Secure Multi-Source Multicast

Alejandro Cohen
BGU

Asaf Cohen
BGU

Muriel Médard
MIT

Omer Gurewitz
BGU

***Abstract*—The principal mission of *Multi-Source Multicast* (MSM) is to disseminate all messages from all sources in a network to all destinations. MSM is utilized in numerous applications. In many of them, securing the messages disseminated is critical.**

A common secure model is to consider a network where there is an eavesdropper which is able to observe a subset of the network links, and seek a code which keeps the eavesdropper ignorant regarding *all the messages*. While this is solved when all messages are located at a single source, *Secure MSM* (SMSM) is an open problem, and the rates required are hard to characterize in general.

In this paper, we consider *Individual Security*, which promises that the eavesdropper has zero mutual information with *each message individually*, or, more generally, with *sub sets of messages*. We completely characterize the rate region for SMSM under individual security, and show that such a security level is achievable at the full capacity of the network, that is, the cut-set bound is the matching converse, similar to *non-secure* MSM. Moreover, we show that the field size is similar to non-secure MSM and does not have to be larger due to the security constraint.

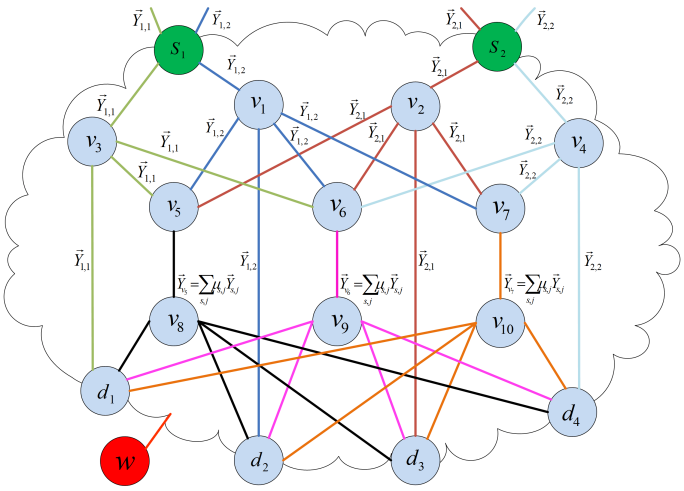

Figure 1: Secure multi-source multicast with LNC, for two sources s_i, with two messages each and four legitimate destination nodes d_i. The eavesdropper min-cut is at most 1. The edges in the graph point downward.

I. Introduction

Linear Network Coding (LNC) [1] and Random Linear Network Coding (RLNC) [2] are essential for efficient utilization of network resources. With network coding, *multiple sources* can multicast information to all destinations simultaneously, at rates up to the min-cut between the sources and the destinations. Figure 1 depicts a simple example: the min-cut from any source to any destination is 2, and from both sources to any destination is 4, hence one can disseminate *2 messages from each source to all destinations*. However, in many practical multicast applications, it is important to ensure privacy is not compromised if an eavesdropper (Eve) is present in the network. Indeed, the theory of secure network coding is vast. We include here only the most relevant works.

When the sources are co-located at a single node, several secure network coding solutions were suggested [3]–[8]. Such solutions guarantee the mutual information between Eve's data, $\mathbf{Z}$, and all the messages is 0. For example, returning to Figure 1, if only source s_1 had messages to send, and Eve would be able to wiretap one link in the network, then secure network coding would guarantee secure dissemination of one message from the source to all destinations. This is a reduction in rate compared to the full capacity, as the min-cut from s_1 to any destination is 2. However, when requiring zero mutual information with all messages from the source, this rate reduction is essential, and matches the converse result.

When the network includes multiple sources which are not co-located, the problem is more involved. Clearly, applying a single-source, secure network coding solution at each source would give an achievable scheme. In the example, if Eve wiretaps one link, one can clearly multicast one message *from each source, to all destinations*. This solution, however, may be wasteful, as it is half of the full capacity of the network, "wasting" one message *per source*, although Eve may capture only a single link regardless of the number of sources. Indeed, there is no matching converse result for the above solution.

In [9], [10], the authors gave a necessary and sufficient condition for Secure Multi-Source Multicast (SMSM). However, it is a condition on *ranks of matrices* having the global encoding vectors as columns, and, unlike non-secure MSM or secure single-source multicast, it does not translate directly to *rate or min-cut constraints*. Thus, the problem of determining the rate region in SMSM is an open problem in general [11], and as mentioned in [12, Section VI], seeking models for which it is solvable is important. In [13], the authors characterized the network coding capacity of several models, including SMSM, via the entropic region Γ^*. Yet, to date, this region is not fully characterized.

Main Contribution

In this paper, we consider SMSM under an *Individual Security* constraint. In this model, the eavesdropper is kept ignorant, in the sense of having zero mutual information, regarding each

A.Cohen, A,Cohen and O. Gurewitz are with the Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel (e-mail: alejandr@post.bgu.ac.il; coasaf@post.bgu.ac.il; gurewitz@post.bgu.ac.il). M.Médard is with the Laboratory for Information and Decision Systems at the Massachusetts Institute of Technology (medard@mit.edu). This research was partially supported by the Israeli MOITAL NEPTUN consortium and by the European Union Horizon 2020 Research and Innovation Programme SUPERFLUIDITY under Grant 671566. Parts of this work appeared at the IEEE International Symposium on Information Theory (ISIT), 2017.

message separately (or, more generally, regarding sub sets of messages), yet may potentially obtain *insignificant* information about mixtures of packets transmitted. Such a security model was recently used in various canonical problems, e.g., wiretap channels [14], more general broadcast channels [15]–[18] and multiple-access channels [19], [20], and, although not specifically mentioned as such, is also related to weakly secure network coding [21] and the notion of *algebraic security* [22], [23], which consider the information in linear combinations of messages. Moreover, a related single-source problem is that of distributed storage [24]–[26], which we also address.

