Scientia Iranica D (2019) 26(3), 1749–1761

Sharif University of Technology
Scientia Iranica
Transactions D: Computer Science & Engineering and Electrical Engineering
http://scientiairanica.sharif.edu

On the equivalency of reliability and security metrics for wireline networks

M.M. Mojahedian*, M.R. Aref, and A. Gohari

Information Systems and Security Lab. (ISSL), Sharif University of Technology, Tehran, P.O. Box 11155-8639, Iran.

Received 4 December 2017; accepted 16 April 2018

KEYWORDS
Wireline networks;
Perfect secrecy;
Strong secrecy;
Weak secrecy;
ϵ-error decoding;
Zero-error decoding;
Random binning.

Abstract. This study considers a secure network coding problem in which some secret keys are shared among legitimate nodes, and there exists an eavesdropper that is able to hear a subset of links. We show the equivalency of secure network coding under weak and strong secrecy conditions. For linear network coding, we show a stronger result: equivalency of "perfect secrecy and zero-error constraints" to "weak secrecy and ϵ-error constraints". This is a secure version of the result obtained by Langberg and Effros on the equivalence of zero-error and ϵ-error regions in the network coding problem with co-located sources. Jalali and Ho exploited extractor functions to prove the weak and strong rate region equivalency for this network; however, to prove this equivalency, some tools are developed in random binning, and the equivalency in a slightly more general setting is proved.

1. Introduction

A reliable and secure communication requires low error probability and low information leakage. However, there are different metrics for error probability and information leakage. Two important reliability metrics are ϵ or zero probability of error. An ϵ-error criterion requires the (average or maximal) error probability to vanish as the blocklength increases, while a zero-error criterion demands the error to be exactly zero for every given blocklength. Three important security metrics include weak, strong, or perfect secrecy. A weak notion of secrecy requires the *percentage* of the message that is leaked to vanish as the code blocklength increases, while a strong notion of secrecy requires the *total amount* of leaked information (not its percentage) to vanish as the blocklength increases. Perfect secrecy requires absolutely *zero* leakage of information for every given blocklength.

These reliability and security metrics lead to different notions of capacity, which can be quite different. For instance, zero-error capacity, which was originally introduced by Shannon [1], can be zero in a point-to-point channel, while ϵ-error can be non-zero for the same channel. One can then ask: "how does capacity behave under different reliability and security metrics?" There are some works in the literature that address this interesting question. In [2,3], the authors showed that, in the network coding problem with co-located sources, the rate region did not increase by relaxing zero-error to the ϵ-error condition. Maurer and Wolf [4] proved the rate region equivalency of weak and strong secure conditions in the source-model secret key agreement problem. The authors in [5] exploited the same approach as in [4] to prove the rate region equivalency for a more general network with multiple sources and sinks. Unlike the model adopted in this

*. *Corresponding author. Tel.: +98 21 66165900*
E-mail addresses: m_mojahedian@ee.sharif.edu (M.M. Mojahedian); aref@sharif.edu (M.R. Aref); aminzadeh@sharif.edu (A. Gohari)

doi: 10.24200/sci.2018.5695.1428

work, [5] considered an acyclic topology for the network and, also, assumed that the transmitters had separate messages, not a common message to send. In [6], the equivalency of weak and perfect secrecy conditions (with ϵ-error probability) for the secure index coding problem was shown. Moreover, it was shown that zero-error probability could be achieved at a cost of a multiplicative constant. To the best of our knowledge, no other work except [6] has concentrated on the equivalency of weak and perfect secrecy. However, the setup of this problem, reviewed in Figure 1, is restricted. For instance, the adversary is assumed to have full access to the communication links, and the shared keys are either shared between pairs of nodes, or all of the nodes (no key is shared between subsets of size three for instance). Furthermore, the network topology of index coding is a special case of wireline networks. While there are many works addressing the security aspects of wireline networks [7-18] in various settings, as far as we know, Ref. [5] is the work that studied how the secrecy region changes with weak and strong secrecy constraints in the secure network coding problem. Finally, important aspects of secure communication such as secure throughput in the presence of an active adversary who can corrupt a limited number of links were considered. For more details about the works on the secure network coding problem, one can refer to [17].

1.1. The authors contribution

This study considers a general wireline network consisting of sources, intermediate nodes, and sinks, which are interconnected by error-free links. The links are directional with given capacities. Thus, wireline network can be represented by a directed weighted graph. This graph is allowed to have directed cycles. The source nodes have messages that are desired by sink nodes. Moreover, nodes in the network have access to infinite private randomness (only available to the nodes themselves) and, also, a number of rate-limited shared keys. Each key is shared among a subset of sources, relays or destination nodes. These secret keys are helpful in hiding messages from an eavesdropper who has access to a subset of the links.

Our main result is to show that changing weak to perfect conditions and ϵ-error to zero-error constraint does not affect the achievable secure rate region of linear network coding (if nodes are restricted to linear operations). When the nodes are allowed to perform non-linear operations, weak and strong secrecy conditions are shown to be equivalent. In order to prove the rate region equivalency of weak and strong secrecy conditions, tools from random binning of sources are required. Output Statistics of Random Binning (OSRB) is a tool introduced in [19] to describe the joint pmf of bin indices of multiple random variables. To prove our

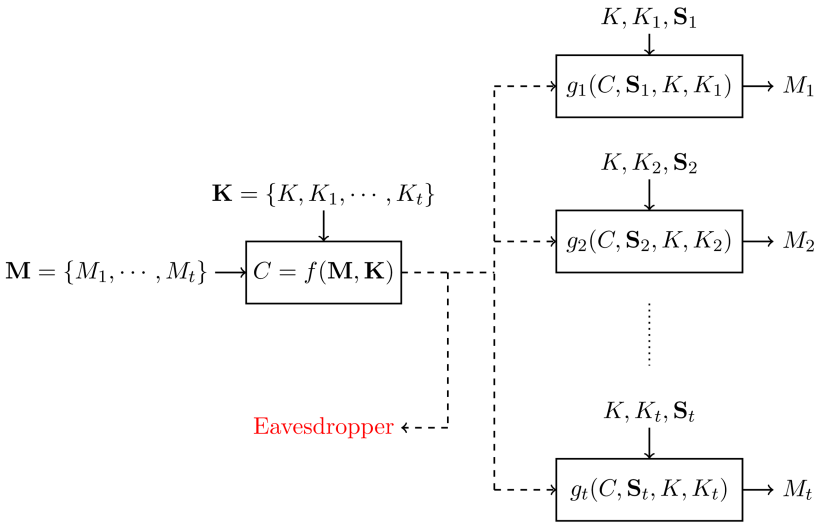

Figure 1. The schematic of a perfectly-secure index coding problem. This is a generalization of Shannon's cypher system [26] to an index coding setup, which was introduced by Birk and Kol [27] in the context of satellite communication and studied further in [27-36]. In the secure index coding problem, there is a transmitter sending t messages $M_1, M_2, \cdots, M_t$ to t legitimate receivers in the presence of an eavesdropper. Each receiver i, $i \in [t]$ has a side information set $\mathbf{S}_i$ which is a subset of messages $\{M_1, M_2, \cdots, M_t\}$ except M_i. Furthermore, there is a common key K shared among all the legitimate parties and private keys $K_1, K_2, \cdots, K_t$ shared between the transmitter and each of the receivers. The transmitter applies a (randomized) function to the messages and keys to compute public code C. Then, C is broadcast, and all the receivers, including the eavesdropper, can hear C. Each receiver, i, applies a function to the information available to it, namely K, K_i and messages in $\mathbf{S}_i$ to compute M_i. The goal is to find the minimum number of information bits that should be broadcast by the server so that each client can recover its desired messages with *zero-error* probability; further, the eavesdropper could not retrieve any information about the messages by having C *(perfect secrecy)*.

results, some new versions of the OSRB theorem are stated and proved.

The rest of this paper is organized as follows. In Section 2, the system model is defined. Section 3 lays out the main results. The proofs are presented in Section 4. Some results of linear codes are provided in Section 3.4. Section 5 concludes this paper.

1.2. Notation

Random variables are denoted by capital letters and their values by lowercase letters. Herein, $[k]$ is used to denote the set of $\{1, 2, \cdots, k\}$. For a given subset $\mathcal{S} \subset [t]$ and a sequence of random variables $M_1, M_2, \cdots, M_t$ are used $M_{\mathcal{S}}$ to denote the set $\{M_i : i \in \mathcal{S}\}$. When $\mathcal{S} = [t]$ is the full set, instead of $M_{[t]}$, bold font is used to denote full sets or its vector form, i.e., $\mathbf{M}$ is used to either denote the message set $\{M_1, M_2, \cdots, M_t\}$ or the vector $[M_1, M_2, \cdots, M_t]$. Whether $\mathbf{M}$ is a set or a vector is clarified in the context. The total variation distance between two pmfs, p_X and q_X, is defined as follows:

$$|p_X - q_X|_1 = \frac{1}{2} \sum_x |p_X(x) - q_X(x)|.$$

In addition, $\mathbb{1}[\cdot]$ is used to denote the indicator function; it is equal to one if the condition inside $[\cdot]$ holds; otherwise, it is zero. $f(n) = o(g(n))$ means that $\lim_{n\to\infty} f(n)/g(n) \to 0$. Finally, all the logarithms in this paper are of base two.

2. System model and definitions

2.1. System model

It is assumed here that there are t messages $M_1, M_2, \cdots, M_t$. Let us denote the set of all messages by $\mathbf{M} = \{M_1, M_2, \cdots, M_t\}$. As shown in Figure 2, the wireline network considered in this paper consists of source nodes, receiver nodes (sink nodes), and some intermediate relay nodes. The nodes (source, sink, and intermediate nodes) are interconnected by error-free point-to-point links. In addition, there exists an eavesdropper who is able to hear some of the links. Each source node has access to a subset of messages. Similarly, each sink node desires to obtain a subset of messages. The source and sink nodes are part of the wireline network.

