# Network Coding Multicast Key-Capacity

Michael Langberg          Michelle Effros

arXiv:2202.03918v2 [cs.IT] 19 May 2022

*Abstract*—For a multi-source multi-terminal noiseless network, the *key-dissemination* problem involves the task of multicasting a secret key $K$ from the network sources to its terminals. As in secure multicast network-coding, in the key-dissemination problem the source nodes have access to independent randomness and, as the network is noiseless, the resulting key $K$ is a function of the sources' information. However, different from traditional forms of multicast, in key-dissemination the key $K$ need not consist of source messages, but rather may be *any* function of the information generated at the sources, as long as it is shared by all terminals. Allowing the shared key $K$ to be a mixture of source information grants a flexibility to the communication process which gives rise to the potential of increased key-rates when compared to traditional secure multicast. The multicast *key-capacity* is the supremum of achievable key-rates, subject to the security requirement that the shared key is not revealed to an eavesdropper with predefined eavesdropping capabilities. The key-dissemination problem (termed also, secret key-agreement) has seen significant studies over the past decades in memoryless network structures. In this work, we initiate the study of key-dissemination in the context of noiseless networks, i.e., network coding. In this context, we study similarities and differences between traditional secure-multicast and the more lenient task of key-dissemination.

## I. INTRODUCTION

A *key-dissemination* communication protocol is one in which a key $K$, which is at times secret, is shared among a collection of users as a prelude to future communication tasks requiring shared user common knowledge. The task of key dissemination (termed also, secret key-agreement) has seen significant studies over the past decades in memoryless network structures, e.g., [1]–[13] in which a collection of nodes wish to share a common key over a noisy network structure which is subject to eavesdropping. Typical network structures in the studies above include a broadcast channel enhanced with a public noiseless-channel, where the key is generated at the source node and the eavesdropper has both noisy access to the broadcasted information and noiseless access to the public channel. Remarkably, the public channel improves on the achievable key rate despite being completely exposed to eavesdropping.

This work initiates the study of key-dissemination in the context of noiseless networks, i.e., in the context of Network Coding. Roughly speaking, for a multi-source, multi-terminal network, in the key-dissemination problem one wishes to multicast a key $K$ of rate $R$ from a collection of sources to a collection of terminal nodes. Sources have access to

M. Langberg is with the Department of Electrical Engineering at the University at Buffalo (State University of New York). Email: mikel@buffalo.edu

M. Effros is with the Department of Electrical Engineering at the California Institute of Technology. Email: effros@caltech.edu

independent randomness, and, as the network is noiseless, the resulting key $K$ is a function of the sources' information. However, unlike traditional forms of secure multicast, there is no requirement on $K$ beyond the following three constraints. First, $K$ should be delivered to all terminal nodes, second, $K$ should not be revealed to an eavesdropper with predefined eavesdropping capabilities, and third, $K$ is uniform and has rate at least $R$. Allowing the shared key $K$ to be any function of the source information grants a flexibility to the communication process which gives rise to the potential of increased key-rates when compared to traditional secure multicast. Given a network instance, one seeks to determine the *key-capacity*, naturally defined as the closure of all achievable key rates. Formal definitions of the concepts above (and additional ones that appear below) are given in detail in Section II.

The eavesdropper capabilities in the model under study may differ depending on the motivation at hand. For example, one may consider the extreme scenario in which every network node is considered a malicious entity; here, we require that for each non-terminal network node $v$, *including* each source node contributing to the randomness determining $K$, the information passing through $v$ is independent of $K$. Figure 1.a depicts an example. This scenario may be appropriate for network protocols that share a secret key between a pair of users to later be used as a one-time-pad for the secure communication of sensitive information.

On the other extreme, consider a setting in which no security is required. Such a setting may be applicable for communication among trusted parties. Now, key-dissemination becomes the task of communicating *any form* of shared information $K$ to the network terminals without constraining what other network components may learn. While this setting resembles that of traditional (non-secure) communication, it leaves open the possibility of increased rate due to the possibility that $K$ may be any function of the sources but need not be sufficient to reconstruct source information.

### A. Related work

The problem of network-coding, multi-source, multi-terminal, key-dissemination is closely related to the task of *secure "wiretap" multicast network coding* in which the goal is to securely multicast source information to a collection of terminals in the presence of an eavesdropper with, as above, predefined eavesdropping capabilities. In full generality, the model of secure multicast network-coding distinguishes between source nodes that have access to message information, and nodes that generate independent randomness used to enable secure communication. The majority of prior works study single-source multicast in which the single source node generates both messages and independent randomness, i.e., no

additional network nodes can generate randomness, and the eavesdropper can access any collection of up-to $z$ network links for a security parameter $z$, e.g., [14]–[20]. A major result in this context includes a characterization of the secure multicast capacity, which can be efficiently obtained by linear codes.

The model in full generality, where several network nodes may generate messages and/or independent randomness, is studied in, e.g., [21]–[26]; its capacity is less well understood. Specifically, [23] shows that determining the secure-multicast capacity in instances with a single message-generating source, a single terminal, and certain eavesdropping capabilities is NP-Hard; [21], [22] show, for single-source, single-terminal settings in which the eavesdropper can access any single ($z = 1$) edge in the network (each of unit capacity), that determining the secure-rate when any node can generate random keys is as hard as the problem of characterizing the (non-secure) capacity region of the $k$-unicast problem. The $k$-unicast problem is a well known open problem in the study of network codes, e.g., [22], [27]–[29].

Secure network coding and key-dissemination are similar in the sense that the information eventually shared between terminals is kept secret from the network eavesdropper. They differ in that in the former source nodes hold message information that must be recovered while in the latter the key $K$ may be any function of the independent randomness held by the source nodes. The flexible decoding in key-dissemination opens the possibility of a key-rate $R$ that exceeds the secure-multicast capacity. The study at hand addresses the differences and similarities between key-dissemination and secure-multicast. Our results are summarized in Section I-B.

The problem of key-dissemination is related to other tasks beyond that of secure multicast. Examples include network coding scenarios in which the communicated information is something other that pure source bits. For example, network coding function-communication, e.g., [30]–[32], in which a predetermined function of the source information, such as a sum of source values [33]–[37], is to be shared between all terminal nodes. Sum function network codes might lend themselves to the problem of key-dissemination, as a key $K$ set to be the sum of all source information is independent of partial sums (including individual source randomness) communicated over network edges. Two networks illustrating key dissemination using sum function network codes are depicted in Figure 1. As with secure multicast in it general form, determining the capacity of sum networks is as hard as determining the capacity of multiple-unicast network coding [34]; this is shown through a reduction implying, rather counter intuitively, that linear codes do not suffice to achieve capacity in sum-networks.