We completely characterize the rate region for individually secure MSM. Specifically, we show that secure communication is achievable up to the min-cut, that is, without any decrease in the rate or any message "blow-up" by extra randomness. In fact, due to the individual security constraint, messages protect one another, and in the context of Figure 1, one is able to send *two messages from each source securely, although Eve may observe any single link*. In that sense, we non-trivially extend the single-source multicast results of [21] and [27] to multi-source multicast, giving both linear codes as well as non-linear codes over a small field size.

We then turn to a few applications where the suggested coding scheme can be useful. Specifically, we consider data centers, wireless networks and live broadcasting of video using multi-path streaming, and show how the individual security coding schemes suggested in this paper are applicable, achieving the full capacity of those systems. Finally, we show that the coding scheme is applicable to algebraic gossip as well [28], resulting in *secure gossip* without extra rounds. For example, consider the "Random Phone Call" model. This model was introduced in [29] as special case of uniform gossip. In each round of communication, every participant may "call" a random participant, and send one unit of information. The goal is, naturally, to disseminate messages from the source to *all* participants. Rigorously, the underlying graph is complete and unweighted. A detailed analysis of this model is given in [30], [31]. It was shown that in a random phone call model with v nodes, the flooding time is $\Theta(\log v)$, with constant throughput. Of course, this is without any secrecy constraint. Any phone call which Eve listens to contains relevant information, and results in leakage. Using the code suggested in this paper, we will show that one can design a secure gossip scheme, which makes sure that as long as Eve does not listen to too many calls, she remains complectly ignorant regarding any specific message, and all this without any loss in throughput or number of rounds.

The structure of this paper is as follows. In Section II, a SMSM model is formally described. Section III includes our main results, with the individually-SMSM achievability proved in Section IV and converse proved in Section V. Section VI includes a linear code construction for the individually-SMSM model. Section VII describes a Strongly-SMSM algorithm and proves a direct result for it. In Section VIII, we show a few important examples, for which the individual security coding is applicable. Section IX concludes the paper.

II. Model and Problem Formulation

SMSM is specified by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ and $\mathcal{E}$ are the node set and the edge set, respectively. We assume noise-free links of unit capacity. This capacity can be thought of as one "packet" of c bits, plus some negligible overhead.[1]

The node set $\mathcal{V}$ contains a subset of source nodes $\mathcal{S} = \{S_1, \dots S_{|S|}\}$ and a subset of legitimate destination nodes $\mathcal{D} = \{D_1, \dots D_{|D|}\}$. Each of the sources has its own set of k independent and uniformly distributed messages of length c each, over the binary field. We denote them by a messages matrix

$$\mathbf{M}_s = [\vec{M}_{s,1}; \vec{M}_{s,2}; \dots; \vec{M}_{s,k}] \in \{0,1\}^{k \times c},$$

where each row corresponds to a separate message $\vec{M}_{s,j}$, $j \in \{1, \dots, k\}$. Note that both the independence of the messages, as well as their uniform distribution are critical to achieve secrecy. These assumption are, indeed, common in the related literature as well [12], [20], [27].

We assume an eavesdropper which can obtain a subset of w packets traversing the network. Specifically, we define the eavesdropper matrix as

$$\mathbf{Z}_w = [Z_1^c; Z_2^c; \dots; Z_w^c] \in \{0,1\}^{w \times c}.$$

We denote the values of min-cuts in the network by $\rho(.;.)$. For example, for $s_1 \in \mathcal{S}$ and $d_1 \in \mathcal{D}$, $\rho(s_1; d_1)$ represents the value of the min-cut from source node s_1 to legitimate node d_1. $\rho(s_1; z)$ represents the value of the min-cut from source node s_1 to the eavesdropper (assuming z is a virtual node with infinite capacity from the w edges observed by Eve) and $\rho(\mathcal{S}; d_1)$ represents the value of the min-cut from all the source nodes to legitimate node d_1.

The goal is to design secure multi-source multicast coding scheme where legitimate nodes send their available messages in order to disseminate all the messages to all the legitimate destination nodes, yet, observing w packets from the communication between legitimate nodes, the eavesdropper is ignorant regarding the messages.

Definition 1. An MSM algorithm with parameters k and w is *Reliable* and *Individually* or *Strongly* secure if:
(1) Reliable: At the legitimate destination node $d \in \mathcal{D}$, letting $\mathbf{Y}_d$ denote the message matrix obtained, for any set of messages $\mathbf{M}_s, s \in \mathcal{S}$, we have

$$P(\hat{\mathbf{M}}_s(\mathbf{Y}_d) \neq \mathbf{M}_s) \leq \epsilon,$$

where $\hat{\mathbf{M}}_s(\mathbf{Y}_d)$ is the estimation of messages $\mathbf{M}_s$ at d.
(2) Individually secure: At the eavesdropper, observing w packets, we have

$$H(M_{s,j}|\mathbf{Z}_w) = H(M_{s,j}),$$

for all $j \in \{1, \dots, k\}$ and for all $s \in \mathcal{S}$.
(3) Strongly secure: At the eavesdropper, observing w packets, for all $s \in \mathcal{S}$ we have

$$H(\mathbf{M}_s|\mathbf{Z}_w) = H(\mathbf{M}_s).$$

[1] As in most LNC solutions, a header is required for each message. Thus, we assume messages of length c, large enough to make the overhead in the header negligible.