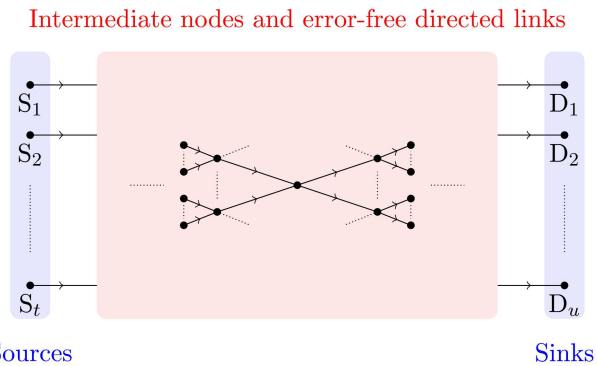

Figure 2. The directed graph representation of a wireline network. Nodes of the network are connected to each other via directed links of limited capacity. The directed graph is allowed to have cycles. In this figure, there are t source nodes and u sink nodes. The models allow for shared secret keys between various subsets of the nodes. Each node produces its outputs on its ongoing links based on its inputs, shared keys, and its own private randomness.

There is also a set of keys $\mathbf{K} = \{K_1, K_2, \cdots, K_\Delta\}$ of limited rates, each of which is shared among a subset of the nodes. Hence, every node can use its available keys for encoding. Moreover, each source or relay nodes can use a private randomness. Let us denote the set of all private randomness vectors by the set $\mathbf{W} = \{W_1, W_2, \cdots, W_\Theta\}$. Random variables $M_1, \cdots, M_t, K_1, \cdots, K_\Delta, W_1, \cdots, W_\Theta$ are mutually independent and uniform over their alphabet sets.

The edges of the wireline network have limited capacity. For a code of blocklength n, an edge with capacity C_e can carry at most $n(C_e + \epsilon_n)$ bits where ϵ_n converges to zero as n tends to infinity. Similarly, if the rate of message M_i is R_{M_i}, then M_i is a binary sequence of length nR_{M_i} in a code of blocklength n. The same holds for the rate of shared keys R_{K_i}. The aim of the nodes of the network is to maximize communication rates R_{M_i} while minimizing key rates R_{K_i} as much as possible in such a way that the desired reliability (error probability condition at sinks) and security conditions are met (Private randomness is commonly considered as a free resource and studying its rate is not of interest). The resulting fundamental trade-off between R_{M_i} and R_{K_i} describes the capacity region of the problem.

It is assumed that the adversary can observe a collection E of the edges in the network. By fixing a coding strategy by the nodes in the network, the eavesdropper will end up with a collection of observations from the network. Random variable $\mathbf{C}$ is used to denote all the information the eavesdropped has obtained. Random variable $\mathbf{C}$ is a function of $\mathbf{M}$, $\mathbf{K}$, and $\mathbf{W}$:

$$\mathbf{C} = f(\mathbf{M}, \mathbf{K}, \mathbf{W}).$$

Linear network coding:

In linear network coding, it is assumed that there is a finite field $\mathbb{F}$. Each of variables M_i, K_i, and W_i is a string of independent and uniformly distributed symbols from field $\mathbb{F}$. All the coding operations are restricted to taking weighted linear combinations in $\mathbb{F}$. Then, eavesdropper's information $\mathbf{C}$ can be expressed as follows:

$$\mathbf{C} = A\mathbf{M} + B\mathbf{K} + G\mathbf{W}, \tag{1}$$

for some matrices A, B, and G where:

$$\mathbf{M} = \left[M_1, M_2, \cdots, M_t\right]^{\mathrm{T}},$$

$$\mathbf{K} = \left[K_1, K_2, \cdots, K_\Delta\right]^{\mathrm{T}},$$

$$\mathbf{W} = \left[W_1, W_2, \cdots, W_\Theta\right]^{\mathrm{T}}.$$

2.2. Decoding and secrecy metrics

Decoding conditions:

- *Zero-error decoding.* Each receiver is able to decode its desired messages with exactly zero-error probability for every given blocklength;
- *ϵ-error decoding.* Each receiver is able to recover its desired message with the vanishing probability of error as the blocklength grows.

Secrecy conditions:

- *Perfect secrecy.* Assuming that $K_1, \cdots, K_\Delta, W_1, \cdots, W_\Theta$ are mutually independent and uniform over their alphabet sets, the conditional pmf $p(\mathbf{C} = \mathbf{c}|\mathbf{M} = \mathbf{m})$ should not depend on the value of $\mathbf{m}$ for any given $\mathbf{c}$. Equivalently, for any distribution on input message set $\mathbf{M}$, we should have:

$$I(\mathbf{M}; \mathbf{C}) = 0, \qquad \forall p_{\mathbf{M}}(\mathbf{m}), \tag{2}$$

  as long as message set $\mathbf{M}$, key set $\mathbf{K}$, and private randomness set $\mathbf{W}$ are mutually independent.
- *Strong secrecy.* In strong secrecy, the independence between $\mathbf{M}$ and $\mathbf{C}$ no longer exists. There are two definitions of ϵ-strong secrecy in the literature [19,20, Lemma 1]: given $\epsilon_1 > 0$, the first definition requires that:

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon_1. \tag{3}$$

  The above equation can be also expressed in terms of KL divergence:

$$D(p_{\mathbf{MC}} || p_{\mathbf{M}} p_{\mathbf{C}}) \leq \epsilon_1.$$

  The second definition of strong secrecy requires a bound on the total variation distance (instead of KL divergence). Given some $\epsilon_2 > 0$, we require:

$$\|p_{\mathbf{MC}} - p_{\mathbf{M}} p_{\mathbf{C}}\|_1 \leq \epsilon_2. \tag{4}$$

Remark 1 (Connection between the two definitions). *Let us denote the alphabet set of* $\mathbf{M}$ *by* $\mathcal{M}$*. According to [20, Lemma 1], if* ϵ_1*-strong secrecy of the first definition and* ϵ_2*-strong secrecy of the second definition hold, then:*

$$\frac{\log_2 e}{2}\epsilon_2^2 \leq \epsilon_1 \leq \epsilon_2 \log \frac{|\mathcal{M}|}{\epsilon_2},$$

provided that $|\mathcal{M}| > 4$*. Hence, if* ϵ_1 *becomes small,* ϵ_2 *also becomes small, i.e., strong secrecy in terms of mutual information implies strong secrecy in terms of total variation distance. This can also be shown by Pinsker's inequality as follows:*

$$\|p_{\mathbf{MC}} - p_{\mathbf{M}} p_{\mathbf{C}}\|_1 \leq \sqrt{\frac{1}{2} D(p_{\mathbf{MC}} || p_{\mathbf{M}} p_{\mathbf{C}})} \leq \sqrt{\frac{\epsilon_1}{2}}.$$

For the reverse direction, assume that message M_i *takes values in* $\{1, 2, \cdots, 2^{nR_i}\}$ *where* n *is the blocklength, and* R_i *is the rate of the* i*th message. Then,* $\log|\mathcal{M}| = n\sum_i R_i$*. If we can ensure that the value of* ϵ_2 *decreases in blocklength* n exponentially fast*, then* $n\epsilon_2$ *converges to zero as* n *becomes large, and* $\epsilon_2 \log(|\mathcal{M}|/\epsilon_2)$ *will also converge to zero. This will imply that* ϵ_1 *vanishes as* n *tends to infinity. Thus, if strong secrecy in terms of total variation distance holds with an exponentially vanishing* ϵ_2*, one can conclude the strong secrecy in terms of mutual information.*

- *Weak secrecy.* Similar to strong secrecy, $\mathbf{M}$ and $\mathbf{C}$ are not independent; instead of Eqs. (2) and (3), we say that ϵ-weak secrecy holds if:

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon \cdot H(\mathbf{M}). \tag{5}$$

According to the above definitions, perfect secrecy condition (2) is stronger than strong secrecy condition (3), which in turn is stronger than weak secrecy constraint (5).

Remark 2. *Consider the weak secrecy condition* $I(\mathbf{M}; \mathbf{C}) \leq \epsilon \cdot H(\mathbf{M})$ *and let* $\mathbf{M} \in \{0,1\}^{nR}$ *be* nR *uniform bits. Herein,* n *is the blocklength and* R *is the coding rate. Then, the weak secrecy constraint becomes:*

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon \cdot H(\mathbf{M}) = \epsilon n R,$$

which shows that normalized leakage $\frac{1}{n} I(\mathbf{M}; \mathbf{C}) \leq \epsilon'$ *where* $\epsilon' = \epsilon R$*. Therefore, the weak secrecy condition relates to the normalized leakage, while the strong secrecy condition considers the unnormalized leakage.*

2.3. Some definitions

To prove the equivalence of the weak and strong secrecy, random binning concepts, which are defined in the following, should be used:

- *Random binning.* In random binning, each realization of a random variable is randomly mapped to a bin index. Therefore, random binning is a random function such as $\mathfrak{B} : \mathcal{M} \to \bar{\mathcal{M}}$ which uniformly and independently maps each symbol $m \in \mathcal{M}$ to symbol $\bar{m} \in \bar{\mathcal{M}}$. In other words, $B = \mathfrak{B}(m)$ is a uniform random variable on the set $\{0, 1, \cdots, |\bar{\mathcal{M}}| - 1\}$; for any $m_1 \neq m_2 \in \mathcal{M}$, $B_1 = \mathfrak{B}(m_1)$ is independent of $B_2 = \mathfrak{B}(m_2)$;
- *Linear random binning.* In linear random binning, mapping function $\mathfrak{B}$ is linear. Each (affine) linear random binning has a matrix representation of the form $\bar{M} = AM + V$, where A is the random matrix, and V is the random vector, all with independent

and uniform entries in $\mathbb{F}$. M is considered as a sequence of symbols in finite field $\mathbb{F}$ with the length of ℓ_m and bin index $\bar{M}$ as a sequence of length $\ell_{\bar{m}}$ in $\mathbb{F}$. Linear random binning matrix will be of size $A_{\ell_{\bar{m}} \times \ell_m}$, and V will be of length $\ell_{\bar{m}}$;