In both secure-multicast and functional-communication, the information transmitted is required to be a certain predetermined function of the source information. *Pliable index coding* [38] is an example prior work in which the information decoded at terminals is of a flexible nature loosely reminiscent of the flexibility of the key $K$ in the key-dissemination problem. Index coding is a representative form of multiple-unicast network coding [39]–[41] in which a server holding all
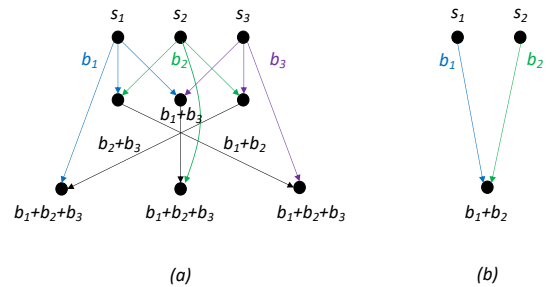


Fig. 1: Two simple example networks expressing the difference between secure-multicast and key-dissemination. Source $s_i$ generates random bit $b_i$. Terminals appear on the lowest layer of the networks. All edges are of capacity 1. Networks *(a)* and *(b)* are examples in which the key-dissemination capacity is 1, with $K$ being the sum-of-sources, even when the eavesdropper is capable of accessing all information available to any single non-terminal node of the network (including the source nodes). The secure-multicast capacity with such an eavesdropper is 0. While Network *(b)* is a trivial such example, Network *(a)* also acts as a simplified example for the proof of Theorem 3.4 exhibiting a multiplicative advantage of $\alpha = 2$ to answer Question 1 *"To mix or not to mix,"* with a definitive demonstration that mixing offers a rate advantage (giving $\mathbf{R}_{\text{key}}(\mathcal{I}) = 1$ and $\mathbf{R}_{\text{key}(2)}(\mathcal{I}) = 0.5$).

source messages wishes to communicate through a capacity-limited noiseless broadcast channel with multiple terminals, each holding potentially distinct message side-information and requiring potentially distinct messages. Pliable index coding [38] is a variant of index coding in which terminals are required to decode not a specific source message, but *any* message they do not already have as side information, a flexibility implying significant rate advantages when compared to traditional index coding. Various forms of security in the context of index coding and pliable index-coding have been studied, e.g., in [42]–[45].

Finally, the problem of secret-key generation in the context of wireless networks using the methodology of network coding (i.e., that of performing coding operations at internal network nodes) has appeared, for example, in the context of sensor networks [46], dynamic wireless systems [47], and multiresolutional streaming [48]. The models, questions, and results of the works above differ significantly from those presented in this work.

### B. Main questions and results addressed in this work

In this work we study the relationship between the key-dissemination problem and the traditional secure-multicast problem. Our study is guided by the following two questions:

*Question 1:* **To mix or not to mix?** *Does the flexibility allowing $K$ to be any function of source randomness improve the rate of communication when compared to traditional communication, in which pre-specified messages must be decoded at terminals. In other words, does allowing terminals the ability to directly decode a* mixture *of source randomness hold rate benefits?*

*Question 2:* **How hard is key-dissemination?** *While efficient, capacity-achieving codes for non-secure (multiple-source) multicast network coding and for certain settings of secure multicast are well understood, and the design of such codes for other settings of secure multicast is currently open, what can be said for the key-dissemination problem regarding the tasks of determining the capacity and mastering code-design?*

In our study of the key-dissemination problem, we present the following results. Our results are presented below in a loose manner and stated rigorously after our model is presented in Section II.

*1) Single-source case:* When only one source can generate randomness, we show that key-dissemination is equivalent to secure multicast. Namely, with respect to Question 1, there is no benefit in this setting to solutions that "mix," i.e., to solutions in which terminals directly decode a mixture of source randomness. Moreover, with respect to Question 2, code design and capacity are well understood for certain eavesdropping capabilities and are open for others; this corresponds to the state of the art for secure multicast. Our results for the single-source case are presented in Theorem 3.1.

*2) Non-secure case:* In the non-secure multi-source setting of key-dissemination, one wishes to establish shared randomness $K$ among terminal nodes, but does not need to protect $K$ from other network components. While this setting resembles that of traditional (non-secure) multicast, it leaves open the possibility that directly decoding a "mixture" of source randomness (in the sense of Question 1) may increase the key rate. For linear codes, which are capacity achieving for traditional (non-secure) multi-source multicast network coding, we show in Theorem 3.2 that mixing does not help, thus resolving Question 1 in the negative. For general codes in the non-secure case, Questions 1 and 2 remain open and are subject to future work.

*3) General case, complexity:* We study Question 2 in the context of key dissemination and show in Theorem 3.3 and Corollary 3.1 that computing the capacity of the key dissemination problem even when only single edges may be eavesdropped, is as hard as determining the multiple-unicast network coding capacity. Our hardness result is based on reducing hard instances of secure multicast to the key-dissemination problem.

*4) General case, mixing:* Finally, we study Question 1 in the context of key dissemination in its general form. For multi-source key-dissemination, depending on the eavesdropping capabilities, it is not hard to construct simple instances that have large key-dissemination rate while the corresponding secure-multicast rate is zero. As a result, mixing has an advantage here. Two such instances are given in Figure 1. In each we assume that the eavesdropper has access to source nodes, and therefor it is necessary for each source random variable to be independent from the shared key $K$. Such a stringent security requirement does not allow a positive secure-multicast rate, but mixing at terminal nodes may allow a large key-dissemination rate.

To better understand the potential benefits in allowing the decoders to *directly* decode a mixture of source randomness,

we compare between two potential decoding procedures in the context of key-dissemination. First consider a 2-stage decoding procedure in which each terminal starts by decoding source information (as in the setting of secure-multicast) and only then proceeds in defining $K$ to be a function of the decoded source information from the first stage. For example, as in Figure 1.b, one may consider a terminal that decodes, in the first stage, message $b_1$ from source 1 and $b_2$ from source 2, and defines the key $K$ to be the sum $b_1 + b_2$ in the second stage. The information held by each source is not independent of the decoded information $(b_1, b_2)$ of the first stage, but is independent of the final key $K$. Implying that, while the secure-multicast rate in this case is zero, one can still obtain a key $K$ from first decoding source messages and then combining them in a secure way to form $K$. Such 2-stage decoders (defined in detail in Section III) are natural for key dissemination; however, they may still be inferior when compared to unrestricted decoders that can directly decode $K$ from their incoming information. Indeed, in Theorem 3.4, we show instances for which there is a multiplicative benefit in rate (that grows with the network size) to directly decoding $K$ over the 2-stage decoder. One such example network, exhibiting a multiplicative benefit of 2, is depicted in Figure 1.a.