Remark 1. The individual-secrecy constraint given in Definition 1.2 does not promise perfect, strong-secrecy [5], [8], [9], which is, having the mutual information with all messages negligible. Individual-secrecy ensures secrecy only on each message $M_{s,j}$ separately. The eavesdropper, observing $\mathbf{Z}_w$, may obtain some information on the combination of k messages since the messages are not independent given $\mathbf{Z}_w$. However, since the k original messages are mutually independent, the leaked information has no meaning [14]–[20], [32]. In other words, if the messages are independent, we have

$$\begin{aligned} I(M_{s,k};\mathbf{Z}_w|M_{s,1},\ldots,M_{s,k-1}) &= H(M_{s,k}|M_{s,1},\ldots,M_{s,k-1}) \\ &\quad - H(M_{s,k}|\mathbf{Z}_w,M_{s,1},\ldots,M_{s,k-1}) \\ &= H(M_{s,k}) - H(M_{s,k}|\mathbf{Z}_w,M_{s,1},\ldots,M_{s,k-1}) \\ &\geq H(M_{s,k}) - H(M_{s,k}|\mathbf{Z}_w) \\ &= I(M_{s,k};\mathbf{Z}_w). \end{aligned}$$

Hence,

$$\begin{aligned} I(\mathbf{M}_s;\mathbf{Z}_w) &= \sum_k I(M_{s,k};\mathbf{Z}_w|M_{s,1},\ldots,M_{s,k-1}) \\ &\geq \sum_k I(M_{s,k};\mathbf{Z}_w). \end{aligned}$$

We require that the r.h.s will be small, however, this does not guarantee that the l.h.s is small. If the eavesdropper receives message $M_{s,j}$ by any other manner than the Individual-SMSM transmissions, Eve may obtain some information on other messages $M_{s,i}, i \neq j$, from $M_{s,j}$ and $\mathbf{Z}_w$. If it is required to prevent the possibility of such an attack, one can get perfect secrecy using Definition 1.3, yet at the price of a lower rate, as given in Section VII.

Remark 2. For multicast problems and LNC, the condition in (1) can be used with $\epsilon = 0$ [1], [2]. Yet, we allow a small error to cope with protocols such as randomized gossip [28], [33], which we discuss later in this paper.

Remark 3. The first code construction we consider, given in Section IV, is based on random coding. Therefore, in that case, the individual secrecy constraint will hold only asymptotically, that is,

$$H(M_{s,j}|\mathbf{Z}_w)/H(M_{s,j}) \to 1$$

as k grows. Then, in Section VI, we suggest a structured linear code, which results in zero mutual information, such that there is no requirement for k to grow.

A. Source and Network Coding

We assume a source $s \in \mathcal{S}$ may use an encoder,

$$f : \mathcal{M}_s \to \mathcal{X}_s \in \{0,1\}^{n\times c},$$

which maps each message matrix $\mathbf{M}_s$ to a matrix $\mathbf{X}_s$ of codewords. When using a strong security constraints, e.g., [5], [8], $n > k$ and this represents a message "blow-up" using a random key, used to confuse Eve. However, the main contribution herein, is that *under individual-secrecy, $n = k$ suffices, and there will be no rate loss due to the secrecy constraint*.

Then, the source packets $\vec{Y}$ transmitted are linear combinations of $\{\vec{X}_r\}_{r=1}^n$ with coefficients in the usual LNC sense, i.e.,

$$\vec{Y} = \sum_{r=1}^{n} \mu_r \vec{X}_r.$$

Each node maintains a subspace Y_v that is the span of all packets known to it. In RLNC, when node v sends a packet, $Out(\vec{Y})$, it chooses uniformly a packet from Y_v by taking a random linear combination. If a deterministic algorithm is used, e.g., [34], the coefficients are calculated based on the network topology. The code we suggest herein is only at the sources, and then utilizes any capacity-achieving, non-secure network code.

B. Gossip in Oblivious Networks

While the results in this paper are tailored to LNC in the sense of [1], [2], they easily apply to *algebraic gossip* [28] as well. Such algebraic gossip protocol have been considered in the literature for many tasks, such as ensuring database consistency, computing aggregate information and other functions of the data [29], [35]–[37]. We briefly describe this model. The network operates in rounds. In each round t, the sources, as well as any legitimate node which has messages it previously received, pick a random node to exchange information with. The information exchange is done by either sending (PUSH) or receiving (PULL) a message. In algebraic gossip, the message sent by a node v is simply a random linear combination of the vectors which form a basis for Y_v. The process stops when all the legitimate nodes have all the messages, i.e., have a full rank matrix. We briefly review the definitions and results from [33] for non-secure gossip networks, which we will use to formulate our result in this context.

Definition 2. A network is *oblivious* if the topology of the network, G_t at time t, only depends on t, $G_{t'}$ for any $t' < t$ and some randomness. We call an oblivious network model furthermore i.i.d., if the topology G_t is independent of t and prior topologies.

The importance of Definition 2 lies in the fact that the topology of an oblivious network may change in time, but only based on the past topology and some external randomness. Topology does not change based on the data traversing the network. Consider a single (uncoded) message, and the set of nodes S_l which received that message after l rounds. S_l advances like a flooding process F. That is, $S_l \subseteq S_{l'} \subseteq \mathcal{V}$ for $l \leq l'$, with an absorbing state $\mathcal{V}$. We say that F stops at time t if the message is received at all nodes after t rounds. Let S_F be the random variable denoting the stopping time of F.

