases, a total of $Tk(M-k)$ secure keys are established between the source and the m destinations.
- *Message sending.* This phase consists of $M-k$ subphases. In each subphase, we choose Tk packets out of the $Tk(M-k)$ securely shared (in the key generation phase) random packets. For each choice of Tk packets, we convert the unsecure scheme achieving $(T\hat{R}_1, T\hat{R}_2, \ldots, T\hat{R}_m)$ to a secure scheme achieving the same rate m-tuple. Towards this end, we expand the Tk shared packets into $\sum_{j=1}^{m} T\hat{R}_j$ packets using an MDS code matrix. With this, we have the same number of random packets as the message packets. We then add the message packets with the random packets and transmit them as it was done in the corresponding unsecure scheme (i.e., in absence of the eavesdropper).

We highlight that the two phases of the proposed scheme (i.e., key generation and message sending) are presented separately just for ease of explanation and understanding. Secure communication over erasure and error free channels indeed requires that the source and destinations agree on the secure keys that are used to encode the message packets. This agreement can be reached through a *key generation* phase. Then, a *message sending* phase can be combined with the key

generation phase as a single code of a certain block length – which equals to nM over $\mathcal{G}_T$ – hence making the security aspect of the scheme consistent with Definition 1. In particular, n is determined by the field size required in the key generation and message sending phases and represents the block length of the code used in one subphase of the key generation or message sending phase over $\mathcal{G}_T$. Thus, this translates to a code of overall block length of nTM over $\mathcal{G}$.

Proof of security. For each of the $M-k$ subphases of the message sending phase, we denote by W_i the $T\hat{R}_i$ messages for D_i, and define W as

$$W = \begin{bmatrix} W_1 \\ W_2 \\ \dots \\ W_m \end{bmatrix}.$$

Moreover, we let K be the vector containing the Tk securely shared random packets. With this, for each of the $M-k$ subphases of the message sending phase, we can write the transmissions over the network $\mathcal{G}_T$ as

$$X = \begin{bmatrix} H_{us} & V \end{bmatrix} \begin{bmatrix} W \\ K \end{bmatrix}, \tag{33}$$

where H_{us} is the encoding matrix used in absence of the eavesdropper and V is the Vandermonde matrix of size $\sum_{i=1}^{m} T\hat{R}_i \times Tk$. Because of the property of Vandermonde matrices, (33) satisfies the security condition in Lemma 1, and hence the scheme above is secure. We also highlight that this Vandermonde matrix V always exists for any finite field of size $\sum_{i=1}^{m} \hat{R}_i$ or more. This follows because of the three following facts: (i) $\sum_{i=1}^{m} \hat{R}_i \geq M$ since, by definition, M is the minimum min-cut capacity between the source and any destination; (ii) $k < M$ since otherwise (31) would evaluate to a zero rate towards any destination; and (iii) $\sum_{i=1}^{m} \hat{R}_i > k$ from the two facts in (i) and (ii). Moreover, this matrix V can be created with a *constant* time complexity by selecting the element in the i-th row and j-th column of V to be $(\alpha_i)^{j-1}$ where the coefficients α_i's are distinct elements from the finite field.

We would like to emphasize that in our setting (according also to Definition 1) the adversary is assumed to eavesdrop any k edges of the network $\mathcal{G}$. For the two-phase scheme described above, from the original graph $\mathcal{G}$ we construct the new graph $\mathcal{G}_T$, where each edge in $\mathcal{G}$ has now been replaced by T parallel edges. Thus, if over the graph $\mathcal{G}$ the adversary was eavesdropping k edges, over $\mathcal{G}_T$ we now allow her to eavesdrop any Tk edges. However, the adversary is not allowed to change this set of Tk eavesdropped edges from one subphase to another. In other words, in each of the M subphases the adversary will always eavesdrop the same set of Tk edges. Note that this is also consistent with the description of the eavesdropper's capabilities in Definition 1. We also point out that, with this assumption of the adversary eavesdropping the same set of Tk edges in each subphase, the proposed two-phase scheme is secure since:

(i) After the k subphases of the key generation phase, the source and the m destinations have securely established $Tk(M-k)$ packets (referred to as secure keys), to which the adversary has no access;

(ii) In each of the $M-k$ subphases of the message sending phase, we transmit $\sum_{i=1}^{m} T\hat{R}_i$ new message packets by using Tk secure keys (out of the $Tk(M-k)$ keys generated in the key generation phase). Thus, it follows that each subphase of the message sending phase is using a set of independent keys from those used in a different subphase.

Analysis of the achieved rate m-tuple. The secure scheme described above requires a total of M subphases, where the first k subphases are from phase 1 (i.e., key generation) and the next $M-k$ subphases are from phase 2 (i.e., message sending). In particular, in the first k subphases, we generate the secure keys and in the remaining $M-k$ subphases, we securely transmit at rates of $(T\hat{R}_1, T\hat{R}_2, \dots, T\hat{R}_m)$. Thus, the achieved secure message rate $(R_1, R_2, \dots, R_m)$ is

$$R_j = \frac{M-k}{M}\hat{R}_j = \left(1 - \frac{k}{M}\right)\hat{R}_j, \forall j \in [m]\ . \tag{34}$$

This concludes the proof of Theorem 11. □

It is worth noting that the capacity region in absence of the eavesdropper was determined in [5, Theorem 9] (see also Lemma 14), and is given by

$$\sum_{i \in \mathcal{A}} R_i \leq M_{\mathcal{A}},\ \forall \mathcal{A} \subseteq [m].$$

By leveraging this result and (31), we can therefore compute the rate region achieved by our secure two-phase scheme, which is given in the next corollary.

Corollary 12: The achievable secure rate region of the two-phase scheme is given by

$$\sum_{i \in \mathcal{A}} R_i \leq M_{\mathcal{A}} - k\left(\frac{M_{\mathcal{A}}}{M}\right),\ \forall \mathcal{A} \subseteq [m],$$

where $M = \min_{i \in [m]} M_{\{i\}}$.

We now comment on the design complexity of this two-phase scheme and provide a trivial upper bound on the field size.

Lemma 13: The complexity of designing the secure two-phase transmission scheme equals $\mathcal{O}(m^3|\mathcal{E}|^3)$. Moreover, a field size of $\mathcal{O}(m + |\mathcal{E}|)$ suffices.

Proof: To design our two-phase scheme for a rate tuple $(R_1, R_2, \dots, R_m)$, we need to use k subphases for multicasting the keys and $M-k$ subphases for routing the multi-commodity information flow. Recall that M is the minimum of the min-cut capacities from the source to any destination $D_i,\ i \in [m]$, and as such M can be found in $\mathcal{O}(m|\mathcal{E}|^{2.5})$ [35] by solving m linear programs. The design of the deterministic matrix for multicasting the keys has a time complexity of $\mathcal{O}(|\mathcal{E}|mM(M+m))$ [4], which can be further upper bounded as $\mathcal{O}(|\mathcal{E}|^3 m)$. Finally, the design of the routing for multi-commodity flow can also be performed using a linear program which has a time complexity of $\mathcal{O}((m|\mathcal{E}|)^{2.5})$ [35]. Thus, the overall time complexity is $\mathcal{O}(m^3|\mathcal{E}|^3)$.