## II. MODEL

### A. Multicast Network Coding

**Network Coding Instance:** An instance $\mathcal{I} = (G, S, D, \mathcal{B})$ of the network coding problem includes an acyclic[1] directed network $G = (V, E)$ in which each edge $e \in E$ has an associated capacity $c_e$, a collection of source nodes $S \subseteq V$, a collection of terminal nodes $D \subseteq V$, and a collection of subsets of edges $\mathcal{B} = \{\beta_1, \ldots, \beta_{|\mathcal{B}|}\}$, $\beta_i \subseteq E$ that may be subject to eavesdropping.

Each source node $s_i \in S$ holds an unlimited collection of independent, uniformly distributed bits $\{b_{ij}\}_j$. Given the acyclic nature of $G$, we assume that communication occurs according to the topological order in $V$, where for blocklength $n$ every edge $e \in E$ carries a message over an alphabet $\mathcal{X}_e^n$ of size $\lfloor 2^{c_e n} \rfloor$. Roughly speaking, multicast-communication at rate $R$ is successful if at the end of the communication process all terminals $d \in D$ share a random variable $K$ uniformly distributed over $[2^{Rn}]$ that is independent from the information held by any individual subset of edges $\beta \in \mathcal{B}$. Here, for $x > 0$, $[x] = \{1, 2, \ldots, \lfloor x \rfloor\}$.

**Network Codes:** More formally, for blocklegth $n$, network code $(\mathcal{F}, \mathcal{G}) = (\{f_e\}, \{g_j\})$ is an assignment of encoding functions $\{f_e\}$ for each edge $e \in E$ and a decoding function $g_j$ to each terminal $d_j \in D$. For every edge $e = (u, v)$, the edge message $X_e^n \in \mathcal{X}_e^n$ from $u$ to $v$ is equal to the evaluation of encoding function $f_e$ on inputs $X_{\text{In}(u)}^n$. Here, for a generic node $u_0$, $X_{\text{In}(u_0)}^n$ equals $((X_{e'}^n : e' = (v, u_0) \in E), (\{b_{ij}\}_j : u_0 = s_i))$ and captures all information available to node $u_0$ during the communication process. Communication proceeds according to a topological order on $E$ and is considered

---

[1]We assume acyclicity for simplicity. Using standard techniques outlined, e.g., in [49], our results hold also for cyclic networks.

successful if for every terminal $d_j \in D$ the evaluation of decoding functions $g_j$ on the vector of random variables $X^n_{\text{In}(d_j)}$ equals the reproduction of a uniform random variable $K$ over alphabet $[2^{Rn}]$ for a target rate $R$ such that for every $\beta \in B$, $I(K; (X^n_e : e \in \beta)) = 0$. That is, we seek zero-error key-dissemination with perfect security[2]. Specifically,

**Key-dissemination feasibility:** Instance $\mathcal{I}$ is said to be $(R, n)_{\text{key}}$-feasible if there exists a network code $(\mathcal{F}, \mathcal{G})$ with blocklength $n$ such that

- **Key Rate:** $K$ is a uniform random variable with $H(K) = Rn$.
- **Decoding:** For all $d_j \in D$, $H(K|X^n_{\text{In}(d_j)}) = 0$.
- **Secrecy:** $I(K; (X^n_e : e \in \beta)) = 0$ for any subset $\beta \in \mathcal{B}$.

**Secure-multicast (sum-rate) feasibility:** Our model slightly changes when discussing secure-multicast. In the secure-multicast setting, one distinguishes between source-nodes $S_m$ that hold message information and source nodes $S_r$ that hold independent randomness used for masking. The two subsets may intersect. As before, we assume that every node $s_i$ in $S_m \cup S_r$ holds an unlimited collection of independent bits $\{b_{ij}\}_j$. Instance $\mathcal{I} = (G, (S_m, S_r), D, \mathcal{B})$ is said to be $(R, n)_{\text{sec}}$-feasible if there exists a network code $(\mathcal{F}, \mathcal{G})$ with blocklength $n$ such that

- **Message Rate:** $K$ is a uniform random variable with $H(K) = Rn$ such that $K$ equals a collection of bits included in $(b_{ij} : s_i \in S_m)$, i.e., bits generated by sources in $S_m$.
- **Decoding:** For all $d_j \in D$, $H(K|X^n_{\text{In}(d_j)}) = 0$.
- **Secrecy:** $I(K; (X^n_e : e \in \beta)) = 0$ for any subset $\beta \in \mathcal{B}$.

Notice the difference between secure-multicast feasibility and key-dissemination feasibility, in the former the key $K$ consists of a collection of random bits $b_{ij}$ generated at source nodes $s_i \in S_m$ while in the latter $K$ may consist of any function of random bits $\{b_{ij}\}_{ij}$ (of sources $s_i \in S$).

*Definition 2.1 (Key Capacity and Secure Capacity):* The multicast key-capacity of $\mathcal{I}$, denoted by $\mathbf{R}_{\text{key}}(\mathcal{I})$, is the maximum $R$ for which for all $\Delta > 0$ there exist infinitely many blocklengths $n$ such that $\mathcal{I}$ is $(R - \Delta, n)_{\text{key}}$-feasible. Restricting all encoding and decoding operations to be linear, we define the multicast linear key-capacity $\mathbf{R}^L_{\text{key}}(\mathcal{I})$ analogously. The secure capacity $\mathbf{R}_{\text{sec}}(\mathcal{I})$ and its linear variant $\mathbf{R}^L_{\text{sec}}(\mathcal{I})$ are the corresponding capacities.

## III. FORMAL STATEMENT OF RESULTS

Throughout this work we study the connections between key-dissemination and secure-multicast. In many of the statements below, given an instance $\mathcal{I} = (G, S, D, \mathcal{B})$ of the key-dissemination problem, we define a corresponding "refined" instance for secure-multicast $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ which is identical to $\mathcal{I}$ except for the definition of $S_m$ and $S_r$ which are both set to equal $S$, i.e., in $\mathcal{I}_{\text{sec}}$, all source nodes in $S$ can generate both message bits and random bits

---

used for masking. By our definitions in Section II, it holds for $\mathcal{I}$ and the corresponding $\mathcal{I}_{\text{sec}}$ that $\mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}}) \leq \mathbf{R}_{\text{key}}(\mathcal{I})$, as any code that is $(R, n)_{\text{sec}}$-feasible on $\mathcal{I}_{\text{sec}}$ is also $(R, n)_{\text{key}}$-feasible on $\mathcal{I}$. Our study is motivated by the potential benefit of $\mathbf{R}_{\text{key}}(\mathcal{I})$ over $\mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$.