Definition 3. We say an oblivious network with a vertex set V floods in time T with throughput α if there exists a prime power q such that for every vertex $v \in V$ and every $k > 0$ we have

$$P[S_F \geq T + k] < q^{-\alpha k}.$$

III. Main Results

The three main results in this paper completely characterize the rate region for individually secure multi-source multicast. We give tight achievability and converse, and a tight characterization of the number of rounds required under a gossip model. Specifically, we first note that the individually secrecy constrain in Definition 1 is $I(M_{s,j};\mathbf{Z}_w) = 0$ for any single message j. However, ensuring the mapping from $\mathbf{M}_s$ to $\mathbf{X}_s$ mixes the messages appropriately, i.e., satisfies rank constraints similar to [12, Lemma 3.1], can, in fact, ensure Eve is kept ignorant on any *set of* $k-(w+k\epsilon)$ *messages*, where $k\epsilon \geq 1$ is an integer and $\epsilon = o(k)$. That is, guarantee k_s-individual perfect secrecy with respect to any set of $k_s \leq k-(w+k\epsilon)$ messages. Let $\mathbf{M}_s^{k_s}$ denote a set of k_s messages from s. Thus, the first main result is the following achievability theorem, which states that k_s-individually-secure multi-source multicast is achievable at rates up to the network min-cuts, using LNC.

A. Individually Secure MSM

Theorem 1. *Assume an SMSM network $(\mathcal{V},\mathcal{E},\mathcal{S},\mathcal{D},w)$. There exists a coding scheme which disseminates k messages from each source in $\mathcal{S}$, to all destinations in $\mathcal{D}$, while keeping an eavesdropper which observes $w<k$ links ignorant with respect to any set of $k_s \leq k-(w+k\epsilon)$ messages individually, where $\epsilon = o(k)$, such that $I(\boldsymbol{M}_s^{k_s};\mathbf{Z}_w)=0$, if:*

1) *For all $s\in\mathcal{S}$ and all $d\in\mathcal{D}$, $\rho(s,d)\geq k$.*
2) *For all $d\in\mathcal{D}$, $\rho(\mathcal{S},d)\geq k|S|$.*

In Section IV-B, we prove the k_s-individual perfect secrecy constraint is indeed met. In particular, for any single message j as given in Definition 1, we have

Corollary 1. *Assume an SMSM network $(\mathcal{V},\mathcal{E},\mathcal{S},\mathcal{D},w)$. There exists a coding scheme which disseminates k messages from each source in $\mathcal{S}$, to all destinations in $\mathcal{D}$, while keeping an eavesdropper which observes $w<k$ links ignorant with respect to each message individually if:*

1) *For all $s\in\mathcal{S}$ and all $d\in\mathcal{D}$, $\rho(s,d)\geq k$.*
2) *For all $d\in\mathcal{D}$, $\rho(\mathcal{S},d)\geq k|S|$.*

Note that under strong-secrecy, i.e., requiring Eve's mutual information *with all messages simultaneously* to be zero, the problem of MSM is still open [11], [12, Section VI]. Clearly, if Eve observes w links, a naive implementation, which increases the message rates from each source by w, can send k messages from each source where $n\geq k+w+k\epsilon$ and achieve strong secrecy if:

1) For all $s\in\mathcal{S}$ and all $d\in\mathcal{D}$, $\rho(s,d)\geq n$.
2) For all $d\in\mathcal{D}$, $\rho(S,d)\geq n|S|$.

However, such an implementation is clearly wasteful, and, to date, the optimal strategy is unknown. Obviously, the required rates under strong secrecy are higher than the min-cut bound, as even for single-source multicast one needs $\rho(s_1,d_i)\geq k+w$ [5]. Thus, the importance of Theorem 1 is that under individual secrecy, not only the rate region can be characterized, and is achievable using linear network coding, individually secure MSM *is possible up to the min-cuts in the network*.

In Section VII, we do provide a code for Strong-SMSM. It is important to note that in the code suggested, the alphabet size does not increase with the network parameters due to the strong-security constraint.

Under an individual secrecy constraint, the converse below gives a stronger result than the min-cut bound.

Theorem 2. *Assume an SMSM network $(\mathcal{V},\mathcal{E},\mathcal{S},\mathcal{D},w)$. Under individual security for $k-w$ messages, that is, requiring $I(\boldsymbol{M}_s^{k-w};\mathbf{Z}_w)=0$ for any set of $k-w$ messages, one must have*

$$H(\boldsymbol{M}_s)\leq \rho(s,d_i)-\rho(s,z)+w.$$

This result should be interpreted as follows. If Eve observes w independent links, and $\rho(s;z)=w$, then one must have $H(\mathbf{M}_s)\leq\rho(s,d_i)$, which is the cut set bound. Of course, as mentioned before, the surprising part is that this bound is tight, hence such a level of security is available without any loss in rate. Yet, Theorem 2 is slightly stronger, in the sense that if somehow Eve observes more then w links, yet one still wishes to be secure with respect to any set of $k-w$ messages, then $H(\mathbf{M}_s)$ should be *strictly* smaller than $\rho(s,d_i)$ and by the same amount. E.g., if Eve observes $w+e$ links, we have $H(\mathbf{M}_s)\leq\rho(s,d_i)-e$. This means a linear increase in Eve's power results in a linear decrease in rate.