The field size required for constructing the deterministic multicast matrix is m [4]. We also require an MDS code for

encoding the message packets before routing. This requires a field size of $|\mathcal{E}|$ (corresponding to the Vandermonde or similar MDS matrix). Thus, a trivial bound on the field size requirement is $\mathcal{O}(m + |\mathcal{E}|)$. However, since our encoding schemes are linear, we believe that vector encoding schemes, such as the subspace coding scheme in [36], could be adapted to this case and leveraged to achieve a small finite field size. This is part of our current investigation. □

We conclude this section, by highlighting two fundamental features of our two-phase scheme:

1) Different from the scheme designed in Section V, which only applies to separable networks, the two-phase scheme applies to networks with *arbitrary* topologies.
2) The two-phase scheme is oblivious to the network structure, and uses all the network resources in both phases. In other words, different from the optimal scheme of Section IV for $m = 2$ destinations, the two-phase scheme does not seek to optimally separate the information and key flows. This causes the scheme to be suboptimal (see also Corollary 12) as also remarked by the detailed analysis in [30, Section 4.3].

VII. Comparisons and Non-Reversibility of Multiple Unicast Traffic

In this section, we make some comparisons and discuss properties of multiple unicast traffic. In particular, in Section VII-A, we compare the secure rate region for $m = 2$ destinations in Theorem 3 with the capacity region when the adversary is absent. The goal of this analysis is to quantify the rate loss that incurs to guarantee security. In Section VII-B, we prove that the secure capacity region for $m = 2$ destinations is non-reversible. Specifically, we show that, if we switch the role of the source and destinations and we reverse the directions of the edges, then the new secure capacity region differs from the original one. This is a surprising result since it implies that – different from the unsecure case where non-reversible networks must necessary have non-linear network coding solutions [37], [38] – under security constraints even networks with linear network coding solutions can be non-reversible if the traffic is multiple unicast.

A. Comparison With the Unsecure Capacity Region

The unsecure capacity region (i.e., capacity in the absence of the eavesdropper) for a multiple unicast network with a single source and multiple destinations described in Section II, is well known [5, Theorem 9] and given by the following lemma.

Lemma 14: The unsecure capacity region for the multiple unicast traffic over networks with single source node and m destination nodes is given by

$$R_{\mathcal{A}} \leq M_{\mathcal{A}}, \quad \forall \mathcal{A} \subseteq [m] \ , \tag{35}$$

where $R_{\mathcal{A}} := \sum_{i \in \mathcal{A}} R_i$ and $M_{\mathcal{A}}$ is defined in Definition 2.

By comparing (3) with (35) (evaluated for the case $m = 2$), we observe that in the presence of the eavesdropper, different from the unicast and multicast scenarios where we always lose a rate k in each dimension, in the multiple unicast case the loss might be strictly smaller than k per dimension. An example is given below to illustrate this.

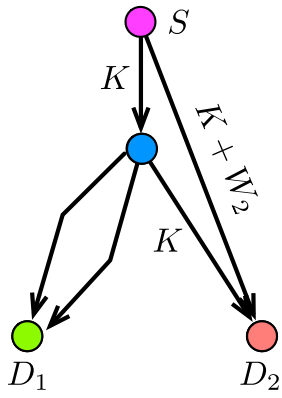
Example 7: Consider a network with a single source and $m = 2$ destinations with $M_{\{1\}} = 2$, $M_{\{2\}} = 2$ and $M_{\{1,2\}} = 3$. In the absence of any eavesdropper, according to (35) the rate pair $(1.5, 1.5)$ is Pareto optimal. However, in the case of an adversary eavesdropping any $k = 1$ edge of her choice, according to (3), the secure rate pair $(1, 1)$ is achievable, and hence only a rate of 0.5 per destination (i.e., dimension) is lost for security, as opposed to a loss of 1 per component for the unicast and multicast traffic.

B. Non-Reversibility of the Secure Capacity Region

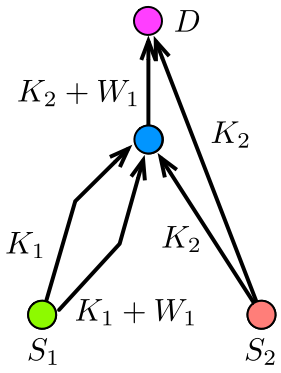
In order to characterize the unsecure capacity region in (35), network coding is not necessary and routing is sufficient (see also [5, Theorem 9]). Thus, from the result in [38], it directly follows that the capacity result in (35) is reversible. In particular, let $\mathcal{G}$ be a network with single source and m destinations with a certain capacity region (that can be computed from Lemma 14). Then, the reverse graph $\mathcal{G}'$ is constructed by switching the role of the source and destinations and by reversing the directions of the edges. Thus, $\mathcal{G}'$ will have m sources and one single destination. The result in [38] ensures that $\mathcal{G}$ and $\mathcal{G}'$ will have the same capacity region, i.e., the result in Lemma 14 characterizes also the unsecure capacity region for the multiple unicast traffic over networks with m sources and single destination.

We now focus on the secure case. In Section IV, we have characterized the secure capacity region for a multiple unicast network with single source and $m = 2$ destinations. In particular, Theorem 3 shows that the secure capacity region does not depend on the specific topology of the network and it can be fully characterized by the min-cut capacities $M_{\{1\}}, M_{\{2\}}$ and $M_{\{1,2\}}$ and by the number k of edges eavesdropped by Eve. We now show that this result is non-reversible, i.e., the secure capacity region of the reverse network is not the same as the one of the original network. Moreover, we also show that the secure capacity region of networks with 2 sources and a single destination cannot anymore be characterized by only the min-cut capacities, i.e., it also depends on the specific network topology.

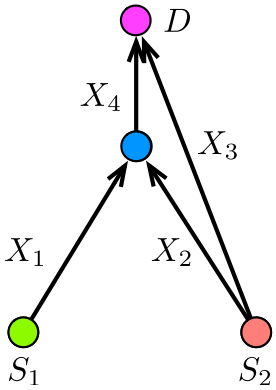
Consider the three networks in Fig. 4 and assume $k = 1$, i.e., Eve eavesdrops one edge of her choice. For the network in Fig. 4(a) we have min-cut capacities $\left(M_{\{1\}}, M_{\{2\}}, M_{\{1,2\}}\right) = (1, 2, 2)$ and hence from Theorem 3 it follows that a corner point for the secure capacity region for this network is given by $(R_1, R_2) = (0, 1)$. This point can be achieved by simply using the scheme shown in Fig. 4(a), where K represents the key and W_2 the message for D_2. Now, consider the network in Fig. 4(b) that is obtained from Fig. 4(a) by switching the role of the source and destinations and by reversing the directions of the edges. For this network, which has the same min-cut capacities as the network in Fig. 4(a), the rate pair $(R_1, R_2) = (1, 0)$ is securely achievable using the scheme shown in Fig. 4(b) where W_1 is the message of S_1 and K_1 and K_2 are the keys generated by S_1 and S_2, respectively. The rate pair $(R_1, R_2) = (1, 0)$, which is securely achieved



(a) $(R_1, R_2) = (0, 1)$ is capacity.



(b) $(R_1, R_2) = (1, 0)$ is achievable.



(c) $(R_1, R_2) = (1, 0)$ is not achievable.

Fig. 4. Network examples for non-reversibility.

by the network in Fig. 4(b), cannot be securely achieved by the network in Fig. 4(a). This result implies that a secure rate pair that is feasible for one network might not be feasible for the reverse network, i.e., the secure capacity regions can be different and hence cannot be derived from one another. The achievability of the pair $(R_1, R_2) = (1, 0)$ in Fig. 4(b) also shows that the outer bound in (2) does not hold for networks with single destination and multiple sources, in which case it is possible to achieve rates outside this region.