- *Distributed random binning.* In distributed random binning, there are a set of random functions $\mathfrak{B}_i : \mathcal{M}_i \to \bar{\mathcal{M}}_i$, $i \in [t]$ where each $\mathfrak{B}_i$ is a random binning function and $\mathfrak{B}_i$s are mutually independent. Distributed linear random binning can be characterized by matrices A_i and drift terms V_i, $\bar{M}_i = A_i M_i + V_i$ where entries of all of A_i and V_i are mutually independent and uniform over $\mathbb{F}$. It should be noted that the following facts hold in distributed linear binning:
  (i) *Uniformity property:* For any values of m_i and $\bar{m}_i$, we have:
  $$\mathbb{P}\left(A_i m_i + V_i = \bar{m}_i\right) = \frac{1}{|\bar{\mathcal{M}}_i|}, \tag{6}$$
  (ii) *Pairwise independence property:* For any values of m_i, m_j, $\bar{m}_i$, and $\bar{m}_j$, we have:
  $$\mathbb{P}(A_i m_i + V_i = \bar{m}_i, A_j m_j + V_j = \bar{m}_j) = \frac{1}{|\bar{\mathcal{M}}_i|^2}. \tag{7}$$

3. Main results

3.1. From weak to strong secrecy for linear and non-linear codes

Consider a collection $\{E_1, E_2, E_3, \cdots, E_r\}$ of subsets of edges of the communication network. Assume that the adversary chooses an index $i \in [r]$ and eavesdrops on the set of edges E_i of the network for the entire communication.

Given message rates R_{M_i}, $i = 1, 2, \cdots, t$ and key rates R_{K_i} for $i = 1, 2, \cdots, \Delta$, it is notable that these message and key rates are achievable as asymptotically and weakly secure if there is a sequence of codes $\mathscr{C}_j$ whose message and key rates converge to R_{M_i}, $i = 1, 2, \cdots, t$ and R_{K_i} for $i = 1, 2, \cdots, \Delta$ as j tends to infinity; furthermore, $\mathscr{C}_j$ is ϵ_j-weakly secure, i.e., satisfying:

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon_j H(\mathbf{M}),$$

for some vanishing sequence $\epsilon_j \to 0$ as j tends to infinity. The mutual information should vanish when the adversary chooses any set of edges E_i for $i \in [r]$. It is proposed that the given message and key rates are achievable as asymptotically and weakly secure with linear codes if one can find a sequence of linear codes $\mathscr{C}_j$ with the above properties.

It is stated here that message rates R_{M_i}, $i = 1, 2, \cdots, t$ and key rates R_{K_i} for $i = 1, 2, \cdots, \Delta$ are achievable as asymptotically and strongly secure if a similar condition holds, except that we require $\mathscr{C}_j$ to be ϵ_j-strongly secure, i.e.:

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon_j,$$

for some vanishing sequence ϵ_j. Asymptotically, strongly secure achievable rates with linear codes are defined similarly.

Theorem 1 (From weak secrecy to strong secrecy for linear and non-linear codes). *Any message and key rates R_{M_i} and R_{K_i} that are achievable as asymptotically, weakly secure are also achievable as asymptotically, strongly secure. In addition, any message and key rates R_{M_i} and R_{K_i} that are achievable as asymptotically, weakly secure with linear codes are also achievable as asymptotically, strongly secure with linear codes.*

In order to prove the above theorem, tools from random binning of sources that are given in the following are required.

3.2. Output statistics of random binning

Output Statistics of Random Binning (OSRB) is a tool introduced in [19] to describe the joint pmf of bin indices of multiple random variables.

Theorem 2 (OSRB Theorem - Theorem 1 in [19]). *Consider dependent random variables $(M_1, M_2, \cdots, M_t, C)$ with joint pmf $p(m_1, m_2, \cdots, m_t, c)$ on the finite alphabet set $\prod_{i=1}^{t} \mathcal{M}_i \times \mathcal{C}$. Let $\mathbf{M}^n$, C^n be n i.i.d. repetitions of $(\mathbf{M}, C)$ where $\mathbf{M} = (M_1, M_2, \cdots, M_t)$, i.e.:*

$$p(\mathbf{m}^n, c^n) = \prod_{i=1}^{n} p(\mathbf{m}_i, c_i).$$

Moreover, it is assumed that distributed random binning function $\mathfrak{B}_i : \mathcal{M}_i^n \to \bar{\mathcal{M}}_i = [2^{nR_i}]$, $i \in [t]$ maps each sequence of $\mathcal{M}_i^n$ independently and uniformly to the bin index set $[2^{nR_i}]$ that induces the following pmf:

$$P(\mathbf{m}^n, c^n, \bar{\mathbf{m}}) = p(\mathbf{m}^n, c^n) \cdot \prod_{i=1}^{t} \mathbb{1}\left[\mathfrak{B}_i(m_i^n) = \bar{m}_i\right],$$

where $\mathbf{m}^n = \{m_i^n, i \in [t]\}$ and $\bar{\mathbf{m}} = \{\bar{m}_i \in [2^{nR_i}], i \in [t]\}$. Note that $P(\mathbf{m}^n, c^n, \bar{\mathbf{m}})$ shown by capital letter is a random pmf, which is equal to $p_{\mathbf{m}^n, c^n | \mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_t}$ for each fixed binning.

According to the OSRB theorem, for each $\mathcal{S} \subseteq [t]$, if the binning rate vector $(R_1, R_2, \cdots, R_t)$ satisfies the inequality,

$$\sum_{i \in \mathcal{S}} R_i < H(\mathbf{M}_{\mathcal{S}} | C),$$

the expected value of the total variation of the joint pmf $P(c^n, \bar{\mathbf{m}})$ from the $p_{c^n} \prod_{i=1}^{t} p_{[2^{nR_i}]}^{U}$ tends to zero as n approaches infinity:

$$\lim_{n\to\infty} \mathbb{E}_{\mathfrak{B}} \left\| P(c^n, \bar{\mathbf{m}}) - p_{c^n} \prod_{i=1}^{t} p^U_{[2^{nR_i}]} \right\|_1 \to 0. \qquad (8)$$

In the above equation, $\mathfrak{B} = \{\mathfrak{B}_i,\ i \in [t]\}$ is the set of all random functions, and $p^U_{[2^{nR_i}]}$ refers to the uniform distribution on the bin index set $[2^{nR_i}]$. The expectation in Relation (8) is to take over the random realization of the binning mappings.

To prove our results, we state and prove the following improved version of the OSRB theorem, which states that the average of the total variation distance in Relation (8) converges to zero and *exponentially fast*.

Proposition 1. *Assuming that all the random variables in the statement of Theorem 2 take values in finite sets, the expected value of the total variation of the joint pmf $P(c^n, \bar{\mathbf{m}})$ from $p_{c^n} \prod_{i=1}^{t} p^U_{[2^{nR_i}]}$ tends to zero and exponentially fast as $2^{-\kappa n}$ for some constant κ, as n approaches infinity.*

A linear version of the OSRB theorem is also required. Assume that M_is are vectors of symbols in a finite field $\mathbb{F}$. Then, n, i.i.d. repetitions of M_i, namely M_i^n, can be also understood as a (longer) sequence of symbols in $\mathbb{F}$. Thus, a linear random binning of rate R_i, namely $\mathfrak{B}_i : \mathcal{M}_i^n \to \bar{\mathcal{M}}_i = \mathbb{F}^{\frac{nR_i}{\log|\mathbb{F}|}}$, can be constructed as $\bar{M}_i = A_i M_i^n + V_i$ for some random matrices such as A_i and vector V_i with mutually independent and uniform entries. We can now state the linear version of the OSRB theorem.

Theorem 3 (Linear OSRB). *Assume that M_is are the vectors of symbols in a finite field. Theorem 2 holds if the general random binning is replaced with linear random binning.*

3.3. Simulation from a bin index

In a wireline network, a message M may be available at multiple source nodes. In the proof of Theorem 1, a type of coordination among the source nodes with access to M is required. To ensure this coordination, it is assumed that an additional common key is shared among these source nodes. The rate of this extra key is computed by the tool provided in this section.

Assume that X is distributed uniformly on some alphabet set and let X^n be an i.i.d. repetition of X. Let $B = \mathfrak{B}(x^n) \in \{0, 1, \cdots, 2^{nR} - 1\}$ be a random binning of X^n at rate R. Given any particular realization of the binning, we end up with some joint distribution p_{BX^n} where B is a function of X^n. According to this joint distribution, the conditional pmf $p_{X^n|B}$ is considered. Observe that multiple X^n may be mapped to $B = b$; hence, $p_{X^n|B}$ is not a deterministic channel. We now ask for the minimum random bit rate required to simulate channel $p_{X^n|B}$ as defined by Steinberg and Verdu in [21]. In other words, given input B of the channel $p_{X^n|B}$, we ask for the minimum number of uniformly random bits (independent of input B) that we need to simulate channel $p_{X^n|B}$ accurately. In particular, if the simulated channel is denoted by $\tilde{p}_{X^n|B}$, the total variation distance:

$$\|p_B p_{X^n|B} - p_B \tilde{p}_{X^n|B}\|_1,$$

is defined as a measure of the accuracy of channel simulation [21].