The achievability (direct) and the leakage proof are given in Section IV using a random, non-linear code, and in Section VI using a structured linear code. We note that using the non-linear code, the field size is determined only by the network coding scheme and its multicast structure (we elaborate about it in Section III-C), and there is no increase in the field size due to the security constraint. Of coarse, it requires k to be large, but the code is over a binary field. On the down side, in the non-linear code, both the sources and the destinations must store a big codebook, which includes all the possible bins and codewords. We also note that the non-linear code is more straightforward, easy to understand and uses a simple binning scheme, which is common in information theory, yet is used here with a security twist. On the other hand, using the linear code suggested, there is no requirement for k to grow, and the encoding/decoding is done by a linear function, such that it is not required to store a big codebook. Yet, to obtain the secrecy constraint, the code requires a field size greater than or equal to q^u at the sources and destinations, where $u=c/\log_2(q)\geq k$. This leads to calculations over a large finite field, which are complex. In both cases, the sophisticated coding is only at the sources and destinations. The network code field size and the coding at intermediate nodes can remain small.

Finally, it is important to note that the constraint on how many messages Eve catches is set on the entire network, thus, Eve may catch w messages of a single source, or w messages from several sources all together. Secrecy is maintained in any case, as under individual secrecy, messages from other sources can only increase secrecy, and any network code cannot create linear combinations with other messages which reduce the secrecy level. This is another benefit of the model, and hence the network code can be any LNC, without an increase in alphabet size. In that context, the codes given in [20], [27] for single source multi-cast, if considered under this individual

secrecy setting, can also only increase secrecy when applied to multi-source multi-cast. Thus, such codes constitute an achievable scheme as well.

B. Algebraic Gossip

As mentioned earlier, the suggested code easily applies to algebraic gossip as well, since this can be viewed as linear network coding over a time-extended graph. The following result captures the number of rounds required to (individually) securely disseminate k messages from each of the $|S|$ sources to all nodes in the network.

Theorem 3. *Assume an oblivious network that floods in time T with throughput α. Then, for $|S|$ nodes in the network with k messages each, algebraic gossip spreads the $k|S|$ messages to all nodes with probability $1-\epsilon$ after*

$$T' = T + \frac{1}{\alpha}(k|S| + \log \epsilon^{-1})$$

rounds, while keeping any eavesdropper which observes at most w packets, ignorant with respect to any set of k_s messages individually.

The proof is based on applying Theorem 1 above, together with known results from the Gossip literature. The complete details are deferred to Section IV-C. Note that the result above is constant-optimal, as T is the number of rounds required for a single message, hence one cannot expect less that T' above for $k|S|$ messages. This is a perfect pipelining property [33], thus, surprisingly, one can gossip securely messages to all parties in the network, without any loss in rate and without any centralized mechanism for routing, key exchange or any other encryption mechanism, as long as the eavesdropper is interested in single messages.

C. Alphabet Size

Without secrecy constraints, Jaggi *et al*. proved that a field with size greater than or equal to the number of destinations is sufficient for multicast under LNC [34]. However, this may not hold if it is required to keep an eavesdropper ignorant. Cai *et al*. [5] devised a code which requires a field of exponential size to obtain secrecy. There, the field size must be larger than $\binom{|E|}{w}$. Feldman *et al*. [38] showed that there exist networks that require a field of size at least $\Theta(|E|^{\frac{w}{2}})$. In [8], the authors demonstrate that secure network coding can be considered as a network generalization of the wiretap channel of type II. When d is the number of destinations in the multicast connection, a field of size $\binom{2k^3d^2}{w-1+d}$ is sufficient, which is independent of $|V|$ and $|E|$ but is still exponential in other network parameters.

In the solution we suggest herein, the field size is determined only by the network coding scheme, that is, only by the requirement for *reliability*, and is not increased by the individual-security constraints. In the gossip case, for example, since $q^{-\alpha k} = 2^{-(\alpha \log q)k}$, any field size greater than or equal to 2 will suffice, and an increase in the field size has only a logarithmic effect on the throughput, meaning only a logarithmic multiplier on the number of rounds T' required.

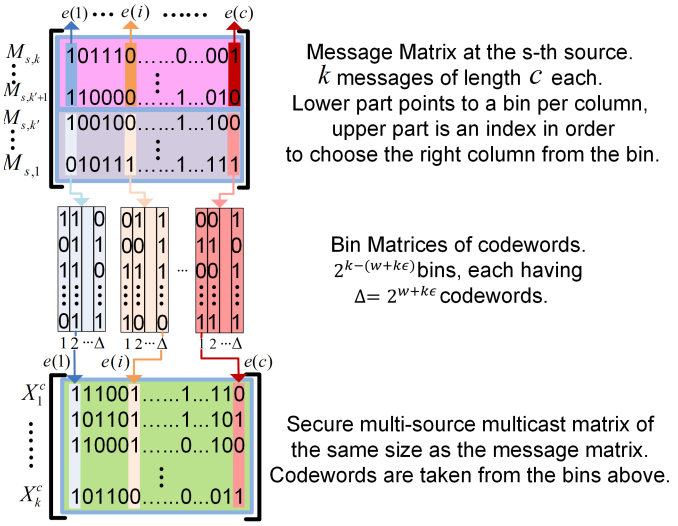

Figure 2: Binning and source encoding process for Individual-SMSM.