Consider now the network in Fig. 4(c). This network has the same min-cut capacities as the network in Fig. 4(b), i.e., $\left(M_{\{1\}}, M_{\{2\}}, M_{\{1,2\}}\right) = (1, 2, 2)$. We now show that the rate pair $(R_1, R_2) = (1, 0)$, which can be securely achieved in the network in Fig. 4(b), cannot be securely achieved in the network in Fig. 4(c). Let $X_i, i \in [4]$, be the transmitted symbols as shown in Fig. 4(c). With this, we have

$$\begin{aligned} R_1 &= H(W_1) \\ &\overset{(a)}{=} H(W_1) - H(W_1|X_3, X_4) \\ &\overset{(b)}{\leq} H(W_1) - H(W_1|X_1, X_2, X_3) \\ &= I(W_1; X_1, X_2, X_3) \\ &= I(W_1; X_1) + I(W_1; X_2, X_3|X_1) \\ &\overset{(c)}{=} I(W_1; X_2, X_3|X_1) \\ &= H(X_2, X_3|X_1) - H(X_2, X_3|W_1, X_1) \\ &\overset{(d)}{=} H(X_2, X_3) - H(X_2, X_3) = 0 \ , \end{aligned}$$

where: (i) the equality in (a) follows because of the decodability constraint; (ii) the inequality in (b) follows because of the 'conditioning reduces the entropy' principle and since X_4 is a deterministic function of (X_1, X_2); (iii) the equality in (c) follows because of the perfect secrecy requirement; (iv) finally, the equality in (d) follows since (X_2, X_3) is independent of (W_1, X_1). This result shows that the rate pair $(R_1, R_2) = (1, 0)$ is not securely achievable in the network in Fig. 4(c). This implies that, for a network with single destination and multiple sources, we cannot characterize the secure capacity region based only on the min-cut capacities $\left(M_{\{1\}}, M_{\{2\}}, M_{\{1,2\}}\right)$, i.e., the result would also depend on the specific network topology.

VIII. Conclusions and Open Questions

In this paper, we considered a source that aims to securely send private messages to m destinations, in the presence of a passive adversary that eavesdrops any k edges of her choice. We derived an outer bound expressed in terms of min-cut capacities, and designed schemes that achieve the secure capacity for the cases of (i) $m = 2$, k arbitrary, and arbitrary network topologies; (ii) $m = 3$, k arbitrary, two-layer and arbitrary separable network topologies; (iii) m arbitrary, $k = 1$, two-layer and arbitrary separable network topologies; (iv) m and k arbitrary for network topologies satisfying certain min-cut conditions. We note that in all these cases our achievable schemes are of polynomial-time complexity. However, unlike two-layer networks, for arbitrary separable networks, identifying the network separation may require an exhaustive search. This indicates that for arbitrary networks as well, identifying a capacity achieving scheme is a hard problem. Accordingly, we also proposed a suboptimal polynomial-time scheme that applies to all networks, arbitrary m and k, and for any subset of destinations $\mathcal{A} \subseteq [m]$, loses a maximum sum-rate of $k\left(\frac{M_{\mathcal{A}}}{M} - 1\right)$ compared to the outer bound (recall that $M_{\mathcal{A}}$ is the min-cut capacity between the source and the set of destinations in $\mathcal{A}$, and M is $\min_{i \in [m]} M_{\{i\}}$).

To the best of our knowledge, our work is the first to consider security for multiple unicast sessions over networks. Given this, several open questions remain, that include: (i) proving Conjecture 1; (ii) leveraging subspace codes or other vector coding designs that require smaller alphabet size; and (iii) deriving polynomial-time algorithms for arbitrary networks that perform close to the optimal.

Appendix A
Proof of Lemma 4

For completeness, we here report the proof of the result in Lemma 4, which is a direct consequence of [8, Theorem 1]. In particular, this result shows that any graph $\mathcal{G}$ with single source and $m = 2$ destinations is separable. The graph $\mathcal{G}$ has min-cut capacity $M_{\{i\}}, i \in [2]$, towards destination D_i and min-cut capacity $M_{\{1,2\}}$ towards $\{D_1, D_2\}$, from

which $M'_{\{i\}}, i \in [2]$, and $M'_{\{1,2\}}$ can be computed by using the expressions in (5). For any graph with two destinations, we represent this min-cut capacities triple, i.e., the min-cut capacity to destination D_1, the min-cut capacity to destination D_2, and the min-cut capacity to destination $\{D_1, D_2\}$ as:

$$\left(M_{\{1\}}, M_{\{2\}}, M_{\{1,2\}}\right) = \left(M'_{\{1\}}+M'_{\{1,2\}}, M'_{\{2\}}+M'_{\{1,2\}}, M'_{\{1\}}+M'_{\{2\}}+M'_{\{1,2\}}\right),$$

where the equality follows by using (5). We now prove Lemma 4 in two steps. We first show that the graph $\mathcal{G}$ can be separated into two graphs: $\mathcal{G}'_{\{1\}}$ with min-cut capacities $\left(M'_{\{1\}}, 0, M'_{\{1\}}\right)$ and $\mathcal{G}'_{res}$ with min-cut capacities

$$\left(M'_{\{1,2\}}, M'_{\{2\}}+M'_{\{1,2\}}, M'_{\{2\}}+M'_{\{1,2\}}\right) .$$

Then, by applying the same principle we further separate the graph $\mathcal{G}'_{res}$ into two graphs: $\mathcal{G}'_{\{2\}}$ with min-cut capacities $\left(0, M'_{\{2\}}, M'_{\{2\}}\right)$ and $\mathcal{G}'_{\{1,2\}}$ with min-cut capacities $\left(M'_{\{1,2\}}, M'_{\{1,2\}}, M'_{\{1,2\}}\right)$. This would complete the proof of Lemma 4.

We now prove that we can separate the graph $\mathcal{G}$ into the two graphs $\mathcal{G}'_{\{1\}}$ and $\mathcal{G}'_{res}$. Towards this end, from the original graph $\mathcal{G}$, we create a new directed acyclic graph $\mathcal{G}'$ where a new node D' is connected to D_1 through an edge of capacity $M'_{\{1\}}+M'_{\{1,2\}}$ and to D_2 through an edge of capacity $M'_{\{2\}}$. It is not difficult to see that in $\mathcal{G}'$ the min-cut capacity between S and D' is $M'_{\{1\}}+M'_{\{1,2\}}+M'_{\{2\}} = M_{\{1,2\}}$, where the equality follows from (5c). From the max-flow min-cut theorem, we can find $M_{\{1,2\}}$ edge-disjoint paths from S to D'; we color the edges in these paths *green*. We can also find $M_{\{2\}}$ edge-disjoint paths from S to D_2; we color the edges in these paths *red*. Notice that, at the end of this process, some of the edges can have both *green* and *red* colors. We also highlight that:

- Out of the $M_{\{1,2\}}$ *green* paths from S to D', $M'_{\{1\}}+M'_{\{1,2\}}$ paths flow through D_1 and $M'_{\{2\}}$ flow through D_2.
- If a path is exclusively *green*, it flows through D_1 since otherwise, in addition to the $M_{\{2\}}$ *red* edge-disjoint paths from S to D_2, we would have also this path and thereby violate the min-cut capacity constraint to D_2.