*Theorem 3.1 (Single source case):* Let $\mathcal{I} = (G, S, D, \mathcal{B})$ be an instance of the key-dissemination problem with $|S| = 1$, and let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be the corresponding instance of the secure multicast problem with $S_m = S_r = S$, then

$$\mathbf{R}_{\text{key}}(\mathcal{I}) = \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$$

*Theorem 3.2 (Non-secure case):* Let $\mathcal{I} = (G, S, D, \mathcal{B})$ be an instance of the key-dissemination problem with $\mathcal{B} = \phi$, and let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be the corresponding instance of the secure multicast problem with $S_m = S_r = S$, then

$$\mathbf{R}^L_{\text{key}}(\mathcal{I}) = \mathbf{R}^L_{\text{sec}}(\mathcal{I}_{\text{sec}}).$$

*Remark 3.1:* The question of whether Theorem 3.2 holds for general (not necessarily linear) codes remains open. In other words, Question 1 restricted to the non-secure setting, which asks if "mixing helps," is unsolved. Equivalently, since $\mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}}) = \mathbf{R}^L_{\text{sec}}(\mathcal{I}_{\text{sec}})$ in this case, it is unknown if there is an advantage to non-linear codes in key-dissemination when $\mathcal{B} = \phi$.

*Theorem 3.3:* Let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be a secure-multicast instance with $|S_m| = 1$. Let $R$ be a rate parameter. One can efficiently construct an instance $\mathcal{I}_{\text{key}} = (G_{\text{key}}, S_{\text{key}}, D_{\text{key}}, \mathcal{B}_{\text{key}})$ of the key dissemination problem such that $R \in \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$ if and only if $R \in \mathbf{R}_{\text{key}}(\mathcal{I}_{\text{key}})$.

In [21], it is shown that even for secure-multicast instances $\mathcal{I}_{\text{sec}}$ for which $S_m$ is of size 1, $D$ is of size 1, $\mathcal{B} = \{\beta_e = \{e\} | e \in E\}$ consists of all single-edge subsets of $E$, all edges in $E$ are of unit capacity, and $S_r = V$, computing the secure-multicast capacity is as hard as resolving the capacity of multiple-unicast network coding instances. Corollary 3.1 follows from the instance $\mathcal{I}_{\text{key}}$ obtained in the reduction from Theorem 3.3.

*Corollary 3.1 (Key-dissemination is* hard*):* Determining the capacity of the key-dissemination problem is at least as difficult as determining the capacity of the multiple-unicast network coding problem.

As discussed previously, to address Question 1 in the general key-dissemination setting, we first define the *2-stage decoding rate for key-dissemination.*

**2-stage key-dissemination feasibility:** Instance $\mathcal{I}$ to the key-dissemination problem is said to be $(R, n)_{\text{key}(2)}$-feasible if there exists a network code $(\mathcal{F}, \mathcal{G})$ with blocklength $n$ such that

- **Key-rate:** $K$ is a uniform random variable with $H(K) = Rn$.
- **2-Stage decoding:** There exists a collection $M$ of bits included in $(b_{ij} : s_i \in S)$ such that for all $d_j \in D$, $H(M|X^n_{\text{In}(d_j)}) = 0$. Moreover, $K$ may be determined from $M$, i.e., $H(K|M) = 0$.
- **Secrecy:** $I(K; (X^n_e : e \in \beta)) = 0$ for any subset $\beta \in \mathcal{B}$.

---

[2]Although we do not discuss asymptotically vanishing error and/or weaker security requirements in this work, our results can be extended to these settings given the broad nature of the results in [21].

The 2-stage key-dissemination capacity $\mathbf{R}_{\text{key}(2)}(\mathcal{I})$ of instance $\mathcal{I}$ is defined analogously to the key-capacity $\mathbf{R}_{\text{key}}(\mathcal{I})$ of Definition 2.1.

We are now ready to state our theorem comparing $\mathbf{R}_{\text{key}(2)}(\mathcal{I})$ with $\mathbf{R}_{\text{key}}(\mathcal{I})$.

*Theorem 3.4 (General case, mixing helps):* For any integer $\alpha > 1$, there exist instances $\mathcal{I} = (G, S, D, \mathcal{B})$ of the key-dissemination problem such that

$$\mathbf{R}_{\text{key}}(\mathcal{I}) \geq \alpha \mathbf{R}_{\text{key}(2)}(\mathcal{I})$$

## IV. Proofs

Before presenting our proofs, we here roughly outline the proof ideas. In the single source case of Theorem 3.1, any uniform key $K$ obtained through key dissemination (potentially via mixing operations at the terminal nodes in the sense of Question 1) can be replaced by a collection of message bits, as required in secure-multicast, using an appropriate pre-encoding function at the single source. In the non-secure case of Theorem 3.2, any uniform key $K$ obtained through (linear) key dissemination can be replaced by a collection of message bits across different sources through an iterative process in which, at each step, an identified bit $b_{ij}$ (held by some source $s_i$) that is independent of $K$ is deterministically set to 0. This process reduces the support of $K$ and can be shown to preserve key rate. One proceeds until $K$ can be represented as a collection of message bits as required in secure-multicast. The reduction in Theorem 3.3 essentially uses an identical instance $\mathcal{I}_{\text{key}} \simeq \mathcal{I}_{\text{sec}}$, with the requirement that in $\mathcal{I}_{\text{key}}$ any shared key $K$ is a function of information generated at $S_m$ corresponding to message-bits in $\mathcal{I}_{\text{sec}}$. This is obtained by adding to $\mathcal{I}_{\text{key}}$ an additional terminal that is only connected from $S_m$. Finally, the proof of Theorem 3.4 involves instances reminiscent of *combination networks* [50], that, on one hand, allow a key capacity of 1 by multicasting a key $K$ equal to the sum-of-sources, and, on the other, are designed to have a limited non-secure multicast sum-rate. The later, together with the pre-defined security requirements, limits the 2-stage key-capacity to obtain the stated gap. A simplified example network is depicted in Figure 1.a for the special case of $\alpha = 2$.

**Proof of Theorem 3.1:** *Let $\mathcal{I} = (G, S, D, \mathcal{B})$ be an instance of the key-dissemination problem with $|S| = 1$, and let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be the corresponding instance of the secure multicast problem with $S_m = S_r = S$, then*

$$\mathbf{R}_{\text{key}}(\mathcal{I}) = \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$$

*Proof:* The fact that $\mathbf{R}_{\text{key}}(\mathcal{I}) \geq \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$ follows from our definitions as discussed above. To prove that $\mathbf{R}_{\text{key}}(\mathcal{I}) \leq \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$, consider a network code $(\mathcal{F}, \mathcal{G}) = (\{f_e\}, \{g_j\})$ for $\mathcal{I}$ that is $(R, n)_{\text{key}}$-feasible. Let $K = f(m)$ where $f$ is the global-encoding function for $K$ and $m = (b_j : j \in [\ell])$ is the vector of random bits used by the (single) source $s$ in the communication over $\mathcal{I}$. Here, for an integer $\ell$, we denote the set $\{1, 2, \ldots, \ell\}$ by $[\ell]$. If $|m| = \ell = Rn$, then by our definitions it follows that $K$ must equal a permutation of $m$; thus slightly modifying the decoding functions in $\mathcal{I}_{\text{sec}}$ to output $m$ we obtain an $(R, n)_{\text{sec}}$-feasible code for $\mathcal{I}_{\text{sec}}$.