IV. Code Construction and a Proof for Individual-SMSM (Theorem 1 and Theorem 3)

At each source node $s \in \{1, \ldots, |S|\}$, we map each column of the message matrix $\mathbf{M}_s$ to a column of the same length. Specifically, as depicted in Figure 2, in the code construction phase, for each possible value for the partial column $M_{s,1}(i); \ldots; M_{s,k'}(i), 1 \leq i \leq c$, of length $k' = k - (w + k\epsilon)$ in the message matrix, we generate a bin, containing several columns of length k. At this point, we only mention that ϵ is such that $k\epsilon$ is an integer, as it represents a number of bits. At the end of the leakage proof, we discuss how small ϵ has to be exactly and how it affects the mutual information. The number of columns in a bin *corresponds* to w, the number of packets that the eavesdropper can wiretap, in a relation that will be made formal in the sequel. Then, to map the i-th column of the s-th message matrix, we select a column from the bin corresponding to $M_{s,1}(i); \ldots; M_{s,k'}(i)$. The specific column within that bin is chosen according to $M_{s,k'+1}(i); \ldots; M_{s,k}(i)$. That is, the lower part of the original column points to the bin, and the upper part of the original column serves as an *index* in order to choose the right column from the bin. This way, a new, $k \times c$ message matrix $\mathbf{X}_s$ is created. This message matrix contains k new messages of the same size c. We may now turn to the detailed construction and analysis.

1) Codebook Generation: Set $\Delta = 2^{w+k\epsilon}$. Let $P(x) \sim Bernoulli(1/2)$. Using a distribution $P(X^k) = \prod_{j=1}^{k} P(x_j)$, for each possible column $M_1(i); \ldots; M_{k'}(i)$ in the message matrix, that is, $2^{k-(w+k\epsilon)}$ possibilities, generate Δ independent and identically distributed codewords $x^k(e), 1 \leq e \leq \Delta$. Thus, we have $2^{k-(w+k\epsilon)}$ bins, each of size $2^{w+k\epsilon}$. Note that the length of the columns in the bins is k, thus the codebook matrix is of the same size as $\mathbf{M}_s$. The codebook is depicted in Figure 2.

2) Source and legitimate Node encodings: At the s-th source node, the encoder selects, for each column i of

bits $M_{s,1}(i);\ldots;M_{s,k'}(i)$, one codeword, $x^k(e(i))$, from the bin indexed by $M_{s,1}(i);\ldots;M_{s,k'}(i)$, where $e(i) = M_{s,k'+1}(i);\ldots;M_{s,k}(i)$. That is, $k' = k-(w+k\epsilon)$ bits of the column choose the bin, and the remaining $w+k\epsilon$ bits choose the codeword within the bin.

Then, similar to many RLNC protocols, the sources transmit linear combinations of the rows, with random coefficients. Nodes transmit random linear combinations of the vectors in $\mathcal{S}_v$, which is maintained by each node according to the messages received at the node.

A. Reliability

The reliability proof using RLNC is almost a direct consequence of [2]. Clearly, the min-cut is given by Theorem 1. Hence, the legitimate nodes can easily reconstruct $\mathbf{X}_s$ for each s (simple, non-secure, multi-source multicast). Then, each destination maps $\mathbf{X}_s$ back to $\mathbf{M}_s$, as per column $1 \leq i \leq c$, the index of the bin in which the codeword $\mathbf{X}_s$(i) resides is $M_{s,1}(i);\ldots;M_{s,k'}(i)$ and the index of the codeword location in that bin is $M_{s,k'+1}(i);\ldots;M_{s,k}(i)$. It is important to note that since the codebook is generated randomly, the mapping is not exactly 1:1 and there is a possibility for a repetition of codewords. However, averaged over all messages, the error probability from such a repetition is negligible, and this scheme guarantees successful decoding with high probability. Considering the number of bins and the number of codewords in each bin as given in the codebook generation phase, the analysis on the probability of successfully decoding $\mathbf{M}_s(i)$ from $\mathbf{X}_s(i)$ is a direct consequence using standard analysis of random coding [39, Section 3.4]. Note also that such a repetition can also be circumvented using a random permutation of the columns rather than random binning, though analysis is more complicated due to the memory in the process.

An example, obtaining both reliability and individual secrecy for two sources, with two messages each and four legitimate destination nodes, where the eavesdropper min-cut is at most 1, is given in Figure 1. Note that secure communication with respect to *one message* is possible while sending two messages from each source to all destinations.

Remark 4. The proposed binning scheme has many similarities with the random binning scheme introduced by Wyner's seminal work on degraded wiretap channel, which relies on information theoretic principles to obtain Physical Layer security [40]. Since its publication in 1975, Wyner's binning scheme was utilized by numerous studies, models and solutions, e.g., comprehensive surveys can be found in [39], [41]. In the conventional binning scheme, each message is associated with a bin (i.e., the number of bins equals the number of messages) which contains multiple codewords. The number of codewords per bin depends on the capacity of the eavesdropper. Accordingly, the sent codeword incorporates both the bin index and a (private) random key which is used to select the codeword from the corresponding bin (e.g., [39, Chapter 3]).

However, there are a few differences between the typical binning scheme and the scheme proposed herein, as well as the code construction phase. Most importantly, in the suggested scheme we utilize the binning scheme differently such that we exploit some of the messages to protect the other messages and vice versa. In particular, in the suggested scheme each column in the message matrix is partitioned into two; the first partition points to a specific bin (similar to the message itself in the conventional binning scheme), while the second partition points to a specific codeword (in contrast to the conventional binning scheme in which the codeword is chosen at random). Note that as a result, each message-matrix-column points to one possible codeword while in the usual scheme each message points to multiple codewords. Specifically, in order to achieve the full capacity of the network, the number of bins (the first partition) is equal to the total number of messages minus the number of packets that the eavesdropper can wiretap, and the number of codewords per bin (the second partition) equals the number of packets that the eavesdropper can wiretap. This, of course, means there is no private key, and part of the information is used as a key to protect the other part. The final transformation from messages to codewords is 1:1 rather than one to many.