Observe that $H(X^n|B) = H(X^n) - H(B) = n\log|\mathcal{X}| - H(B) \geq n\log|\mathcal{X}| - nR$. Intuitively speaking, to simulate conditional pmf $p_{X^n|B}$, a random source of average rate $\log|\mathcal{X}| - R$ is required. The following theorem shows that the rate $\log|\mathcal{X}| - R + \delta$ (for any $\delta > 0$) is sufficient with high probability.

Theorem 4. *Consider some $R < \log|\mathcal{X}|$ and $\delta > 0$. Let T be a source of randomness, uniformly distributed over an alphabet $\mathcal{T}$ satisfying $\frac{1}{n}\log|\mathcal{T}| \leq \tilde{R} = \log|\mathcal{X}| - R + \delta$. Given any realization of the binning, a deterministic simulation function $\phi(T, B)$ is imposed on the channel:*

$$\tilde{p}_{X^n|B}(x^n|b) = \frac{1}{|\mathcal{T}|} \sum_t \mathbb{1}[\phi(t, b) = x^n].$$

Then, it can be claimed that one can find a deterministic simulation function ϕ for any realization of the binning such that:

$$\mathbb{E}_{\mathfrak{B}} \|P_B P_{X^n|B} - P_B \tilde{P}_{X^n|B}\|_1 \leq 2^{-\eta n},$$

converges to zero exponentially fast in n for some $\eta > 0$. Herein, the expectation is taken over all realizations of the binning. Furthermore, if the binning from X^n to B is linear, then one can find a deterministic linear simulation function $\phi(T, B)$ to satisfy the desired property.

3.4. Results for linear codes

For linear codes, a stronger result is shown. More precisely, in Theorem 5, it is shown that, for the linear case, the rate region with a strongly-secure condition is equivalent to one with a perfectly-secure constraint. Theorem 6 states the equivalency of ϵ-error to zero-error rate region for the linear case.

Theorem 5 (From strong secrecy to perfect secrecy for linear codes). *Take an arbitrary linear code $\mathscr{C}$ with adversary observing:*

$$\mathbf{C} = A\mathbf{M} + B\mathbf{K} + G\mathbf{W},$$

as defined in Eq. (1). If the strong secrecy constraint $I(\mathbf{M}; \mathbf{C}) \leq \epsilon$ holds for some $\epsilon < 1$, or the strong secrecy constraint $\|p_{\mathbf{MC}} - p_{\mathbf{M}} p_{\mathbf{C}}\|_1 \leq \epsilon$ holds for some $\epsilon < 1/2$, then code $\mathscr{C}$ is also perfectly secure, i.e., $I(\mathbf{M}; \mathbf{C}) = 0$.

Theorem 6 (From ϵ-error to zero-error for linear codes). *Take an arbitrary linear code $\mathscr{C}$ over a*

finite field $\mathbb{F}$. If the average error probability of a sink node is less than $1-1/|\mathbb{F}|$, then the error probability of the sink node has to be zero.

4. Proofs

4.1. Proof of Theorem 1

We begin by assuming that $r = 1$, i.e., there is only one set of edges E_1 that the adversary can observe. We show in Remark 3 how the result can be extended to arbitrary r.

4.1.1. Assumptions and definitions

Some definitions: Assume that there are u sink nodes and message M_i is desired by sinks $\mathcal{T}_i \subseteq [u]$. Let us consider $\hat{M}_{ij}$ to be the reconstruction of M_i by sink $j \in \mathcal{T}_i$. Since the error probability of code $\mathscr{C}$ is ϵ_b, By Fano's inequality, we have:

$$H(M_i|\hat{M}_{ij}) \leq h(\epsilon_b) + \epsilon_b \log|\mathcal{M}_i|, \qquad \forall j \in \mathcal{T}_i. \tag{9}$$

Let $\delta_i = h(\epsilon_b) + \epsilon_b \log|\mathcal{M}_i|$, and:

$$\delta = \max_{i\in[t]} \delta_i. \tag{10}$$

If we fix the coding operations at all nodes, the output reconstructions and eavesdropper's information will be the functions of message $\mathbf{M}$, secret key $\mathbf{K}$, and private randomness $\mathbf{W}$:

$$\left(\hat{\mathbf{M}}, \mathbf{C}\right) = g(\mathbf{M}, \mathbf{K}, \mathbf{W}).$$

Independent repetitions of code $\mathscr{C}$: Assume that the above code is independently run n times. In other words, instead of considering one copy of message M_i, assume that n i.i.d. copies $M_i(1), M_i(2), \cdots, M_i(n)$ exist for $i \in [t]$. For each of n copies of the messages, the given code is run, and the sinks produce reconstructions $\hat{M}_{ij}(1), \hat{M}_{ij}(2), \cdots, \hat{M}_{ij}(n)$ for $i \in [t], j \in \mathcal{T}_i$. We call expansion n i.i.d. repetitions of the code and denote it by $\mathscr{C}^n$. Observe that the rate of expanded code $\mathscr{C}^n$ is equal to the rate of original code $\mathscr{C}$, because even though the links in the network use n times a single code, the message communicated over the network is also multiplied by n. Similarly, the rates of secret keys shared among the network nodes remain unchanged. By summing up the weak secrecy conditions $I(\mathbf{M}(i); \mathbf{C}(i)) \leq \epsilon_a \cdot H(\mathbf{M}(i))$ for each repetition of the code, we obtain that:

$$I(\mathbf{M}([n]); \mathbf{C}([n])) \leq \epsilon_a \cdot H(\mathbf{M}([n])),$$

where $\mathbf{M}([n]) = \{\mathbf{M}(1), \mathbf{M}(2), \cdots, \mathbf{M}(n)\}$ is a collection of all messages of $\mathscr{C}^n$. It is observed that the weak secrecy condition holds with the same parameter ϵ_a for $\mathscr{C}^n$. However, the error probability of expanded code $\mathscr{C}^n$ is higher, because $\mathscr{C}^n$ will be in error if an error occurs in *any* of n iterations of the code. Nonetheless, by properly appending the expanded space provided by $\mathscr{C}^n$, we not only bring down the error probability, but also go from weak secrecy to strong secrecy at a cost of sacrificing an asymptotically vanishing reduction in message rates.

We can represent expanded code $\mathscr{C}^n$ by i.i.d. variables $(\hat{\mathbf{M}}(i), \mathbf{C}(i), \mathbf{M}(i), \mathbf{K}(i), \mathbf{W}(i))$ for $i \in [n]$ and follow that:

$$(\hat{\mathbf{M}}(i), \mathbf{C}(i)) = g(\mathbf{M}(i), \mathbf{K}(i), \mathbf{W}(i)).$$

4.1.2. High-level structure of the proof

Suppose that there is a code $\mathscr{C}$ that satisfies the weak secrecy condition with parameter ϵ_a, i.e.,

$$I(\mathbf{M}; \mathbf{C}) \leq \epsilon_a \cdot H(\mathbf{M}), \tag{11}$$

where $\mathbf{C}$ is the eavesdropper's side information from observing edges in E_1. In addition, assume that the error probability of the code is ϵ_b. Then, a sequence of strongly-secure codes $\mathscr{C}'_n$ is presented whose information leakage vanishes as n tends to infinity. The message rates of $\mathscr{C}'_n$ converge to a number that is at least $R_{M_i} - \beta$, and the key rates of $\mathscr{C}'_n$ converge to a number that is at most $R_{K_i} + \beta$, where β is a constant that depends only on ϵ_a and ϵ_b. Furthermore, β converges to zero as ϵ_a and ϵ_b converge to zero. Constructing this sequence of strongly secure codes completes the proof. This sequence of codes is constructed by repeating original code $\mathscr{C}$ and properly appending the repeated code.

4.1.3. Formal proof

Step 1: Construction of $\widetilde{M}_i$ and F_i for $i \in [t]$: Let $R_i = \log|\mathcal{M}_i|$. This quantity is proportional to R_{M_i} of code $\mathscr{C}$. In fact, if code $\mathscr{C}$ consists of k uses of the network, then $R_{M_i} = R_i/k$ is the message sent per network use. Let:

$$\tilde{R}_i = R_i - 2\epsilon_a \cdot H(\mathbf{M}) - 2\delta, \tag{12}$$

$$R_{F_i} = 2\delta, \tag{13}$$

where δ was defined in Eq. (10).

Observe that the repetitions of message M_i, i.e., $M_i([n])$, has alphabet set $\mathcal{M}_i^n$. Two independent binnings of $\mathcal{M}_i^n$ are considered: one into $2^{n\tilde{R}_i}$ bins and another into $2^{nR_{F_i}}$ bins. These binnings are done randomly and independently. By applying the (random) binning mapping to $M_i([n])$, let us denote the bin indices by $\widetilde{M}_i$ and F_i, respectively. The binning mappings can be linear or non-linear depending on whether we are proving the theorem for linear or non-linear case.