Let $|m| = \ell > Rn$. As $K$ is uniform, for each instance $k$ of $K$ the preimage $f^{-1}(k)$ has size exactly $2^{\ell - Rn}$. Thus, there exists a pre-encoding permutation $\pi$ over $\{0, 1\}^{\ell}$ for which for all $k$, $\pi^{-1}(f^{-1}(k))$ is of size exactly $2^{\ell - Rn}$ and the mapping $f(\pi(m))$ depends only on $m' = (b_j : j \in [Rn])$. This implies that the code that first uses the pre-encoding $\pi$ on $m$ and then proceeds using $(\mathcal{F}, \mathcal{G})$ is $(R, n)_{\text{sec}}$-feasible. Specifically,

- **Message Rate:** $K$ is a uniform random variable with $H(K) = Rn$ such that $K$ equals the collection of bits $(b_j : j \in [Rn])$ generated by the single source $s \in S_m = S_r = S$.
- **Decoding:** For all $d_j \in D$, $H(K|X_{\text{In}(d_j)}^n) = 0$.
- **Secrecy:** Let $\beta \in \mathcal{B}$, and let $h_\beta(m)$ represent the global encoding function of the original code $(\mathcal{F}, \mathcal{G})$ for $\mathcal{I}$ corresponding to $(X_e : e \in \beta)$. In the original code, we have, for any $\beta \in \mathcal{B}$, that $I(K; (X_e : e \in \beta)) = I(f(m); h_\beta(m)) = 0$. In the new code for $\mathcal{I}_{\text{sec}}$, the edges $e \in \beta$ transmit $h_\beta(\pi(m))$. As $\pi$ is a permutation on $\{0, 1\}^{\ell}$ and $m$ is uniform, it now follows in the new code that $I(K; h_\beta(\pi(m)) = I(f(\pi(m)); h_\beta(\pi(m))) = I(f(m); h_\beta(m)) = 0$ for any subset $\beta \in \mathcal{B}$ by the security of $(\mathcal{F}, \mathcal{G})$ on $\mathcal{I}$.

**Proof of Theorem 3.2:** *Let $\mathcal{I} = (G, S, D, \mathcal{B})$ be an instance of the key-dissemination problem with $\mathcal{B} = \phi$, and let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be the corresponding instance of the secure multicast problem with $S_m = S_r = S$, then*

$$\mathbf{R}_{\text{key}}^L(\mathcal{I}) = \mathbf{R}_{\text{sec}}^L(\mathcal{I}_{\text{sec}}).$$

*Proof:* The fact that $\mathbf{R}_{\text{key}}^L(\mathcal{I}) \geq \mathbf{R}_{\text{sec}}^L(\mathcal{I}_{\text{sec}})$ follows from our definitions as discussed above. To show that $\mathbf{R}_{\text{key}}^L(\mathcal{I}) \leq \mathbf{R}_{\text{sec}}^L(\mathcal{I}_{\text{sec}})$, consider a linear network code $(\mathcal{F}, \mathcal{G}) = (\{f_e\}, \{g_j\})$ for $\mathcal{I}$ that is $(R, n)_{\text{key}}$-feasible. Let $K = Am$ where for $S = (s_i : i \in |S|)$, $m_i = (b_{ij} : j \in [\ell_i])$ are the independent random bits used by source $s_i$ in the communication process, $m = (b_{ij} : s_i \in S, j \in [\ell_i])$ is the vector of random bits used by all sources during communication, $\ell = \sum_{s_i \in S} \ell_i$ is the size of $m$, and $A$ is the $nR \times \ell$ global-encoding matrix of $K$. Similar to the proof of Theorem 3.1, if $|m| = \ell = Rn$, then by our definitions it follows that $K$ must equal a linear permutation of $m$ and thus slightly modifying the decoding functions in $\mathcal{I}_{\text{sec}}$ to output $m$ we obtain an $(R, n)_{\text{sec}}$-feasible code for $\mathcal{I}_{\text{sec}}$.

Assume that $|m| > Rn$, we now claim that there exists $s_i \in S$ and $j \in [\ell_i]$ such that the matrix $A'$ obtained from $A$ by replacing the column in $A$ corresponding to $b_{ij}$ by the all zero column, satisfies $H(A'm) = Rn$. This implies that a new key $K' = A'm$ of the same rate can be communicated using the same linear network code $(\mathcal{F}, \mathcal{G})$ in which source $s_i$ replaces the random bit $b_{ij}$ by a constant value of 0, or equivalently, source $s_i$ omits random bit $b_{ij}$ from the linear combinations transmitted on its outgoing links. The latter, in turn, implies that the modified code uses fewer bits from $m$, i.e., only $(\ell - 1)$ bits instead of the previous $\ell$. Continuing in this manner inductively, i.e., reducing the number of bits used from $m$ by zeroing out columns of $A$, we eventually obtain a linear multicast code for which exactly $Rn$ bits from

$m$ are used to determine the uniform rate-$R$ key shared by the terminals. This now implies, as discussed in the case that $|m| = Rn$, that $\mathcal{I}_{\text{sec}}$ is $(R, n)_{\text{sec}}$-feasible. Notice, that it is crucial that we are studying the case of $\mathcal{B} = \phi$, as the process above does not necessarily preserve independence between the resulting key and other forms of information transmitted on network links.

To prove the claim above, assume $|m| = \ell > Rn$. Thus there exists $s_i \in S$, $j \in [\ell_i]$ such that the column of $A$ corresponding to $b_{ij}$ is a linear combination of the remaining columns of $A$. Let $A'$ be the matrix obtained from $A$ by zeroing out the column corresponding to $b_{ij}$. By our construction, the rank of $A'$ equals that of $A$, or equivalently $H(A'm) = H(K') = Rn$.

*Remark 4.1:* It is still open whether Theorem 3.2 holds for general (not necessarily linear) codes. In other words, the answer to Question 1 restricted to the non-secure setting, which asks if "mixing helps", is unknown. An affirmative answer would imply that $\mathbf{R}_{\text{key}}(\mathcal{I}) > \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$ and thus, as $\mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}}) = \mathbf{R}_{\text{sec}}^L(\mathcal{I}_{\text{sec}}) = \mathbf{R}_{\text{key}}^L(\mathcal{I})$ when $\mathcal{B} = \phi$, that $\mathbf{R}_{\text{key}}(\mathcal{I}) > \mathbf{R}_{\text{key}}^L(\mathcal{I})$, i.e., that there is an advantage to non-linear codes in key-dissemination when $\mathcal{B} = \phi$.