Second, in the suggested scheme, prior to the message coding, we mix the message matrix such that each bit in the transmitted packet is associated with a mixture of bits in the original messages (note that this message mixing is done prior to and independently from the network combinations performed by the network coding mechanism). Specifically, instead of coding the message matrix rows (the messages themselves), we code the columns of the message matrix (auxiliary messages each of which is composed from one bit from each original message). Note that we still send rows of the resulting coded matrix which mean that each bit in each captured packet conveys a coded version of many bits each coming from a different message. Since messages protect one another in our scheme, this trick allows us to require only that the messages are independent, but bits within a message are not required to be independent.

Obviously, there are also several limitations to the suggested scheme compared to the vanilla-version of the Wiretap code. First, it is important to note that achieving full capacity of the network requires a compromise on the secrecy level. Specifically, the suggested scheme ensures "Individual Secrecy", which guarantees that the eavesdropper has zero mutual information with each message individually, rather than "conventional secrecy constraint" which requires zero leakage of information to the eavesdropper, when normalized by the message length, independently from any other message. Second, as mentioned, attaining secrecy while utilizing the message mixing technique requires that the messages be independent and uniformly distributed (a common assumption in the related literature, e.g., [12], [20], [27]). Third, we require the total number of messages to be sufficiently large (large k), as the mutual information to the eavesdropper decays as a function of the total number of messages (Section IV-B). From a secrecy perspective, however, we do not need message length to grow.

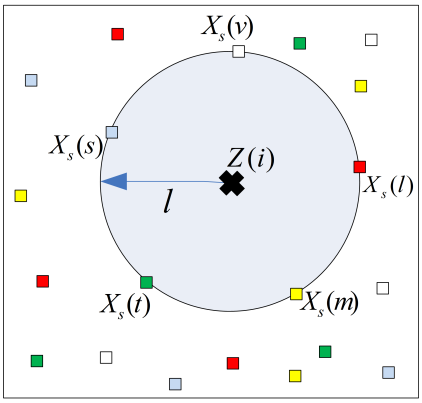

Figure 3: Codewords for Individual-SMSM algorithm lie exactly in a ball of radius $l = k - w$ around Z.

B. Information Leakage at the Eavesdropper

We now prove the k_s-individual security constraint is met, that is, $I(\mathbf{M}_s^{k_s}; \mathbf{Z}_w) \to 0$ as $k \to \infty$ for any set of $k_s \leq k-(w+k\epsilon)$ messages, where $\mathbf{Z}_w = \mathbf{W}[\mathbf{X}_1, \cdots, \mathbf{X}_{|S|}]$ and $\mathbf{W}$ is an arbitrary encoding matrix due to the network code. At the end of this subsection, we also quantify the rate at which the mutual information can decay as a function of k.

In particular, for the simplest individual secrecy constraint, we wish to show that $I(M_{s,j}; \mathbf{Z}_w)$ is small for all $s \in \mathcal{S}$ and all j. However, herein we prove a stronger result, by showing that given $\mathbf{Z}_w$, Eve's information, all possibilities for any set of $k_s \leq k-(w+k\epsilon)$ messages $\mathbf{M}_s^{k_s}$ are almost equally likely. Hence Eve has no intelligent estimation for $\mathbf{M}_s^{k_s}$ and $M_{s,j}$.

Denote by $\mathcal{C}_k$ the random codebook and by $\mathbf{X}_s$ the set of codewords corresponding to $\vec{M}_{s,1} \dots \vec{M}_{s,k}$. To analyze the information leakage at the eavesdropper, note that Eve has access to at most w linear combinations on the rows of $\mathbf{X}_s$.

Next, note that the columns of $\mathbf{X}_s$ are independent (by the construction of the codebook, creating $\mathbf{X}_s$ is done independently per-column; c columns are used only to reduce the NC overhead). Hence, it suffices to consider the information leakage for each column $i \in \{1, \dots, c\}$ from $\mathbf{X}_s$ separately, denoted by $\mathbf{X}_s$(i).

For each column i of $\mathbf{M}_s$, the encoder has $2^{k'}$ bins, with Δ independent and identically distributed codewords in each, out of which one is selected. Hence, there is an exponential number of codewords, from the eavesdropper's perspective, that can generate a column in $\mathbf{X}_s$, and we require that Eve is still confused even given the w linear combinations on each column. Let $\mathbf{Z}_w(i)$ be the w linear combinations Eve has on column i.