According to Proposition 1, for any $\mathcal{S} \subseteq [t]$, if the binning rate vector:

$$\left(\tilde{R}_1, R_{F_1}, \tilde{R}_2, R_{F_2}, \cdots, \tilde{R}_t, R_{F_t}\right),$$

satisfies the following inequality:

$$\sum_{i\in\mathcal{S}} \tilde{R}_i + R_{F_i} < H(M_{\mathcal{S}}|\mathbf{C}) = H(M_{\mathcal{S}}) - I(M_{\mathcal{S}};\mathbf{C})$$

$$= \sum_{i\in\mathcal{S}} R_i - I(M_{\mathcal{S}};\mathbf{C}), \tag{14}$$

then one can find $\kappa > 0$ such that for sufficiently large enough n:

$$\mathbb{E}\left\| P_{\widetilde{\mathbf{M}}\mathbf{F}\mathbf{C}([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}([n])} \right\|_1 \leq 2^{-\kappa n}, \tag{15}$$

where the expected value is over all of the random binning mappings and p^U is the uniform distribution. Consider that Eq. (14) holds by the choice of $\tilde{R}_i$ and R_{F_i} given in Eqs. (12) and (13). The reason is that:

$$\sum_{i\in\mathcal{S}} \tilde{R}_i + R_{F_i} = \left(\sum_{i\in\mathcal{S}} R_i\right) - 2\epsilon_a|\mathcal{S}|\cdot H(\mathbf{M})$$

$$\overset{(a)}{\leq} \left(\sum_{i\in\mathcal{S}} R_i\right) - \epsilon_a|\mathcal{S}|\cdot H(\mathbf{M}) - |\mathcal{S}|\cdot I(\mathbf{M};\mathbf{C})$$

$$\leq \left(\sum_{i\in\mathcal{S}} R_i\right) - \epsilon_a|\mathcal{S}|\cdot H(\mathbf{M}) - I(M_{\mathcal{S}};\mathbf{C})$$

$$< \left(\sum_{i\in\mathcal{S}} R_i\right) - I(M_{\mathcal{S}};\mathbf{C}),$$

where (a) follows the weak secrecy condition.

Next, some Slepian-Wolf decoders should be defined here. Csiszár in [22, Theorems 1 and 3] proved the existence of error exponents for the Slepian-Wolf theorem [23] for random non-linear and linear binning. This result implies that $M_i([n])$ can be recovered from bin index F_i and side information $\hat{M}_{ij}([n])$ for any $j \in \mathcal{T}_i$ with an error probability of at most $2^{-n\beta_i}$ for some $\beta_i > 0$ if:

$$R_{F_i} > H\left(M_i|\hat{M}_{ij}\right),$$

and n is sufficiently large. Note that the probability of success of the Slepian-Wolf decoder is with respect to random binning (computed by taking the statistical average over all random binnings). Observe that R_{F_i} given in Eq. (13) satisfies this inequality because of Eqs. (9) and (10). Let:

$$R_{G_i} = 2\epsilon_a \cdot H(\mathbf{M}) + 3\delta. \tag{16}$$

As $R_{G_i} + \tilde{R}_i > H(M_i)$, by Theorem 4, one can simulate the channel $p_{M_i([n])|\widetilde{M}_i}$ using randomness of rate R_{G_i} within an average total variation distance of at most $2^{-n\zeta_i}$ for some $\zeta_i > 0$.

We claim that there is a *deterministic* binning such that for some $\eta > 0$:

(i) We have:

$$\left\| p_{\widetilde{\mathbf{M}}\mathbf{F}\mathbf{C}([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}([n])} \right\|_1 \leq 2^{-\eta n}. \tag{17}$$

(ii) For any i, with probability $1 - 2^{-\eta n}$, one can recover $M_i([n])$ from bin index F_i and side information $\hat{M}_{ij}([n])$ for any $j \in \mathcal{T}_i$.

(iii) For any i, one can simulate the channel $p_{M_i([n])|\widetilde{M}_i}$ using randomness of rate R_{G_i} within a total variation distance of at most $2^{-\eta n}$.

The reason is that we determine that the average of the sum of the total variation distance of Relation (17) plus the error probabilities of the Slepian-Wolf decoders plus the total variation distance of the channel simulator converges to zero (exponentially fast) over all random instances.

Hence, there must exist a deterministic binning (a fixing of binnings) that makes this total sum converge to zero (exponentially fast).

Step 2: Completing the proof using $\widetilde{M}_i$ and F_i for $i \in [t]$: A new code $\widetilde{\mathscr{C}}$ is constructed as follows: the ith message is denoted by $\widetilde{M}_i$ and is uniformly distributed over a set of size $2^{n\tilde{R}_i}$. The nodes of the network also have shared keys of the same length as they have in $\mathscr{C}^n$. Additionally, the source nodes that obtain the ith message $\widetilde{M}_i$ are assumed to share a common secret key of rate R_{G_i}. This secret key is used by them to simulate the same channel $p_{M_i([n])|\widetilde{M}_i}$. The source nodes pass their messages $\widetilde{M}_i$ through this channel to produce $M_i([n])$. Having produced $M_i([n])$, the nodes can find F_i (which is a function of $M_i([n])$). Furthermore, with their simulated $M_i([n])$, we can use the encoding and decoding operations of $\mathscr{C}^n$. This gives the adversary random variable $\mathbf{C}([n])$. Furthermore, the source nodes send variables F_i through the network links. This comes at a negligible additional cost since R_{F_i} can be made arbitrarily small. This gives the adversary random variables $\mathbf{C}([n])$ and $\mathbf{F}$.

Secrecy and reliability analysis: Observe that the induced pmf on $\widetilde{M}_i$, $M_i([n])$ and F_i is as follows:

$$p^U_{\widetilde{\mathbf{M}}} \cdot \tilde{p}_{\mathbf{M}([n])|\widetilde{\mathbf{M}}} \cdot p_{\mathbf{F},\mathbf{C}([n])|\mathbf{M}([n])}.$$

By Relation (17):

$$\|p^U_{\widetilde{\mathbf{M}}} - p_{\widetilde{\mathbf{M}}}\|_1 \leq 2^{-\eta n},$$

and by (iii) in Step 1:

$$\|p_{\widetilde{\mathbf{M}}}\tilde{p}_{\mathbf{M}([n])|\widetilde{\mathbf{M}}} - p_{\widetilde{\mathbf{M}}} p_{\mathbf{M}([n])|\widetilde{\mathbf{M}}}\|_1 \leq 2^{-\eta n}.$$

Referring to [19, Lemma 3, part 3], we obtain that:

$$\|p^U_{\widetilde{\mathbf{M}}} \cdot \tilde{p}_{\mathbf{M}([n])|\widetilde{\mathbf{M}}} \cdot p_{\mathbf{F},\mathbf{C}([n])|\mathbf{M}([n])} - p_{\widetilde{\mathbf{M}}}$$

$$\cdot p_{\mathbf{M}([n])|\widetilde{\mathbf{M}}} \cdot p_{\mathbf{F},\mathbf{C}([n])|\mathbf{M}([n])}\|_1 \leq 2 \times 2^{-\eta n}.$$

Hence, the induced pmf of the code $\widetilde{\mathscr{C}}$ is very close to the induced pmf of $\mathscr{C}^n$ with $\widetilde{M}_i$ and F_i created as deterministic bin indices of $M_i([n])$. According to Relation (17), it can be concluded that the strong secrecy condition (total variation distance definition) holds with the total variations in the new code $\widetilde{\mathscr{C}}$, message vector $\widetilde{\mathbf{M}}$ is almost independent of $\mathbf{F}$, $\mathbf{C}([n])$. Since the distance dropping exponentially fast in n, based on Remark 1, the strong secrecy condition is obtained in the sense of vanishing mutual information between $\widetilde{\mathbf{M}}$ and $\mathbf{F}$, $\mathbf{C}([n])$.

The sink nodes use the encoding and decoding operations of $\mathscr{C}^n$. This allows the sinks to produce reconstructions $\hat{M}_{ij}(1), \hat{M}_{ij}(2), \cdots, \hat{M}_{ij}(n)$. Since F_is are also sent from source nodes to sink nodes via the network links, based on the property (ii) given above, the sinks can decode their intended messages with vanishing error probability. This completes the proof.

Remark 3. *An eavesdropper who can choose to eavesdrop on anyone of E_is for some $i \in [r]$ can be thought of as r eavesdroppers with the ith eavesdropper gaining access to the messages on the set of edges in E_i. It is also assumed that $\mathbf{C}_i$ is the information obtained by eavesdropper i from the set E_i of edges in the network. We proved above that if the weak secrecy condition $I(\mathbf{M}; \mathbf{C}_i) \leq \epsilon_i \cdot H(\mathbf{M})$ holds, then there exists a $\kappa_i > 0$ by random binning, such that for sufficiently large enough n.*

$$\mathbb{E}\left\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \right\|_1 \leq 2^{-\kappa_i n}.$$

Accordingly, there exist $\kappa_1, \kappa_2, \cdots, \kappa_r > 0$ such that:

$$\sum_{i=1}^{r} \mathbb{E}\left\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \right\|_1 \leq \sum_{i=1}^{r} 2^{-\kappa_i n}.$$

Additionally, by the linear property of the expectation, one can write:

$$\mathbb{E}\sum_{i=1}^{r} \left\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \right\|_1 \leq \sum_{i=1}^{r} 2^{-\kappa_i n} \leq r \times 2^{-\min_i \kappa_i n}.$$

Because there are finitely many subsets E_i of edges in the network, r is bounded from above by a constant that does not depend on n. Thus, there exists $\lambda > 0$ such that:

$$\mathbb{E}\sum_{i=1}^{r} \left\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \right\|_1 \leq 2^{-\lambda n}.$$

Therefore, for each and every i, we have:

$$\mathbb{E}\left\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \right\|_1 \leq 2^{-\lambda n}.$$

Accordingly, there exists a deterministic binning satisfying strong secrecy condition for each i.

$$\| P_{\widetilde{\mathbf{MFC}}_i([n])} - p^U_{\widetilde{\mathbf{M}}} p^U_{\mathbf{F}} p_{\mathbf{C}_i([n])} \|_1 \leq 2^{-\lambda n}, \qquad \forall i \in [r].$$

4.2. Proof of Proposition 1

This follows the proof of the OSRB theorem (Theorem 1 in [19]) with minor modifications. Herein, we only mention how the proof should be modified without repeating the entire proof. In our re-statement of the OSRB theorem above, a notation that is suitable for our purposes here is used, which is different from the one used in [19]. However, just for the purpose of writing the modification that needs to be made in the proof given in [19], the notation and definitions of [19] are adopted. We refer the reader to [19] for the definition of variables that we use below.