**Proof of Theorem 3.3:** *Let $\mathcal{I}_{\text{sec}} = (G, (S_m, S_r), D, \mathcal{B})$ be a secure-multicast instance with $|S_m| = 1$. Let $R$ be a rate parameter. One can efficiently construct an instance $\mathcal{I}_{\text{key}} = (G_{\text{key}}, S_{\text{key}}, D_{\text{key}}, \mathcal{B}_{\text{key}})$ of the key dissemination problem such that $R \in \mathbf{R}_{\text{sec}}(\mathcal{I}_{\text{sec}})$ if and only if $R \in \mathbf{R}_{\text{key}}(\mathcal{I}_{\text{key}})$.*

*Proof:* Let $R$ be a given rate parameter. We first construct the instance $\mathcal{I}_{\text{key}} = (G_{\text{key}}, S_{\text{key}}, D_{\text{key}}, \mathcal{B}_{\text{key}})$ of the key dissemination problem with $G_{\text{key}} = (V_{\text{key}}, E_{\text{key}})$. Instance $\mathcal{I}_{\text{key}}$ is obtained from $\mathcal{I}_{\text{sec}}$ by adding a new terminal $d_{\text{key}}$ to the set $D$ to obtain $V_{\text{key}} = V \cup \{d_{\text{key}}\}$ and $D_{\text{key}} = D \cup \{d_{\text{key}}\}$, by adding a new edge of capacity $R$ connecting source $s$ of $S_m$ with $d_{\text{key}}$ to give $E_{\text{key}} = E \cup \{(s, d_{\text{key}})\}$, by setting $\mathcal{B}_{\text{key}} = \mathcal{B}$, and by setting $S_{\text{key}} = S_m \cup S_r$.

We show for every $R' \leq R$ that there exists an $(R', n)_{\text{sec}}$-feasible code for $\mathcal{I}_{\text{sec}}$ if and only if there exists an $(R', n)_{\text{key}}$-feasible code for $\mathcal{I}_{\text{key}}$. First assume that there exists an $(R', n)_{\text{sec}}$-feasible code for $\mathcal{I}_{\text{sec}}$. Let $K$ be the rate $R'$ message that is securely communicated from $S_m$ to all terminals in $D$. Using the exact same code on $\mathcal{I}_{\text{key}}$ and communicating $K$ directly on the new edge $(s, d_{\text{key}})$, one can communicate $K$ to all terminals in $D_{\text{key}}$. As the original code is secure in $\mathcal{I}_{\text{sec}}$ for the edge sets in $\mathcal{B} = \mathcal{B}_{\text{key}}$, the code is $(R', n)_{\text{key}}$-feasible for $\mathcal{I}_{\text{key}}$.

Now assume that there exists an $(R', n)_{\text{key}}$-feasible code for $\mathcal{I}_{\text{key}}$. As only information generated at $S_m$ can be shared between the new terminal $d_{\text{key}}$ and other terminals in $D_{\text{key}}$, it holds that the shared uniform key $K$ is a function of the random bits generated at $s$ of $S_m$. Moreover, as $\mathcal{B} = \mathcal{B}_{\text{key}}$, for every $\beta \in \mathcal{B}$ the code on $\mathcal{I}_{\text{key}}$ satisfies $I(K, (X_e^n : e \in \beta)) = 0$. Now, using ideas of Theorem 3.1, one can pre-encode at $s$ to obtain a code that, when restricted to $G$, is an $(R', n)_{\text{sec}}$-feasible code for $\mathcal{I}_{\text{sec}}$. This concludes the proof of our assertion.

**Proof of Theorem 3.4:** *For any integer $\alpha > 1$, there exist instances $\mathcal{I} = (G, S, D, \mathcal{B})$ of the key-dissemination problem such that*

$$\mathbf{R}_{\text{key}}(\mathcal{I}) \geq \alpha \mathbf{R}_{\text{key}(2)}(\mathcal{I})$$

*Proof:* Let $\alpha > 1$. Roughly speaking, the instance $\mathcal{I} = (G, S, D, \mathcal{B})$ we present is reminiscent of the *combination network* [50]. The network $\mathcal{I}$, depicted in a simplified form in Figure 1.a for the special case of $\alpha = 2$, has the following structure. $G$ is acyclic and has three layers of nodes. The first layer consists of the source nodes $S = \{s_1, \ldots, s_r\}$. Here, we set $r$ to be equal to $\alpha + 1$. The second layer consists of two sets of intermediate nodes $U = \{u_1, \ldots, u_r\}$ and $\bar{U} = \{\bar{u}_1, \ldots, \bar{u}_r\}$. The final layer consists of terminal nodes $D = \{d_i\}_{i \in [r]}$. The edge set of $G$ consists of the following edges, an edge $(s_i, u_i)$ for every $i \in [r]$, an edge $(s_j, \bar{u}_i)$ for every $j \neq i$ in $[r]^2$, an edge $(u_i, d_i)$ and $(\bar{u}_i, d_i)$ for every $i \in [r]$. Each edge has capacity 1. For each node $v \in U \cup \bar{U}$, the set $\mathcal{B}$ contains a subset $\beta_v = (e : e \in \text{In}(v))$ comprising all incoming edges to $v$. Thus, $\mathcal{B} = \{\beta_v : v \in U \cup \bar{U}\}$.

We first show that $\mathbf{R}_{\text{key}}(\mathcal{I}) \leq 1$. Consider any network code for $\mathcal{I}$ that is $(R, n)_{\text{key}}$-feasible. Let $K$ be the key shared by all terminal nodes. For nodes $v \in U \cup \bar{U}$, let $e(v)$ be the (single) edge leaving $v$ and let $X_{e(v)}^n$ be the information transmitted on $e(v)$. Since $\beta_v \in \mathcal{B}$, it must hold that $I(K; X_{e(v)}^n) \leq I(K; (X_e^n : e \in \beta_v)) = 0$. We now show that this implies that $R \leq 1$. Let $i \in [r]$, and consider terminal $d_i$. The structure of $\mathcal{I}$ implies that

$$
\begin{aligned}
H(K) &= I(K; X_{e(u_i)}^n, X_{e(\bar{u}_i)}^n) \\
&= I(K; X_{e(u_i)}^n) + I(K; X_{e(\bar{u}_i)}^n | X_{e(u_i)}^n)) \\
&= I(K; X_{e(\bar{u}_i)}^n | X_{e(u_i)}^n)) \leq H(X_{e(\bar{u}_i)}^n) \leq n.
\end{aligned}
$$