The second observation above implies that, if there are $M'_{\{1\}}$ exclusively *green* paths, then we can separate the graph $\mathcal{G}'$ into two graphs: $\mathcal{G}'_{\{1\}}$ that contains all these $M'_{\{1\}}$ exclusively *green* paths and $\mathcal{G}'_{res}$ that contains all the edges of $\mathcal{G}'$ that are not in $\mathcal{G}'_{\{1\}}$. Given this, by simply removing the node D' and its incoming edges, we get $\mathcal{G}'_{\{1\}}$ and $\mathcal{G}'_{res}$. We now show how we can obtain these $M'_{\{1\}}$ exclusively *green* paths. Towards this end, we denote with $\mathcal{P}$ the set of all *green* paths from S to D' (notice that these paths might have also some *red* edges). Then, until there exists a path $p \in \mathcal{P}$ such that either it is not exclusively *green* or it does not start with an edge that is both *red* and *green*, we apply the two following steps:

1) Let e be the first edge in p, which is both *green* and *red* and denote with g the *red* path from S to D_2 that contains the edge e. Recall that, since the $M_{\{2\}}$ *red* paths are edge-disjoint, there is only one *red* path g passing through e. We split the path p into two parts as p_1-e-p_2 and similarly we split the path g into g_1-e-g_2.
2) We add the *red* color to p_1 (that before was all *green*) and we remove the *red* color from g_1, i.e., now each edge in g_1 is either *green* or it does not have any color. Note that in this way we replace the *red* path g_1-e-g_2 with p_1-e-g_2 from source S to D_2, which is also disjoint from the rest of $M_{\{2\}}-1$ *red* paths.

We note that this process will stop only when all the $M_{\{1,2\}}$ paths from S to D' are either exclusively green or start with an edge that is both *red* and *green*. We also note that, since we did not remove any edge, clearly we also did not change any min-cut capacity during this process. Since initially there were $M_{\{2\}}$ *red* edges coming out of S and, in the process of the algorithm, we replaced one *red* by another *red*, then the number of *red* edges outgoing from S still remains the same. Thus, among the $M_{\{1,2\}}$ paths from S to D', only at most $M_{\{2\}}$ paths start with an edge that is both *green* and *red* and therefore, by using (5), at least $M'_{\{1\}}$ are exclusively *green* paths. This proves that the original graph $\mathcal{G}$ can be separated into the two graphs $\mathcal{G}'_{\{1\}}$ and $\mathcal{G}'_{res}$. By using similar arguments, one can then show that the graph $\mathcal{G}'_{res}$ can be separated into the two graphs $\mathcal{G}'_{\{2\}}$ and $\mathcal{G}'_{\{1,2\}}$. This concludes the proof of Lemma 4.

Appendix B
Proof of Security: Theorem 3, Case 1

We here prove that, for any choice of G, there exists a U in

$$X = \begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{bmatrix} \begin{bmatrix} W \\ K \end{bmatrix},$$

such that

$$rk\left(\left.\begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{bmatrix}\right|_{\mathcal{Z}}\right) = rk\left(\left.\begin{bmatrix} G \\ U \end{bmatrix}\right|_{\mathcal{Z}}\right) \tag{36}$$

for every $|\mathcal{Z}| \leq k$. Towards this end, we select a random matrix U and show that with high probability the condition in (36) is satisfied for a sufficiently large field. This proves the existence of such a matrix U. In particular, we have the set of equations in (37), shown at the bottom of the next page, where the labeled equalities follow from: (a) using the union bound; (b) the fact that $\binom{n}{t} \leq \left(\frac{en}{t}\right)^t$, and (d) considering sufficiently large q and arbitrary small values of ϵ. In order to show the inequality in (c), assume that $\mathcal{Z}$ corresponds to k_1 rows in $\begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \end{bmatrix}$ indexed by $\mathcal{Z}_1$ and k_2 rows in $\begin{bmatrix} I_{R_1+R_2} & U \end{bmatrix}$ indexed by $\mathcal{Z}_2$ with $k_1+k_2 \leq k$. With this, we have that

$$rk\left(\left.\begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{bmatrix}\right|_{\mathcal{Z}}\right) = \underbrace{rk\left(\left.\begin{bmatrix} G \end{bmatrix}\right|_{\mathcal{Z}_1}\right)}_{\hat{k}_1\leq k_1} + k_2.$$

This follows since, because of the structure of the matrix, the rows in the block $\begin{bmatrix} 0_{\ell\times(R_1+R_2)} & G \end{bmatrix}$ are linearly

independent of the rows in the block $\left[\begin{array}{cc} I_{R_1+R_2} & U \end{array}\right]$. Moreover, we have

$$rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right) = \hat{k}_1 + k_2,$$

with probability

$$p = \prod_{j=1}^{k_2}\left(1 - \frac{q^{\hat{k}_1+j-1}}{q^k}\right) \overset{(e)}{\geq} \prod_{j=1}^{k_2}\left(1-q^{-1}\right) = \left(1-\frac{1}{q}\right)^{k_2} \overset{(f)}{\geq} \left(1-\frac{1}{q}\right)^{k},$$

where: (i) the inequality in (e) follows since $\hat{k}_1 + j - 1 - k \leq -1$ for all $j \in [k_2]$, and (ii) the inequality in (f) follows since $k_2 \leq k$. This shows that the inequality in (c) above holds.

Appendix C
Proof of Security: Theorem 3, Case 2

We here prove that, for any choice of S and G satisfying $rk\left(\left[\begin{array}{cc} S & G \end{array}\right]\big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\big|_{\mathcal{Z}}\right)$ for all $|\mathcal{Z}| \leq k$, there exists a U in

$$X = \left[\begin{array}{ccc} S & 0_{\ell\times r} & G \\ 0_{r\times t} & I_r & U \end{array}\right]\left[\begin{array}{c} W' \\ W'' \\ K \end{array}\right],$$

such that

$$rk\left(\left[\begin{array}{ccc} S & 0_{\ell\times r} & G \\ 0_{r\times t} & I_r & U \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right) \tag{38}$$

for every $|\mathcal{Z}| \leq k$. Towards this end, we select a random U and show that with high probability the condition in (38) is satisfied for a sufficiently large field. This proves the existence of such a matrix U. By following similar steps as in the proof of Case 1 in Appendix B, we get set of equations in (39), shown at the bottom of the next page, where the inequalities in (a) and (b) follow by using similar arguments as in the proof of Case 1 in Appendix B.

Appendix D
Proof of Lemma 5

In this section, we use an iterative algorithm that, for any permutation $\pi = \{\pi(1), \ldots, \pi(m)\}$ of $[m]$, allows to select $R_{\pi(i)}$ vectors from $\mathcal{N}_{\pi(i)}$ (with $R_{\pi(i)}$ being defined in (19)) so that all the selected $\sum_{i=1}^{m} R_i$ vectors are linearly independent. We next illustrate the main steps of the proposed algorithm.