The proof begins by bounding the total variation distance between two distributions with their fidelity (Lemma 7 of [19]). The paper then states that the expected total variation distance goes to zero, it suffices to show that the corresponding expected fidelity term goes to one as n goes to infinity. Now, to show that the total variation distance goes to zero exponentially fast as $2^{-\alpha n}$, it suffices to show that the "one minus the expected fidelity term" goes to zero exponentially fast. This follows the fact that if an arbitrary sequence $1 - f_n$ tends to zero at least exponentially fast, then $\sqrt{1 - f_n^2} = \sqrt{(1 - f_n)(1 + f_n)}$ also tends to zero exponentially fast.

This fidelity term is bounded from Eqs. (104)-(106) as follows:

$$\mathbb{E}\left[F(P(z^n, b_{[1:T]}); p(z^n)p^U(b_{[1:T]}))\right] \geq p(\mathcal{A}^n_\epsilon)\sqrt{\frac{1}{1 + \sum_{\emptyset \neq \mathcal{S} \subseteq \mathcal{V}} 2^{n(R_{\mathcal{S}} - H(X_{\mathcal{S}}|Z) + \epsilon)}}}, \tag{18}$$

where ϵ is an arbitrary positive number and $\mathcal{A}^n_\epsilon$ is the weak typical set defined as follows:

$$\mathcal{A}^n_\epsilon := \left\{ (x^n_{[1:T]}, z^n) : \frac{1}{n} h(x^n_{[1:T]}|z^n) \geq H(X_{[1:T]}|Z) - \epsilon \right\}. \tag{19}$$

Now, since ϵ is fixed, we know that the probability of i.i.d. $X^n_{[1:T]}, Z^n$ being typical not only converges to one, but also converges exponentially fast. Accordingly:

$$\sqrt{\frac{1}{1 + \sum_{\emptyset \neq \mathcal{S} \subseteq \mathcal{V}} 2^{n(R_{\mathcal{S}} - H(X_{\mathcal{S}}|Z) + \epsilon)}}} \geq \sqrt{1 - \sum_{\emptyset \neq \mathcal{S} \subseteq \mathcal{V}} 2^{n(R_{\mathcal{S}} - H(X_{\mathcal{S}}|Z) + \epsilon)}} \geq 1 - \sum_{\emptyset \neq \mathcal{S} \subseteq \mathcal{V}} 2^{n(R_{\mathcal{S}} - H(X_{\mathcal{S}}|Z) + \epsilon)}, \tag{20}$$

which converges to one exponentially fast if, for each $\mathcal{S} \subseteq [1:T]$, we have $R_{\mathcal{S}} < H(X_{\mathcal{S}}|Z) - \epsilon$. Therefore, both terms on the right-hand side of Relation (18) converge to one exponentially fast. Thus, their product also converges to one exponentially fast.

4.3. Proof of Theorem 3

Eqs. (94) and (98) in [19] represent the only space where random binning enters a calculation in the proof of the OSRB theorem in [19]. However, Eq. (94) in [19] only uses the uniformity condition which is valid for linear binning (Eqs. (6), and (98) in [19] only uses the pairwise independence property that is also valid for linear binning (Eq. (7)).

4.4. Proof of Theorem 4

Fix a realization of the binning mapping $\mathfrak{B}$. Since X^n is uniformly distributed, the conditional distribution of X^n given $B = b$ is also uniform over the set of sequences x^n that are mapped to $B = b$, i.e., $\{x^n : \mathfrak{B}(x^n) = b\}$. We can successfully simulate $p_{X^n|B=b}$ if we can choose a sequence x^n uniformly at random from the set $\{x^n : \mathfrak{B}(x^n) = b\}$. This is possible if $|\{x^n : \mathfrak{B}(x^n) = b\}| \leq 2^{n\tilde{R}}$. Hence, the total variation distance can be bounded from above as follows:

$$\left\|p_B p_{X^n|B} - p_B \tilde{p}_{X^n|B}\right\|_1 \leq \sum_b p_B(b) \mathbb{1}\left[|\{x^n : \mathfrak{B}(x^n) = b\}| > 2^{n\tilde{R}}\right],$$

where we used the fact that when b is such that $|\{x^n : \mathfrak{B}(x^n) = b\}|$ is large, the total variation distance can be at most one. Thus, by taking average over all random binnings, we have:

$$\begin{aligned}\mathbb{E}_{\mathfrak{B}} \left\|P_B P_{X^n|B} - P_B \tilde{P}_{X^n|B}\right\|_1 &\leq \mathbb{P}_{\mathfrak{B},B}\left[|\{x^n : \mathfrak{B}(x^n) = B\}| > 2^{n\tilde{R}}\right] \\ &\overset{(a)}{=} \mathbb{P}_{\mathfrak{B}}\left[|\{x^n : \mathfrak{B}(x^n) = 1\}| > 2^{n\tilde{R}}\right].\end{aligned}$$

where (a) follows symmetry. Now, in a random binning, the number of sequences x^n that are mapped to bin index 1 has a Binomial distribution; we throw $|\mathcal{X}|^n$ sequences, and each falls into the first bin with probability 2^{-nR}. By Markov's inequality, we obtain:

$$\mathbb{P}_{\mathfrak{B}}\left[|\{x^n : \mathfrak{B}(x^n) = 1\}| > 2^{n\tilde{R}}\right] \leq \frac{|\mathcal{X}|^n 2^{-nR}}{2^{n\tilde{R}}} = 2^{-n\delta}.$$

Finally, assume that the binning is linear, i.e., $B = AX^n + V$ for some matrices A and V. Let bin index B be a vector of symbols in $\mathbb{F}$ of length nR' where $R' = \frac{R}{\log|\mathbb{F}|}$. The set $\{x^n : \mathfrak{B}(x^n) = b\} = \{x^n : Ax^n = b - V\}$ is an affine linear subspace with dimension $\text{Null}(A) = n - \text{Rank}(A)$. This set can be written as $Q(b - V) + NT$ for some matrices Q and N and a uniformly distributed vector T whose length is equal to the dimension of $\text{Null}(A)$. If the rank of A is at least $n(R' - \frac{\delta}{\log|\mathbb{F}|})$, the dimension of the null space will be at most $n(1 - R' + \frac{\delta}{\log|\mathbb{F}|})$, and a randomness of size $n(1 - R')\log|\mathbb{F}| = n(\log|\mathcal{X}| - R + \delta)$ would suffice for channel simulation. Hence, the total variation distance can be bounded from above as follows:

$$\mathbb{E}_{\mathfrak{B}}\left\|P_B P_{X^n|B} - P_B \tilde{P}_{X^n|B}\right\|_1 \leq \mathbb{P}_{\mathfrak{B}}\left[\text{Rank}(A) < n\left(R' - \frac{\delta}{\log|\mathbb{F}|}\right)\right]. \tag{21}$$

However, for any $R' < 1$, as is known, the probability that a random matrix $A_{nR'\times n}$ with uniform entries from $\mathbb{F}$ is not full rank vanishes exponentially fast in n; in fact, this probability is lower than $|\mathbb{F}|^{-n(1-R')}(|\mathbb{F}| - 1)^{-1}$ [24, p. 4]. This completes the proof for the linear case.

4.5. Proof of Theorem 5

Assume that $I(\mathbf{M};\mathbf{C}) > 0$ where $\mathbf{C} = A\mathbf{M} + B\mathbf{K} + G\mathbf{W}$. We will show that $I(\mathbf{M};\mathbf{C}) \geq 1$ and $\|p_{\mathbf{MC}} - p_{\mathbf{M}}p_{\mathbf{C}}\|_1 \geq 1/2$. This will conclude the proof.

Assume that $\mathbf{C}$ is a column vector of size k. We claim that one can find a non-zero column vector $\mathbf{z}$ of size k such that $\mathbf{z}^\dagger B = \mathbf{z}^\dagger G = \mathbf{0}$ are the zero vectors; however, $\mathbf{z}^\dagger A \neq \mathbf{0}$, where $\dagger$ is the transpose operator. If this is not the case, equation $\mathbf{z}^\dagger[B, G] = \mathbf{0}$ implies that $\mathbf{z}^\dagger[A, B, G] = \mathbf{0}$, showing that the null space $[B, G]^\dagger$ is the same as the null space of $[A, B, G]^\dagger$. Hence, the rank of the matrix $[A, B, G]$ is equal to that of $[B, G]$. Thus, the image of matrix A is a subset of the image of $[B, G]$. Let us call the image of $[B, G]$ by $\mathscr{I}$, which is a linear subspace of $\mathbb{F}^k$. Since elements of vectors $\mathbf{K}$ and $\mathbf{W}$ are independently and uniformly distributed over $\mathbb{F}$, $B\mathbf{K} + G\mathbf{W}$ will be uniformly distributed over $\mathscr{I}$. Similar to Shannon's one-time-pad strategy, this will imply that $\mathbf{C} = A\mathbf{M} + (B\mathbf{K} + G\mathbf{W})$ will be independent of $A\mathbf{M}$ and masked by $B\mathbf{K} + G\mathbf{W}$. To see this, note that for any value of $\mathbf{M} = \mathbf{m}$, we have $A\mathbf{m} \in \mathscr{I}$, and vector $\mathbf{C} = A\mathbf{m} + B\mathbf{K} + G\mathbf{W}$ will be uniformly distributed over $\mathscr{I}$, too. This is because $\mathscr{I} = A\mathbf{m} + \mathscr{I}$ since $\mathscr{I}$ is a linear subspace. As a result, the conditional distribution $p(\mathbf{C}|\mathbf{m})$ does not depend on the value of $\mathbf{m}$. Hence, perfect secrecy condition holds. However, this contradicts our assumption of $I(\mathbf{M};\mathbf{C}) > 0$. Thus, we can conclude that there is a non-zero column vector $\mathbf{z}$ of size k such that $\mathbf{z}^\dagger B = \mathbf{z}^\dagger G = \mathbf{0}$ are the zero vectors; however, $\mathbf{z}^\dagger A \neq \mathbf{0}$. This implies that $\mathbf{z}^\dagger C = \mathbf{z}^\dagger A\mathbf{M} \neq \mathbf{0}$. Now, observe that:

$$I(\mathbf{M};\mathbf{C}) \geq I\left(\mathbf{M};\mathbf{z}^\dagger\mathbf{C}\right) = I\left(\mathbf{M};\mathbf{z}^\dagger A\mathbf{M}\right) = H\left(\mathbf{z}^\dagger A\mathbf{M}\right) \overset{(a)}{=} \log|\mathbb{F}| \geq 1,$$

where in (a), we used the fact that $\mathbf{M}$ has uniform distribution; hence, $(\mathbf{z}^\dagger A)\mathbf{M}$ is a uniformly distributed symbol in $\mathbb{F}$.