To show that $\mathbf{R}_{\text{key}}(\mathcal{I}) = 1$, we present a network code for $\mathcal{I}$ that is $(1, n)_{\text{key}}$-feasible (i.e., of rate $R = 1$). Roughly speaking, our code communicates the sum of all sources to each terminal $d_i$. Formally, for $n = 1$, source node $s_i$ sends a single bit $b_i$ on all its outgoing edges, and nodes $u_i$ and $\bar{u}_i$ send the binary sum of their incoming information on their single outgoing edge. Summing these, every terminal obtains the (shared) sum $\sum_{i=1}^{r} b_i$. Due to the nature of $K$, for any $\beta_v \in \mathcal{B}$ it holds that $I(K; (X_e^n : e \in \beta_v)) = 0$. We conclude that $\mathcal{I}$ is $(R, n)_{\text{key}}$-feasible for $R = 1$.

We now show that $\mathbf{R}_{\text{key}(2)}(\mathcal{I}) \leq \frac{1}{r-1}$. Consider any network code for $\mathcal{I}$ that is $(R, n)_{\text{key}(2)}$-feasible. Let the decoded messages from the first decoding stage be $M = (b_{ij} : (i, j) \in I)$ and let $K$ be the key obtained by the second stage. Recall that $H(K|M) = 0$. Let $M_i = (b_{ij} : (i, j) \in I)$ be the bits in $M$ generated at source $s_i \in S$, and let $R_i = M_i/n$. For any $i \in [r]$, removing a single edge from $\mathcal{I}$ separates terminal $d_i$ from sources $(s_j : j \neq i)$. Therefore, using standard cut-set bounds with respect to terminal $d_i$, it holds that $\sum_{j \neq i} R_i \leq 1$. By summing the above over $i$, we conclude that $\sum_i \sum_{j \neq i} R_i \leq r$, which in turn implies that $\sum_i R_i \leq \frac{r}{r-1}$. Moreover, as $u_i \in U$ lies on the only path from $s_i$ to terminal $d_i$, $H(M_i | X_{\text{In}(u_i)}^n) = 0$. By our definition of $\mathcal{B}$ we have for all $i \in [r]$ that $I(K; X_{\text{In}(u_i)}^n) = 0$, which now implies that $I(K; M_i) = 0$ for all $i \in [r]$. Similarly, by our definition of

$\mathcal{B}$, it holds that $I(K; (M_j : j \neq i)) = 0$ for all $i \in [r]$ since $\bar{u}_i \in \bar{U}$ lies on the only path from $\{s_j\}_{j \neq i}$ to $d_i$. Thus, for every $i \in [r]$,

$$
\begin{aligned}
H(K) &= I(K; M) \\
&= I(K; (M_j : j \neq i)) + I(K; M_i | (M_j : j \neq i)) \\
&= I(K; M_i | (M_j : j \neq i)) \leq H(M_i) = R_i n.
\end{aligned}
$$

Summing over all $i \in [r]$, we therefor conclude that $rH(K) \leq n \sum_i R_i \leq n \cdot \frac{r}{r-1}$, implying that $Rn = H(K) \leq \frac{n}{r-1}$. We conclude that

$$
1 = \mathbf{R}_{\texttt{key}}(\mathcal{I}) \geq (r-1)\mathbf{R}_{\texttt{key(2)}}(\mathcal{I}) = \alpha \mathbf{R}_{\texttt{key(2)}}(\mathcal{I}).
$$

## V. Conclusions

This work addresses the key-dissemination problem in the context of network coding, in which a number of results comparing key capacity with the traditional secure-multicast capacity are presented. For single-source networks and linear non-secure networks, we show that there is no rate advantage in the flexible nature of the shared key $K$ in key-dissemination when compared to the requirement of secure-multicast that $K$ include source information bits. For general instances, we demonstrate rate advantages of key-dissemination when compared to secure-multicast or restricted forms of 2-stage key-dissemination decoding. Finally, we show that determining the key capacity is as hard as determining the secure-multicast capacity which, in turn, is as hard as determining the multiple-unicast network coding capacity.

Several questions remain open or unstudied in this work. For the non-secure (multiple-source) setting, it is currently unresolved whether *mixing* (in the sense of Question 1) allows improved key rates compared to traditional multi-source multicast. This work does not address the multiple-multicast analog of key-dissemination in which different sets of terminals require independent secret keys, potentially mutually hidden between the different terminal sets. Understanding the multiple-multicast analog of key-dissemination exhibits challenges even for the 2-multicast case and has strong connections to the cryptographic study of *secret sharing*. Finally, efficient communication schemes, especially designed for the multicast (or the multiple-multicast analog) of key-dissemination are not presented in this work. While one can design multicast key-dissemination schemes relying on random linear network coding enhanced with certain security measures, a comprehensive study in this aspect is the subject of ongoing work.

## References

[1] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[2] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[3] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[4] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993.

[5] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiple terminals. *IEEE Transactions on Information Theory*, 50(12):3047–3061, 2004.

[6] Chung Chan and Lizhong Zheng. Multiterminal secret key agreement. *IEEE transactions on information theory*, 60(6):3379–3412, 2014.

[7] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiterminal channel models. *IEEE Transactions on Information Theory*, 54(6):2437–2452, 2008.

[8] Amin Aminzadeh Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals—Part I. *IEEE Transactions on Information Theory*, 56(8):3973–3996, 2010.

[9] Amin Aminzadeh Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals—Part II: Channel model. *IEEE Transactions on Information Theory*, 56(8):3997–4010, 2010.

[10] Mahdi Jafari Siavoshani, Christina Fragouli, Suhas Diggavi, Uday Pulleti, and Katerina Argyraki. Group secret key generation over broadcast erasure channels. In *Forty Fourth IEEE Asilomar Conference on Signals, Systems and Computers*, pages 719–723, 2010.

[11] Peng Xu, Zhiguo Ding, Xuchu Dai, and George K. Karagiannidis. On the private key capacity of the $m$-relay pairwise independent network. *IEEE Transactions on Information Theory*, 62(7):3831–3843, 2016.

[12] Masahito Hayashi, Himanshu Tyagi, and Shun Watanabe. Secret key agreement: General capacity and second-order asymptotics. *IEEE Transactions on Information Theory*, 62(7):3796–3810, 2016.

[13] Prakash Narayan and Himanshu Tyagi. *Multiterminal secrecy by public discussion*. Now Publishers Hanover, MA, USA, 2016.

[14] Ning Cai and Raymond W Yeung. Secure network coding. *IEEE International Symposium on Information Theory*, page 323, 2002.