1) We select $R_{\pi(1)} = \dim(\mathcal{N}_{\pi(1)})$ independent vectors from $\mathcal{N}_{\pi(1)}$. Note that one possible choice for this consists of selecting the basis of the subspace $\mathcal{N}_{\pi(1)}$.
2) Next we would like to select independent vectors from $\mathcal{N}_{\pi(2)}$ that are also independent of the $R_{\pi(1)}$ vectors that we selected in the previous step. Towards this end, we note that a basis of the subspace $\mathcal{N}_{\pi(1)} + \mathcal{N}_{\pi(2)}$ is a subset of the union between a basis of $\mathcal{N}_{\pi(1)}$ and a basis of $\mathcal{N}_{\pi(2)}$. Therefore, we can keep selecting vectors from a basis of $\mathcal{N}_{\pi(2)}$ as long as we select an independent vector. Since there are $\dim(\mathcal{N}_{\pi(1)} + \mathcal{N}_{\pi(2)})$ independent vectors in a basis of $\mathcal{N}_{\pi(1)} + \mathcal{N}_{\pi(2)}$, then we can select
$$R_{\pi(2)} = \dim(\mathcal{N}_{\pi(1)} + \mathcal{N}_{\pi(2)}) - \dim(\mathcal{N}_{\pi(1)})$$
independent vectors from $\mathcal{N}_{\pi(2)}$ that are also independent of the $R_{\pi(1)}$ vectors that we selected in the previous step.
3) Similar to the above step, we now would like to select independent vectors from $\mathcal{N}_{\pi(3)}$ that are also independent of the $R_{\pi(1)} + R_{\pi(2)}$ vectors that we selected in the previous two steps. Towards this end, we note that

$$\Pr\left\{rk\left(\left[\begin{array}{cc} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right),\ \forall|\mathcal{Z}| \leq k\right\} \tag{37a}$$

$$= 1 - \Pr\left\{\bigcup_{|\mathcal{Z}|\leq k}\left[rk\left(\left[\begin{array}{cc} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{array}\right]\Big|_{\mathcal{Z}}\right) \neq rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right)\right]\right\} \tag{37b}$$

$$\overset{(a)}{\geq} 1 - \sum_{|\mathcal{Z}|\leq k}\Pr\left\{rk\left(\left[\begin{array}{cc} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{array}\right]\Big|_{\mathcal{Z}}\right) \neq rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\} \tag{37c}$$

$$\overset{(b)}{\geq} 1 - \left(\frac{e|\mathcal{E}|}{k}\right)^{k}\max_{|\mathcal{Z}|\leq k}\Pr\left\{rk\left(\left[\begin{array}{cc} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{array}\right]\Big|_{\mathcal{Z}}\right) \neq rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\} \tag{37d}$$

$$= 1 - \left(\frac{e|\mathcal{E}|}{k}\right)^{k}\max_{|\mathcal{Z}|\leq k}\left(1 - \Pr\left\{rk\left(\left[\begin{array}{cc} 0_{\ell\times(R_1+R_2)} & G \\ I_{R_1+R_2} & U \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\}\right) \tag{37e}$$

$$\overset{(c)}{\geq} 1 - \left(\frac{e|\mathcal{E}|}{k}\right)^{k}\max_{|\mathcal{Z}|\leq k}\left(1 - \left(1-\frac{1}{q}\right)^{k}\right) \tag{37f}$$

$$\overset{(d)}{>} 1 - \epsilon. \tag{37g}$$

a basis of the subspace $\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)}+\mathcal{N}_{\pi(3)}$ is a subset of the union between a basis of $\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)}$ and a basis of $\mathcal{N}_{\pi(3)}$. Therefore, we can keep selecting vectors from a basis of $\mathcal{N}_{\pi(3)}$ as long as we select an independent vector. Since there are $\dim(\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)}+\mathcal{N}_{\pi(3)})$ independent vectors in a basis of $\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)}+\mathcal{N}_{\pi(3)}$, then we can select

$$R_{\pi(3)} = \dim(\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)}+\mathcal{N}_{\pi(3)}) - \dim(\mathcal{N}_{\pi(1)}+\mathcal{N}_{\pi(2)})$$

independent vectors from $\mathcal{N}_{\pi(3)}$ that are also independent of the $R_{\pi(1)}+R_{\pi(2)}$ vectors that we selected in the previous two steps.

4) We keep using the iterative procedure above for all the elements in π, and we end up with $\sum_{i=1}^{m} R_i$ vectors that are linearly independent.

This concludes the proof of Lemma 5.

Appendix E
Proof of Lemma 7

In this section, we leverage the result in Lemma 5 to prove Lemma 7. We start by noting that the rate region in (20) can be expressed as the polyhedron in (40), shown at the bottom of the page, where $f(\mathcal{A}) := \dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i\right)$. We now prove the following lemma, which states that this function $f(\cdot)$ is a *non-decreasing* and *submodular* function over subsets of $[m]$.

Lemma 15: The set function

$$f(\mathcal{A}) := \dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i\right),\ \forall \mathcal{A}\subseteq[m]$$

is a non-decreasing and submodular function.

Proof: Let $\mathcal{A}\subset\mathcal{B}\subseteq[m]$, then

$$\begin{aligned} f(\mathcal{B}) &= \dim\left(\sum_{i\in\mathcal{B}}\mathcal{N}_i\right) \\ &= \dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i + \sum_{j\in\mathcal{B}\setminus\mathcal{A}}\mathcal{N}_j\right) \\ &\geq \dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i\right) = f(\mathcal{A}), \end{aligned}$$

which proves that the function $f(\cdot)$ is non-decreasing. For proving submodularity, consider two subsets $\mathcal{C},\mathcal{D}\subseteq[m]$. Then, we have

$$\begin{aligned} f(\mathcal{C}\cup\mathcal{D}) &= \dim\left(\sum_{i\in\mathcal{C}\cup\mathcal{D}}\mathcal{N}_i\right) \\ &= \dim\left(\sum_{i\in\mathcal{C}}\mathcal{N}_i + \sum_{j\in\mathcal{D}}\mathcal{N}_j\right) \\ &= \dim\left(\sum_{i\in\mathcal{C}}\mathcal{N}_i\right) + \dim\left(\sum_{j\in\mathcal{D}}\mathcal{N}_j\right) \\ &\quad - \dim\left(\left(\sum_{i\in\mathcal{C}}\mathcal{N}_i\right)\cap\left(\sum_{j\in\mathcal{D}}\mathcal{N}_j\right)\right) \\ &\leq \dim\left(\sum_{i\in\mathcal{C}}\mathcal{N}_i\right) + \dim\left(\sum_{j\in\mathcal{D}}\mathcal{N}_j\right) \\ &\quad - \dim\left(\sum_{k\in\mathcal{C}\cap\mathcal{D}}\mathcal{N}_k\right) \\ &= f(\mathcal{C}) + f(\mathcal{D}) - f(\mathcal{C}\cap\mathcal{D}), \end{aligned}$$

which proves that the function $f(\cdot)$ is submodular. □

Since $f(\cdot)$ is a submodular set function, then the polyhedron defined in (40) is the polymatroid associated with $f(\cdot)$. Moreover, since $f(\cdot)$ is also non-decreasing, then the corner points of the polymatroid in (40) can be found as follows [39, Corollary 44.3a]. Consider a permutation $\pi = \{\pi(1),\ldots,\pi(m)\}$ of $[m]$. Then, by letting $\mathcal{S}_\ell = \{\pi(1),\ldots,\pi(\ell)\}$ for $1\leq\ell\leq m$, we get that the corner points of the polymatroid in (40) can be written as $R_{\pi(\ell)} = f(\mathcal{S}_\ell) - f(\mathcal{S}_{\ell-1})$. Note that by using $f(\mathcal{A}) = \dim\left(\sum_{i\in\mathcal{A}}\mathcal{N}_i\right)$, the above corner points are precisely those in (19) in Lemma 5. Since each rate m-tuple $(R_1,R_2,\ldots,R_m)$, with $R_i, i\in[m]$ being defined in (19), can be securely achieved by our proposed scheme, it follows that the secure rate region in (20) can also be achieved by our scheme. This concludes the proof of Lemma 7.