Next, defining functions $\hat{m} = f(\mathbf{m}) = \mathbf{z}^\dagger A\mathbf{m}$ and $\hat{c} = g(\mathbf{c}) = \mathbf{z}^\dagger\mathbf{c} = f(\mathbf{m})$, observe that $\hat{M} = \hat{C}$ is a uniform symbol in $\mathbb{F}$. Then, we can write:

$$\begin{aligned}\left\|p_{\mathbf{M},\mathbf{C}} - p_{\mathbf{M}} \cdot p_{\mathbf{C}}\right\|_1 &\overset{(a)}{\geq} \left\|p_{\hat{M},\hat{C}} - p_{\hat{M}} \cdot p_{\hat{C}}\right\|_1 \\ &= \frac{1}{2}\sum_{a,b\in\mathbb{F}} |\mathbb{1}[a=b] \times \frac{1}{|\mathbb{F}|} - \frac{1}{|\mathbb{F}|^2}| \\ &= \frac{|\mathbb{F}|(|\mathbb{F}|-1)}{|\mathbb{F}|^2} = \left(1 - \frac{1}{|\mathbb{F}|}\right) \geq \frac{1}{2},\end{aligned}$$

where $\mathbb{1}[\cdot]$ is the indicator function, and step (a) follows the data processing property of the total variation distance (see e.g., [25]), which states that, for any channel $p(y|x)$, we have:

$$\|p(x) - q(x)\|_1 \geq \|p(y) - q(y)\|_1,$$

where $p(y) = \sum_x p(x)p(y|x)$ and $q(y) = \sum_x q(x)p(y|x)$. The desired inequality is achieved if the alphabet $\mathcal{X}$ to be the alphabet of $(\mathbf{M},\mathbf{C})$, $p(x) = p(\mathbf{m},\mathbf{c})$, $q(x) = p(\mathbf{m})p(\mathbf{c})$, and $p(y|x)$ is set to be the application of functions f and g applied to $\mathbf{M}$ and $\mathbf{C}$ parts of X, respectively.

4.6. Proof of Theorem 6

Consider a sink node. The sink node receives a vector $\mathbf{Y}$, which is a linear combination of messages, keys, and private randomness symbols. In other words, we have:

$$\mathbf{Y} = A\mathbf{M} + B\mathbf{K} + G\mathbf{W},$$

for some matrices A, B, and G. Message vector $\mathbf{M}$ can be split into two parts $(\mathbf{M}_1, \mathbf{M}_2)$ where $\mathbf{M}_1$ is the set of messages that the sink nodes seek to decode, and $\mathbf{M}_2$ is the collection of other messages. Similarly, $\mathbf{K}$ can be split into two parts $(\mathbf{K}_1, \mathbf{K}_2)$ where $\mathbf{K}_1$ is the set of secret keys that the sink nodes have, and $\mathbf{K}_2$ is the set of secret keys that are not shared with the sink node. Then, we can write:

$$\mathbf{Y} = A_1\mathbf{M}_1 + A_2\mathbf{M}_2 + B_1\mathbf{K}_1 + B_2\mathbf{K}_2 + G\mathbf{W}.$$

Since the sink has vector $\mathbf{Y}$ and key $\mathbf{K}_1$, its task is to recover $\mathbf{M}_1$ from:

$$\mathbf{Y} - B_1\mathbf{K}_1 = A_1\mathbf{M}_1 + A_2\mathbf{M}_2 + B_2\mathbf{K}_2 + G\mathbf{W}.$$

Note that the sink node does not know any of $\mathbf{M}_2$, $\mathbf{K}_2$, or $\mathbf{W}$. These three variables $\mathbf{M}_2$, $\mathbf{K}_2$, or $\mathbf{W}$ are mutually independent and uniform over their alphabet sets. Let $\mathbf{Z} = \mathbf{Y} - B_1\mathbf{K}_1$. Given a value for $\mathbf{Z} = \mathbf{z}$ for some $\mathbf{m}_1$, we say that $(\mathbf{z}, \mathbf{m}_1)$ is a compatible pair if the equation:

$$A_2\mathbf{m}_2 + B_2\mathbf{k}_2 + G\mathbf{w} = \mathbf{z} - A_1\mathbf{m}_1, \tag{22}$$

has a solution in variables $\mathbf{m}_2$, $\mathbf{k}_2$, $\mathbf{w}$.

Given a pair $(\mathbf{z}, \mathbf{m}_1)$, two possibilities might occur:

1. The pair $(\mathbf{z}, \mathbf{m}_1)$ is not compatible. In this case, $p(\mathbf{m}_1|\mathbf{z}) = 0$ and the sink is certain that its intended message is not equal to $\mathbf{m}_1$;
2. The pair $(\mathbf{z}, \mathbf{m}_1)$ is compatible, and the equation

$$A_2\mathbf{m}_2 + B_2\mathbf{k}_2 + G\mathbf{w} = \mathbf{z} - A_1\mathbf{m}_1, \tag{23}$$

has at least one solution for $\mathbf{m}_2$, $\mathbf{k}_2$, $\mathbf{w}$. Then, note that the number of solutions $(\mathbf{m}_2,\mathbf{k}_2,\mathbf{w})$ that satisfy Eq. (23) is fixed and determined by the dimension of the null space of matrix $[A_2, B_2, G]$. Since $\mathbf{M}_2$, $\mathbf{K}_2$, and $\mathbf{W}$ are mutually independent and uniform, $p(\mathbf{m}_1|\mathbf{z})$ is equal to the number of solutions $(\mathbf{m}_2, \mathbf{k}_2, \mathbf{w})$ of Eq. (23), divided by the total number of triples $(\mathbf{m}_2, \mathbf{k}_2, \mathbf{w})$. This implies that from the perspective of the sink that has vector $\mathbf{z}$, all messages $\mathbf{m}_1$ that are compatible with $\mathbf{z}$ are equally likely to have been the transmitted message.

Assume that the sink's error probability is positive. It is shown that for any vector $\mathbf{z}$ that the sink may end up with, there are at least $|\mathbb{F}|$ sequences $\mathbf{m}_1$ that are compatible with $\mathbf{z}$. Thus, the chance of correct decoding will be at most $1/|\mathbb{F}|$. This would complete the proof.

Now, if the sink's error probability is positive, there exist some vector $\mathbf{z}$ and two distinct compatible sequences $\mathbf{m}'_1 \neq \mathbf{m}^*_1$ with it, i.e., the following two equations have solutions $(\mathbf{m}_2, \mathbf{k}_2, \mathbf{w})$ and $(\mathbf{m}'_2, \mathbf{k}'_2, \mathbf{w}')$:

$$A_2\mathbf{m}^*_2 + B_2\mathbf{k}^*_2 + G\mathbf{w}^* = \mathbf{z} - A_1\mathbf{m}^*_1, \tag{24}$$

$$A_2\mathbf{m}'_2 + B_2\mathbf{k}'_2 + G\mathbf{w}' = \mathbf{z} - A_1\mathbf{m}'_1. \tag{25}$$

By subtracting these two equations, we get that for $\mathbf{m}''_1 = \mathbf{m}^*_1 - \mathbf{m}'_1 \neq \mathbf{0}$, the equation:

$$A_2\mathbf{m}''_2 + B_2\mathbf{k}''_2 + G\mathbf{w}'' = -A_1\mathbf{m}''_1, \tag{26}$$

has a solution:

$$(\mathbf{m}''_2, \mathbf{k}''_2, \mathbf{w}'') = (\mathbf{m}^*_2, \mathbf{k}^*_2, \mathbf{w}^*) - (\mathbf{m}'_2, \mathbf{k}'_2, \mathbf{w}').$$

Now, consider any vector $\mathbf{z}$ that the sink may end up with and let $\mathbf{m}_1$ be the true message sequence that is compatible with $\mathbf{z}$. We claim that $\mathbf{z}$ is also compatible with $\mathbf{m}_1 + \alpha\mathbf{m}''_1$ for any $\alpha \in \mathbb{F}$. This follows multiplying both sides of Eq. (26) by α and, then, adding it up with Eq. (22). Since $\mathbf{m}''_1 \neq 0$, the sequences $\mathbf{m}_1 + \alpha\mathbf{m}''_1$ for different values of α are distinct vectors. Since α has $|\mathbb{F}|$ possibilities, this shows that there are at least $|\mathbb{F}|$ sequences $\mathbf{m}_1$ that are compatible with $\mathbf{z}$.