[15] Jon Feldman, Tal Malkin, C Stein, and RA Servedio. On the capacity of secure network coding. *42nd Annual Allerton Conference on Communication, Control, and Computing*, pages 63–68, 2004.

[16] Ning Cai and Raymond W Yeung. A security condition for multi-source linear network coding. *IEEE International Symposium on Information Theory*, pages 561–565, 2007.

[17] Ning Cai and Raymond W Yeung. On the optimality of a construction of secure network codes. *IEEE International Symposium on Information Theory*, pages 166–170, 2008.

[18] Salim El Rouayheb, Emina Soljanin, and Alex Sprintson. Secure network coding for wiretap networks of type II. *IEEE Transactions on Information Theory*, 58(3):1361–1371, 2012.

[19] Danilo Silva and Frank R Kschischang. Universal secure network coding via rank-metric codes. *IEEE Transactions on Information Theory*, 57(2):1124–1135, 2011.

[20] Sid Jaggi and Michael Langberg. Secure network coding: Bounds and algorithms for secret and reliable communications. In *Chapter 7 of Network Coding: Fundamentals and applications (Muriel Médard and Alex Sprintson ed.)*, pages 183–215. Academic Press, 2012.

[21] W. Huang, T. Ho, M. Langberg, and J. Kliewer. Single-unicast secure network coding and network error correction are as hard as multiple-unicast network coding. *IEEE Transactions on Information Theory*, 64(6):4496–4512, 2018.

[22] Terence H Chan and Alex Grant. Network coding capacity regions via entropy functions. *IEEE Transactions on Information Theory*, 60(9):5347–5374, 2014.

[23] Tao Cui, Tracy Ho, and Joerg Kliewer. On secure network coding with nonuniform or restricted wiretap sets. *IEEE Transactions on Information Theory*, 59(1):166–176, 2012.

[24] Debaditya Chaudhuri and Michael Langberg. Trade-offs between rate and security in linear multicast network coding. In *IEEE International Symposium on Information Theory (ISIT)*, pages 846–850, 2018.

[25] Debaditya Chaudhuri, Michael Langberg, and Michelle Effros. Secure network coding in the setting in which a non-source node may generate random keys. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2309–2313, 2019.

[26] Debaditya Chaudhuri. *Characterization of Rate Regions in Secure Network Coding over General Wiretap Networks*. PhD thesis, University at Buffalo, State University of New York, 2021.

[27] T. Chan and A. Grant. Capacity bounds for secure network coding. *Australian Communications Theory Workshop*, pages 95–100, 2008.

[28] T. Cui, T. Ho, and J. Kliewer. On secure network coding with nonuniform or restricted wiretap sets. *IEEE Transactions on Information Theory*, 59(1):166–176, 2013.

[29] Michael Langberg and Muriel Médard. On the multiple unicast network coding, conjecture. *47th Annual Allerton Conference on Communication, Control, and Computing*, pages 222–227, 2009.

[30] Rathinakumar Appuswamy, Massimo Franceschetti, Nikhil Karamchandani, and Kenneth Zeger. Network coding for computing: Cut-set bounds. *IEEE Transactions on Information Theory*, 57(2):1015–1030, 2011.

[31] Hemant Kowshik and PR Kumar. Optimal function computation in directed and undirected graphs. *IEEE Transactions on Information Theory*, 58(6):3407–3418, 2012.

[32] Virag Shah, Bikash Kumar Dey, and D Manjunath. Network flows for function computation. *IEEE Journal on Selected Areas in Communications*, 31(4):714–730, 2013.

[33] Aditya Ramamoorthy and Michael Langberg. Communicating the sum of sources over a network. *IEEE Journal on Selected Areas in Communications*, 31(4):655–665, 2013.

[34] Brijesh Kumar Rai and Bikash Kumar Dey. On network coding for sum-networks. *IEEE Transactions on Information Theory*, 58(1):50–63, 2012.

[35] Sagar Shenvi and Bikash Kumar Dey. A necessary and sufficient condition for solvability of a 3s/3t sum-network. In *2010 IEEE International Symposium on Information Theory*, pages 1858–1862, 2010.

[36] Rathinakumar Appuswamy and Massimo Franceschetti. Computing linear functions by linear coding over networks. *IEEE transactions on information theory*, 60(1):422–431, 2013.

[37] Sijie Li and Cheuk Ting Li. Arithmetic network coding for secret sum computation. *arXiv preprint arXiv:2201.03032*, 2022.

[38] Siddhartha Brahma and Christina Fragouli. Pliable index coding. *IEEE Transactions on Information Theory*, 61(11):6192–6203, 2015.

[39] Ziv Bar-Yossef, Yitzhak Birk, TS Jayram, and Tomer Kol. Index coding with side information. *IEEE Transactions on Information Theory*, 57(3):1479–1494, 2011.

[40] Salim El Rouayheb, Alex Sprintson, and Costas Georghiades. On the index coding problem and its relation to network coding and matroid theory. *IEEE Transactions on Information Theory*, 56(7):3187–3195, 2010.

[41] Michelle Effros, Salim El Rouayheb, and Michael Langberg. An equivalence between network coding and index coding. *IEEE Transactions on Information Theory*, 61(5):2478–2487, 2015.

[42] Son Hoang Dau, Vitaly Skachek, and Yeow Meng Chee. On the security of index coding with side information. *IEEE Transactions on Information Theory*, 58(6):3975–3988, 2012.

[43] Tang Liu and Daniela Tuninetti. Private pliable index coding. In *IEEE Information Theory Workshop (ITW)*, pages 1–5, 2019.

[44] Shanuja Sasi and B Sundar Rajan. Code construction for pliable index coding. In *IEEE International Symposium on Information Theory (ISIT)*, pages 527–531, 2019.

[45] Tang Liu and Daniela Tuninetti. Secure decentralized pliable index coding. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1729–1734, 2020.

[46] Paulo F Oliveira and Joao Barros. A network coding approach to secret key distribution. *IEEE Transactions on Information Forensics and Security*, 3(3):414–423, 2008.

[47] Shuaifang Xiao, Yunfei Guo, Kaizhi Huang, and Liang Jin. Cooperative group secret key generation based on secure network coding. *IEEE Communications Letters*, 22(7):1466–1469, 2018.

[48] Luisa Lima, Joao Barros, Muriel Médard, and Alberto Toledo. Towards secure multiresolution network coding. In *IEEE Information Theory Workshop on Networking and Information Theory*, pages 125–129, 2009.

[49] Michael Langberg and Michelle Effros. Edge removal in undirected networks. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1421–1426, 2021.

[50] Chi Kin Ngai and Raymond W Yeung. Network coding gain of combination networks. In *Information Theory Workshop*, pages 283–287. IEEE, 2004.