$$\Pr\left\{rk\left(\left[\begin{array}{ccc} S & 0_{\ell\times r} & G \\ 0_{r\times t} & I_r & U \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right),\ \forall|\mathcal{Z}|\leq k\right\} \tag{39a}$$

$$\geq 1-\left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \max_{|\mathcal{Z}|\leq k}\left(1-\Pr\left\{rk\left(\left[\begin{array}{ccc} S & 0_{\ell\times r} & G \\ 0_{r\times t} & I_r & U \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G \\ U \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\}\right) \tag{39b}$$

$$\overset{(a)}{\geq} 1-\left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \max_{|\mathcal{Z}|\leq k}\left(1-\left(1-\frac{1}{q}\right)^k\right) \overset{(b)}{>} 1-\epsilon. \tag{39c}$$

$$P_f := \left\{R\in\mathbb{R}^{[m]} : R\geq\mathbf{0}, \sum_{i\in\mathcal{A}}R_i \leq f(\mathcal{A}),\ \forall\ \mathcal{A}\subseteq[m]\right\}. \tag{40}$$

APPENDIX F
ANALYSIS OF THE DIMENSION OF $(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3)$

From our analysis, we have obtained

$$\dim(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3) \leq k + [k - M_{\cap\{i,j\}}]^+ + [k - M_{\cap\{\ell,\{i,j\}\}}]^+ + t - M_{\{1,2,3\}}. \tag{42}$$

We now further consider two cases.

Case 3A: There exists a pair $(i,j) \in [3]^2, i \neq j$, such that $M_{\cap\{i,j\}} \geq k$. In this case, with the permutation (i,j,ℓ), the expression in (42) becomes

$$\begin{aligned}\dim(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3) &\leq k + [k - M_{\cap\{\ell,\{i,j\}\}}]^+ + t - M_{\{1,2,3\}} \\ &= t - M_{\{1,2,3\}} + \max\{2k - M_{\cap\{\ell,\{i,j\}\}}, k\}.\end{aligned}$$

From (28), this implies that

$$\begin{aligned}\dim(\mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3) &\geq M_{\{1,2,3\}} - \max\{2k - M_{\cap\{\ell,\{i,j\}\}}, k\} \\ &= \min\left\{M_{\{1,2,3\}} - k, M_{\{\ell\}} + M_{\{i,j\}} - 2k\right\},\end{aligned}$$

where the last equality follows since $M_{\{1,2,3\}} = M_{\{i,j\}} + M_{\{\ell\}} - M_{\cap\{\ell,\{i,j\}\}}$. With this, the condition in (26) is satisfied.

Case 3B: We have $M_{\cap\{i,j\}} < k, \forall (i,j) \in [3]^2, i \neq j$. In this case, we compute $\dim(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3)$ as follows: we first fill the positions of x indexed by $\mathcal{M}_1$, for which we have q^k possible choices; we then fill the positions of x indexed by $\mathcal{M}_2$, for which we have *at most* $q^{(k - M_{\cap\{1,2\}})}$ possible choices. However, by following this procedure, we may have fixed more than k positions of x corresponding to indexes in $\mathcal{M}_3$, which is not feasible. If that is the case, we *backtrack*, i.e., we remove the excess choices that we used for filling the positions of x indexed by $\mathcal{M}_2$. Thus,

1) If $M_{\cap\{3,\{1,2\}\}} \leq k$, then

$$\dim(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3) \leq t - M_{\{1,2,3\}} + k + (k - M_{\cap\{1,2\}}) + (k - M_{\cap\{3,\{1,2\}\}}).$$

This, from (28), implies

$$\dim(\mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3) \geq M_{\{1\}} + M_{\{2\}} + M_{\{3\}} - 3k,$$

which satisfies the condition in (26).

2) If $M_{\cap\{3,\{1,2\}\}} > k$, then

$$\dim(\mathcal{V}_1 \cap \mathcal{V}_2 \cap \mathcal{V}_3) \leq t - M_{\{1,2,3\}} + k + (k - M_{\cap\{1,2\}}) - \min\{k - M_{\cap\{1,2\}}, M_{\cap\{3,\{1,2\}\}} - k\}.$$

This, from (28), implies

$$\dim(\mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3) \geq \min\left\{M_{\{1,2,3\}} - k, M_{\{1\}} + M_{\{2\}} + M_{\{3\}} - 3k\right\},$$

which satisfies the condition in (26).

APPENDIX G
PROOF OF SECURITY: SEPARABLE NETWORKS

In this section, we show that for any choice of G of size $|\mathcal{E}| \times M_{[m]}$ with $M_{[m]} \geq k$, there exists a $\tilde{V}$ such that $\tilde{V}$ is an MDS matrix (i.e., any k rows of $\tilde{V}$ are linearly independent) and

$$rk\left(\left[\begin{array}{cc} GM & G\tilde{V} \end{array}\right]\Big|_{\mathcal{Z}}\right) = rk\left(\left[\begin{array}{c} G\tilde{V} \end{array}\right]\Big|_{\mathcal{Z}}\right), \ \forall |\mathcal{Z}| \leq k. \tag{43}$$

We start by noting that

$$\begin{aligned} rk\left(\left[\begin{array}{c} G\tilde{V} \end{array}\right]\Big|_{\mathcal{Z}}\right) &= rk\left(G|_{\mathcal{Z}} \cdot \tilde{V}\right) \\ &\leq rk\left(\left[\begin{array}{cc} GM & G\tilde{V} \end{array}\right]\Big|_{\mathcal{Z}}\right) \\ &= rk\left(G|_{\mathcal{Z}} \cdot \left[\begin{array}{cc} M & \tilde{V} \end{array}\right]\right) \\ &\leq rk\left(G|_{\mathcal{Z}}\right). \end{aligned}$$

Thus, if we prove that, for all $|\mathcal{Z}| \leq k$,

$$rk\left(G|_{\mathcal{Z}} \cdot \tilde{V}\right) = rk\left(G|_{\mathcal{Z}}\right), \tag{44}$$

then we also show that (43) holds. In what follows, we formally prove that a $\tilde{V}$ such that $\tilde{V}$ is an MDS matrix that satisfies the condition in (44) for all $|\mathcal{Z}| \leq k$ can be constructed with high probability. Towards this end, we let $\hat{k} = rk\left(G|_{\mathcal{Z}}\right)$, where $\hat{k} \leq k$ since $|\mathcal{Z}| \leq k$. We have set of equations in (41), shown at the bottom of the page, where: (i) the equality in (a) follows by using the De Morgan's laws, and (ii) the inequality in (b) follows since for two events A and B, we have $\Pr(A \cup B) \leq \Pr(A) + \Pr(B)$. We now further upper bound the two probability terms P_1 and P_2. For P_1, we obtain the set of equations in (45), shown at the bottom of the next page, where: (i) the equality in (c) follows by defining, for a given $\mathcal{Z}$ such that $|\mathcal{Z}| \leq k$, the event

$$A_{\mathcal{Z}} = \left\{rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}} \tilde{V}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\},$$