5. Conclusion

In this paper, a setup was considered that contained t transmitter, u receivers, and some intermediate nodes being connected with directed error-free point-to-point links. It was also assumed that there existed an eavesdropper able to hear a certain subset of links. In order to provide secrecy, each node had access to some keys and private randomness. Defining different conditions associated with decoding error and secrecy, i.e., zero and ϵ-error decoding, as well as weak, strong, and perfect secrecy constraints, this study sought to find a relation between rate regions considering different conditions. In Theorem 5, it was shown that, for the linear case, the rate region with a strongly-secure condition was equivalent to one with a perfectly-secure constraint. Theorem 6 states the equivalency of ϵ-error to zero-error rate region for the linear case. Moreover, it was shown in Theorem 1 for the general case (both linear and non-linear regimes) that relaxing the secrecy condition from strong to weak secrecy does not change the rate region when there is an ϵ-error decoding condition. Our conjecture is that the ϵ-error weakly-secure rate region is equivalent to zero-error perfectly-secure one in the general case.

Acknowledgment

The authors would like to thank Mohammad Hossein Yassaee for his helpful comments.

References

1. Shannon, C.E. "The zero error capacity of a noisy channel", *Information Theory, IRE Transactions on*, **2**(3), pp. 8-19 (1956).
2. Langberg, M. and Effros, M. "Network coding: Is zero error always possible?", In *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, pp. 1478-1485, IEEE (2011).
3. Chan, T. and Grant, A. "On capacity regions of non-multicast networks", In *2010 IEEE International Symposium on Information Theory*, pp. 2378-2382, IEEE (2010).
4. Maurer, U. and Wolf, S. "Information-theoretic key agreement: From weak to strong secrecy for free", In *Advances in Cryptology-EUROCRYPT 2000*, pp. 351-368, Springer (2000).
5. Jalali, S. and Ho, T. "On capacity region of wiretap networks", arXiv preprint arXiv:1212.3859 (2012).
6. Mojahedian, M.M., Gohari, A., and Aref, M.R. "Perfectly secure index coding", *Information Theory, IEEE Transactions on*, **63**(11), pp. 7382-7395 (2017).
7. Cai, N. and Yeung, R.W. "Secure network coding", In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, p. 323, IEEE (2002).
8. Cheng, F. and Yeung, R.W. "Performance bounds on a wiretap network with arbitrary wiretap sets", *IEEE Transactions on Information Theory*, **60**(6), pp. 3345-3358 (2014).
9. Cui, T., Ho, T., and Kliewer, J. "Achievable strategies for general secure network coding", In *Information Theory and Applications Workshop (ITA)*, **2010**, pp. 1-6, IEEE (2010).
10. Cui, T., Ho, T., and Kliewer, J. "On secure network coding with nonuniform or restricted wiretap sets", *IEEE Transactions on Information Theory*, **59**(1), pp. 166-176 (2013).
11. Czap, L., Fragouli, C., Prabhakaran, V.M., and Diggavi, S. "Secure network coding with erasures and feedback", *IEEE Transactions on Information Theory*, **61**(4), pp. 1667-1686 (2015).
12. El Rouayheb, S., Soljanin, E., and Sprintson, A. "Secure network coding for wiretap networks of type ii", *IEEE Transactions on Information Theory*, **58**(3), pp. 1361-1371 (2012).
13. Feldman, J., Malkin, T., Stein, C., and Servedio, R.A. "On the capacity of secure network coding", In *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing*, pp. 63-68 (2004).
14. Huang, W., Ho, T., Langberg, M., and Kliewer, J. "On secure network coding with uniform wiretap sets", In *2013 International Symposium on Network Coding (NetCod)*, pp. 1-6, IEEE (2013).
15. Mishra, S., Fragouli, C., Prabhakaran, V., and Diggavi, S. "Using feedback for secrecy over graphs", In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, IEEE*, pp. 2399-2403 (2013).
16. Silva, D. and Kschischang, F.R. "Security for wiretap networks via rank-metric codes", In *2008 IEEE International Symposium on Information Theory, IEEE*, pp. 176-180 (2008).
17. Fragouli, C. and Soljanin, E. "(Secure) linear network coding multicast", *Designs, Codes and Cryptography*, **78**(1), pp. 269-310 (2016).
18. Dau, S.H., Skachek, V., and Chee, Y.M. "On secure index coding with side information", In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on, IEEE*, pp. 983-987 (2011).
19. Yassaee, M.H., Aref, M.R., and Gohari, A. "Achievability proof via output statistics of random binning", *Information Theory, IEEE Transactions on*, **60**(11), pp. 6760-6786 (2014).
20. Csiszár, I. and Narayan, P. "Secrecy capacities for multiple terminals", *IEEE Transactions on Information Theory*, **50**(12), pp. 3047-3061 (2004).
21. Steinberg, Y. and Verdu, S. "Channel simulation and coding with side information", *IEEE Transactions on Information Theory*, **40**(3), pp. 634-646 (1994).
22. Csiszár, I. "Linear codes for sources and source networks: Error exponents, universal coding", *IEEE*

Transactions on Information Theory, **28**(4), pp. 585-592 (1982).

23. Slepian, D. and Wolf, J. "Noiseless coding of correlated information sources", *IEEE Transactions on information Theory*, **19**(4), pp. 471-480 (1973).
24. Blake, I.F. and Studholme, C. "Properties of random matrices and applications", Unpublished report available at www.cs.toronto.edu/~cvs/coding/random_ report.pdf (2006).
25. Pardo Llorente, M.D.C. and Vajda, I. "About distances of discrete distributions satisfying the data processing theorem of information theory", *IEEE Transactions on Information Theory*, **43**(4), pp. 1288-1293 (1997).
26. Shannon, C.E. "Communication theory of secrecy systems", *Bell System Technical Journal*, **28**(4), pp. 656-715 (1949).
27. Birk, Y. and Kol, T. "Informed-source coding-on-demand (ISCOD) over broadcast channels", In *INFOCOM'98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings, IEEE*, **3**, pp. 1257-1264 (1998).
28. Lubetzky, E. and Stav, U. "Nonlinear index coding outperforming the linear optimum", *Information Theory, IEEE Transactions on*, **55**(8), pp. 3544-3551 (2009).
29. Alon, N., Lubetzky, E., Stav, U., Weinstein, A., and Hassidim, A. "Broadcasting with side information", In *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*, pp. 823-832, IEEE (2008).
30. Bar-Yossef, Z., Birk, Y., Jayram, T., and Kol, T. "Index coding with side information", *Information Theory, IEEE Transactions on*, **57**(3), pp. 1479-1494 (2011).
31. Tehrani, A.S., Dimakis, A.G., and Neely, M.J. "Bipartite index coding", In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pp. 2246-2250, IEEE (2012).
32. Blasiak, A., Kleinberg, R., and Lubetzky, E. "Broadcasting with side information: Bounding and approximating the broadcast rate", *Information Theory, IEEE Transactions on*, **59**(9), pp. 5811-5823 (2013).
33. Blasiak, A., Kleinberg, R., and Lubetzky, E. "Index coding via linear programming", arXiv preprint arXiv:1004.1379 (2010).
34. Arbabjolfaei, F., Bandemer, B., Kim, Y.-H., Sasoglu, E., and Wang, L. "On the capacity region for index coding", In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, IEEE*, pp. 962-966 (2013).
35. Shanmugam, K., Dimakis, A.G., and Langberg, M. "Graph theory versus minimum rank for index coding", arXiv preprint arXiv:1402.3898 (2014).
36. Neely, M.J., Tehrani, A.S., and Zhang, Z. "Dynamic index coding for wireless broadcast networks", In *INFOCOM, 2012 Proceedings IEEE*, pp. 316-324, (2012).

Biographies

Mohammad Mahdi Mojahedian is a PhD candidate in Communication Systems Group, Sharif University of Technology, Tehran, Iran. He received two BSc degrees, one in Communications and the other in Electronics, from Amirkabir University of Technology, Tehran, Iran in 2009 and 2010, and an MSc degree in Communication Systems from Sharif University of Technology, Tehran, Iran in 2012. Since 2012, he has been with the Information Systems and Security Lab (ISSL) at Sharif University of Technology and a visiting student at the Institute for Digital Communications, University of Erlangen, Nuremberg from June 2016 to December 2016. He also has been a finalist for the Jack Keil Wolf student paper award at the ISIT symposium 2015. His research interests include information theory, wireless communications, and computer science.

Mohammad Reza Aref received the BSc degree in 1975 from the University of Tehran, Iran, and the MSc and PhD degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in Electrical Engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of Electrical Engineering at Sharif University of Technology, Tehran since 1995, and he has published more than 290 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.

Amin Gohari is an Associate Professor at Sharif University of Technology, Tehran, Iran. He received his MSc and PhD degrees in Electrical Engineering in 2010 from the University of California, Berkeley, and his BSc degree in 2004 from Sharif University of Technology, Iran. He received the 2010 Eli Jury Award from UC Berkeley, Department of Electrical Engineering for "outstanding achievement in the area of communication networks" and the 2009-2010 Bernard Friedman Memorial Prize in Applied Mathematics from UC Berkeley, Department of Mathematics, for "demonstrated ability to do research in applied mathematics." He also received the Gold Medal from the 41st International Mathematical Olympiad (IMO 2000) and the First Prize from the 9th International Mathematical Competition for University Students (IMC 2002). He is also a co-author of a paper that received the 2013 Jack Keil Wolf ISIT Student Paper Award. He was selected as an exemplary reviewer for Transactions on Communications in 2016 and 2017.