(ii) the equality in (d) follows by using the De Morgan's laws; (iii) the inequality in (e) follows by using the union bound; (iv) the inequality in (f) follows since $\binom{n}{t} \leq \left(\frac{en}{t}\right)^t$; (v) the inequality in (g) follows by defining the event $\hat{A}_{\mathcal{Z}}$ as

$$\hat{A}_{\mathcal{Z}} = \left\{rk\left(\hat{G}\hat{V}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}}\right)\right\},$$

$$\Pr\left\{\left\{rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}} \tilde{V}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}}\right), \ \forall |\mathcal{Z}| \leq k\right\} \cap \left\{\tilde{V} \text{ is MDS}\right\}\right\} \tag{41a}$$

$$\overset{(a)}{=} 1 - \Pr\left\{\left\{rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}} \tilde{V}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}}\right), \ \forall |\mathcal{Z}| \leq k\right\}^c \cup \left\{\tilde{V} \text{ is not MDS}\right\}\right\} \tag{41b}$$

$$\overset{(b)}{\geq} 1 - \underbrace{\Pr\left\{rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}} \tilde{V}\right) = rk\left(\left[\begin{array}{c} G \end{array}\right]\Big|_{\mathcal{Z}}\right), \ \forall |\mathcal{Z}| \leq k\right\}^c}_{P_1} - \underbrace{\Pr\left\{\tilde{V} \text{ is not MDS}\right\}}_{P_2}. \tag{41c}$$

where $\hat{G}$ is the matrix formed by the $\hat{k} = rk\left(\left[\ G\ \right]\big|_{\mathcal{Z}}\right)$ independent rows of $\left[\ G\ \right]\big|_{\mathcal{Z}}$, and $\hat{V}$ is formed by the first $\hat{k}$ columns of $\tilde{V}$. Thus, the inequality in (g) then follows since $\hat{A}_{\mathcal{Z}} \subseteq A_{\mathcal{Z}}$; (vi) the equality in (h) follows due to the following computation. We write

$$\hat{V} = \left[\ v_1 \quad v_2 \quad \dots \quad v_{\hat{k}}\ \right] \implies \hat{G}\hat{V} = \left[\ \hat{G}v_1 \quad \hat{G}v_2 \quad \dots \quad \hat{G}v_{\hat{k}}\ \right].$$

Note that the matrix $\hat{G}\hat{V}$ is of full rank (equal to $\hat{k}$) if the only solution to $\sum_{i=1}^{\hat{k}} c_i \hat{G} v_i = 0$ is $c_i = 0, \forall i \in [\hat{k}]$. Let $\hat{N}$ be the null space of $\hat{G}$, and $\hat{N}^{\perp}$ be the space such that $\hat{N}^{\perp} \cap \hat{N} = \emptyset$ and $\hat{N}^{\perp} \cup \hat{N} = \mathbb{F}_q^{M_{[m]}}$. Then, we can write each $v_i, i \in [\hat{k}]$, as the sum of its projection on $\hat{N}$ (say $v_i^{(a)}$) and the residual in $\hat{N}^{\perp}$ (say $v_i^{(b)}$). This implies that $\hat{G}\hat{V}$ is of full rank if the only solution to $\sum_{i=1}^{\hat{k}} c_i \hat{G} v_i^{(b)} = 0$ is $c_i = 0, \forall i \in [\hat{k}]$ (because $\hat{G}v_i^{(a)} = 0$). Since a random choice of v_i results in a random choice on $v_i^{(b)}$, then the probability of $\hat{G}\hat{V}$ being of full rank is equal to the probability that all the vectors $v_i^{(b)},\ i \in [\hat{k}]$ are mutually independent in $\hat{N}^{\perp}$. This probability, since $\dim(\hat{N}^{\perp}) = \hat{k}$, is equal to $\prod_{i=0}^{\hat{k}-1}\left(1 - \frac{q^i}{q^{\hat{k}}}\right)$; finally, (vii) the inequality in (i) follows since $i - \hat{k} \leq -1$ for all $i \in [0 : \hat{k} - 1]$ and $\hat{k} \leq k$.

For P_2, we obtain

$$\begin{aligned} P_2 &= \Pr\left\{\tilde{V} \text{ is not MDS}\right\} \\ &\overset{(j)}{=} \Pr\left\{\left(\bigcap_{\mathcal{S}:|\mathcal{S}|=k} A_s\right)^c\right\} \\ &\overset{(k)}{=} \Pr\left\{\bigcup_{\mathcal{S}:|\mathcal{S}|=k} (A_{\mathcal{S}})^c\right\} \\ &\overset{(\ell)}{=} \binom{M_{[m]}}{k} \Pr\left\{(A_{\mathcal{S}})^c\right\} \\ &= \binom{M_{[m]}}{k}\left(1 - \Pr\left\{A_{\mathcal{S}}\right\}\right) \\ &\overset{(m)}{=} \binom{M_{[m]}}{k}\left(1 - \prod_{i=0}^{k-1}\frac{q^k - q^i}{q^k}\right) \\ &\overset{(n)}{\leq} \binom{M_{[m]}}{k}\left(1 - \prod_{i=0}^{k-1}\left(1 - \frac{1}{q}\right)\right) \\ &= \binom{M_{[m]}}{k}\left(1 - \left(1 - \frac{1}{q}\right)^k\right), \end{aligned}$$

where: (i) the equality in (j) follows by defining, for a given $\mathcal{S}$ such that $|\mathcal{S}| = k$, the event

$$A_{\mathcal{S}} = \left\{\tilde{V}|_{\mathcal{S}} \text{ is full rank}\right\},$$

(ii) the equality in (k) follows by using the De Morgan's laws; (iii) the equality in (ℓ) follows by selecting uniformly at random all the subsets of k rows out of the $M_{[m]}$ rows, (iv) the equality in (m) follows by counting arguments to ensure that the k selected rows are all independent, and (v) the inequality in (n) follows since $i - k \leq -1$ for all $i \in [0 : k - 1]$.

Thus, we obtain the set of equations in (46), shown at the bottom of the page, where the last inequality holds for sufficiently large values of q and arbitrary small values of ϵ.

$$P_1 = \Pr\left\{rk\left(\left[\ G\ \right]\big|_{\mathcal{Z}}\tilde{V}\right) = rk\left(\left[\ G\ \right]\big|_{\mathcal{Z}}\right),\ \forall |\mathcal{Z}| \leq k\right\}^c \tag{45a}$$

$$\overset{(c)}{=} \Pr\left\{\left(\bigcap_{\mathcal{Z}:|\mathcal{Z}|\leq k} A_{\mathcal{Z}}\right)^c\right\} \overset{(d)}{=} \Pr\left\{\bigcup_{\mathcal{Z}:|\mathcal{Z}|\leq k} (A_{\mathcal{Z}})^c\right\} \overset{(e)}{\leq} \sum_{\mathcal{Z}:|\mathcal{Z}|\leq k} \Pr\left\{(A_{\mathcal{Z}})^c\right\} \tag{45b}$$

$$\overset{(f)}{\leq} \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \max_{\mathcal{Z}:|\mathcal{Z}|\leq k} \Pr\left\{(A_{\mathcal{Z}})^c\right\} = \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \max_{\mathcal{Z}:|\mathcal{Z}|\leq k} \left(1 - \Pr\left\{A_{\mathcal{Z}}\right\}\right) \tag{45c}$$

$$\overset{(g)}{\leq} \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \max_{\mathcal{Z}:|\mathcal{Z}|\leq k} \left(1 - \Pr\left\{\hat{A}_{\mathcal{Z}}\right\}\right) \tag{45d}$$

$$\overset{(h)}{=} \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \left(1 - \prod_{i=0}^{\hat{k}-1}\left(1 - \frac{q^i}{q^{\hat{k}}}\right)\right) \tag{45e}$$

$$\overset{(i)}{\leq} \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \left(1 - \left(1 - \frac{1}{q}\right)^k\right). \tag{45f}$$

$$\Pr\left\{\left\{rk\left(\left[\ G\ \right]\big|_{\mathcal{Z}}\tilde{V}\right) = rk\left(\left[\ G\ \right]\big|_{\mathcal{Z}}\right),\ \forall |\mathcal{Z}| \leq k\right\} \cap \left\{\tilde{V} \text{ is MDS}\right\}\right\} \tag{46a}$$

$$\geq 1 - \left(\frac{\mathrm{e}|\mathcal{E}|}{k}\right)^k \left(1 - \left(1 - \frac{1}{q}\right)^k\right) - \binom{M_{[m]}}{k}\left(1 - \left(1 - \frac{1}{q}\right)^k\right) \tag{46b}$$

$$> 1 - \epsilon. \tag{46c}$$

REFERENCES

[1] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2002, p. 323.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[3] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[4] S. Jaggi *et al.*, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1973–1982, Jun. 2005.

[5] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[6] S. U. Kamath, D. N. C. Tse, and V. Anantharam, "Generalized network sharing outer bound and the two-unicast problem," in *Proc. Int. Symp. Netw. Coding (NetCod)*, Jul. 2011, pp. 1–6.

[7] S. Kamath, D. N. C. Tse, and C.-C. Wang, "Two-unicast is hard," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2014, pp. 2147–2151.

[8] A. Ramamoorthy and R. D. Wesel, "The single source two terminal network with network coding," Aug. 2009, *arXiv:0908.2847*. [Online]. Available: https://arxiv.org/abs/0908.2847

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[11] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. Diggavi, "Secret message capacity of erasure broadcast channels with feedback," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2011, pp. 65–69.

[12] J. Feldman, T. Malkin, C. Stein, and R. Servedio, "On the capacity of secure network coding," in *Proc. 42nd Annu. Allerton Conf. Commun., Control, Comput.*, 2004, pp. 63–68.

[13] S. Y. El Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 551–555.

[14] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with nonuniform or restricted wiretap sets," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 166–176, Jan. 2013.

[15] C.-K. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1136–1143, Feb. 2011.

[16] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

[17] K. Bhattad *et al.*, "Weakly secure network coding," in *Proc. NetCod*, Apr. 104, 2005.

[18] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *Proc. IEEE Inf. Theory Workshop Netw. Inf. Theory*, Jun. 2009, pp. 281–285.

[19] Y. Wei, Z. Yu, and Y. Guan, "Efficient weakly-secure network coding schemes against wiretapping attacks," in *Proc. IEEE Int. Symp. Netw. Coding (NetCod)*, Jun. 2010, pp. 1–6.

[20] S. Jaggi *et al.*, "Resilient network coding in the presence of Byzantine adversaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.

[21] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2004, p. 144.

[22] O. Kosut, L. Tong, and D. Tse, "Nonlinear network coding is necessary to combat general Byzantine attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 593–599.

[23] A. Papadopoulos, L. Czap, and C. Fragouli, "LP formulations for secrecy over erasure networks with feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 954–958.

[24] L. Czap, V. M. Prabhakaran, S. Diggavi, and C. Fragouli, "Triangle network secrecy," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 781–785.

[25] A. Papadopoulos, L. Czap, and C. Fragouli, "Secret message capacity of a line network," 2014, *arXiv:1407.1922*. [Online]. Available: http://arxiv.org/abs/1407.1922

[26] A. Mills, B. Smith, T. C. Clancy, E. Soljanin, and S. Vishwanath, "On secure communication over wireless erasure networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 161–165.

[27] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure network coding for wireless mesh networks: Threats, challenges, and directions," *Comput. Commun.*, vol. 32, no. 17, pp. 1790–1801, Nov. 2009.

[28] G. K. Agarwal, M. Cardone, and C. Fragouli, "Coding across unicast sessions can increase the secure message capacity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2134–2138.

[29] G. K. Agarwal, M. Cardone, and C. Fragouli, "On secure network coding for two unicast sessions: Studying butterflies," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[30] G. V. Agarwal, M. Cardone, and C. Fragouli, "Secure network coding for multiple unicast: On the case of single source," in *Information Theoretic Security*, J. Shikata, Ed. Cham, Switzerland: Springer, 2017, pp. 188–207.

[31] N. Cai and M. Hayashi, "Secure network code for adaptive and active attacks with no-randomness in intermediate nodes," 2018, *arXiv:1712.09035*. [Online]. Available: https://arxiv.org/abs/1712.09035

[32] N. Cai and R. W. Yeung, "A security condition for multi-source linear network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 561–565.

[33] K. Kurosawa, H. Ohta, and K. Kakuta, "How to make a linear network code (strongly) secure," *Des., Codes Cryptogr.*, vol. 82, no. 3, pp. 559–582, Mar. 2017.

[34] D. Andrén, L. Hellström, and K. Markström, "On the complexity of matrix reduction over finite fields," *Adv. Appl. Math.*, vol. 39, no. 4, pp. 428–452, Oct. 2007.

[35] P. M. Vaidya, "Speeding-up linear programming using fast matrix multiplication," in *Proc. 30th Annu. Symp. Found. Comput. Sci.*, Oct. 1989, pp. 332–337.

[36] A. Khaleghi, D. Silva, and F. R. Kschischang, "Subspace codes," in *Cryptography Coding*, M. G. Parker, Ed. Berlin, Germany: Springer, 2009, pp. 1–21.

[37] R. Koetter, M. Effros, and T. Ho, "Network codes as codes on graphs," in *Proc. Conf. Inf. Sci. Syst. (CISS)*, 2004, pp. 1–6.

[38] S. Riis, "Reversible and irreversible information networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4339–4349, Nov. 2007.

[39] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, vol. B. Springer, 2003.

Gaurav Kumar Agarwal received the B.Tech. degree in electronics and communication engineering from the Indian Institute of Technology Roorkee, the M.Eng. degree in telecommunication engineering from the Indian Institute of Science, Bengaluru, and the Ph.D. degree from the ECE Department, UCLA. He was an Intern with Cranfield University–Shrivenham, and Technicolor Research, Los Altos, in 2011 and 2016, respectively.

Martina Cardone received the Ph.D. degree in electronics and communications from Télécom ParisTech (with work done at Eurecom in Sophia Antipolis, France) in 2015. From November 2017 to January 2018, she was a Post-Doctoral Associate with the Electrical and Computer Engineering Department, UMN. From July 2015 to August 2017, she was a Post-Doctoral Research Fellow with the Electrical and Computer Engineering Department, UCLA Henri Samueli School. She is currently an Assistant Professor with the Electrical and Computer Engineering Department, University of Minnesota (UMN). Her main research interests are in network information theory, network coding, and wireless networks with special focus on their capacity, security and privacy aspects. She was a recipient of the NSF CRII Award in 2019, the second prize in the Outstanding Ph.D. Award, Télécom ParisTech, Paris, France, and the Qualcomm Innovation Fellowship in 2014.

Christina Fragouli (Fellow, IEEE) received the B.S. degree in ECE from the National Technical University of Athens, Athens, Greece, and the M.Sc. and Ph.D. degrees in EE from the University of California, Los Angeles (UCLA). She is currently a Professor with the ECE Department, UCLA. Her current research interests are in network security and privacy, wireless networks, and machine learning under communication constraints. She has served as an Information Theory Society Distinguished Lecturer, and as an Associate Editor for the IEEE COMMUNICATIONS LETTERS, journal on *Computer Communication* (Elsevier), the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON INFORMATION THEORY, and the IEEE TRANSACTIONS ON MOBILE COMMUNICATIONS.