Hence, when the number of codewords is 2^k, given the w linear combinations from each column in $\mathbf{Z}_w(i)$, the eavesdropper has at most $2^k(1/2)^w = 2^{(k-w)}$ possible codewords. Denote $l = k - w$. Similar to the technique used in [42] to prove that *myopic adversaries* are blind, we define by the shell $\mathcal{S}h(\mathbf{Z}_w(i), l)$, the set of all k-tuples consistent with $\mathbf{Z}_w(i)$. Clearly, there are 2^l tuples in $\mathcal{S}h(\mathbf{Z}_w(i), l)$. See Figure 3 for a graphical illustration. We assume Eve has the codebook, yet does not know which column from each bin is selected to be the codeword. Hence, we wish to show that given $\mathbf{Z}_w(i)$, Eve will have at least one candidate per bin. The probability for a codeword to fall in a given shell is

$$Pr(\mathbf{X}_s^k(i) \in \mathcal{C}_k \cap \mathbf{X}_s^k(i) \in \mathcal{S}h(\mathbf{Z}_w(i), l)) = \frac{\mathcal{V}ol(\mathcal{S}h(\mathbf{Z}_w(i), l))}{2^k} = \frac{2^{(k-w)}}{2^k}.$$

In each bin of $\mathcal{C}_k$, we have $\Delta = 2^{w+k\epsilon}$ codewords. Thus, the *expected* number of codewords Eve sees on a shell, *per bin* is

$$\mathbf{E}\left[|\{m(i) : X^k(i) \in \mathcal{S}h(Z(i), l)\}|\right] = \frac{2^{w+k\epsilon} * 2^{k-w}}{2^k} = 2^{k\epsilon}.$$

Hence, we can conclude that on average, and if $k\epsilon$ is not too small, for every column in $\mathbf{M}_s$ Eve has a few possibilities *in each bin*, hence cannot locate the right bin. However, it is still important to show that all bins have (asymptotically) equally likely number of candidate codewords, hence Eve cannot locate a preferred bin. In other words, we proved that the average number of candidate codewords per column is $2^{k\epsilon}$. We now wish to show that the *actual* number Eve has in each bin is concentrated around this average.

To this end, we show that now the probability that the actual number of options deviates from the average by more than ε is small. Define the event

$$\mathcal{E}_{C_1}(Z(i), l) := \{(1-\varepsilon')2^{k\epsilon} \leq |m(i) : X_s^k(i) \in \mathcal{S}h(\mathbf{Z}_w(i), l)| \leq (1+\varepsilon')2^{k\epsilon}\}.$$

By the Chernoff bound, we have

$$Pr(\mathcal{E}_{C_1}(Z(i), l)) \geq 1 - 2^{-\varepsilon' 2^{k\epsilon}}.$$

Finally, we are now able to show that the mutual information is indeed negligible. Denote by $\mathbf{1}_{\mathcal{E}_{C_1}}$ the indicator for the event where the actual number of options per column does not deviates from the average. We thus have

$$\begin{aligned}
&I(\mathbf{M}_s^{k_s}(i); \mathbf{Z}_w(i)) \\
&= H(\mathbf{M}_s^{k_s}(i)) - H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i)) \\
&\leq k_s - H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i)) \\
&\leq k_s - H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}}) \\
&= k_s - [P(\mathcal{E}_{C_1}^c) H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}} = 0) \\
&\qquad + P(\mathcal{E}_{C_1}) H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}} = 1)] \\
&\leq k_s - (1 - 2^{-\varepsilon' 2^{k\epsilon}}) H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}} = 1) \\
&\leq k_s - H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}} = 1) + 2^{-\varepsilon' 2^{k\epsilon}} k_s.
\end{aligned}$$

However, since we now condition on $\mathbf{1}_{\mathcal{E}_{C_1}} = 1$, that is, *there was no deviation from the average by more than* ε', Eve's distribution on the bins is almost uniform, and we have $H(\mathbf{M}_s^{k_s}(i)|\mathbf{Z}_w(i), \mathbf{1}_{\mathcal{E}_{C_1}} = 1) \geq k_s(1-\varepsilon')$. Thus,

$$I(\mathbf{M}_s^{k_s}(i); \mathbf{Z}_w(i)) \leq k_s(\varepsilon' + 2^{-\varepsilon' 2^{k\epsilon}}).$$

Note that we are free to choose small ε' and ϵ as long as $k\epsilon$ is an integer. E.g., taking $\varepsilon' = k^{-m}$ and ϵ such that $k\epsilon = \lceil (m+1)\log k \rceil$, for some $m \geq 2$, gives $I(\mathbf{M}_s^{k_s}(i); \mathbf{Z}_w(i)) = O(k^{-m+1})$.

C. Algebraic Gossip (Theorem 3)

Revisiting the above proof of Theorem 1, it is clear that the algorithm suggested therein is a source code, followed by any good NC scheme which can be used to disseminate the encoded packages over the network. This is actually a *universal code* [43], [44], in the sense that it can be applied to any network without requiring knowledge of, or any modifications on, the NC. Special coding is required only at the sources. Hence, using the same source code as in Theorem 1 and then disseminating the encoded messages by a gossip protocol as in [31], which uses RLNC, the reliability at the legitimate nodes is a direct consequence of [33, Theorem 1]. Moreover, the mixing that the gossip protocol does over the network is the *same as RLNC*, hence, the information leakage at the eavesdropper is as proved in Section IV-B. Thus, compared to only a reliability constraint, the number of rounds required for both reliability and individual-secrecy is exactly the same as in the original non-secure gossip protocol.

V. Converse (Theorem 2)

In this section, we derive a converse result, which shows that under individual secrecy on a group of $k-w$ messages, not only the rate is bounded by the min-cut, but, more importantly, any independent link that Eve observes above w will require to reduce the rate *at the same amount* in order to achieve both reliability and secrecy. Thus, the converse result derived herein will be specific for the "individual secrecy" constraint given in Definition 1, and its extension to any set of $k-w$ messages, and hence extend on the well known cut-set bound.

Let $\bar{\mathbf{Z}}$ denote the random variable corresponding to the links which are not available to Eve. Hence, $\mathbf{Y}_d = (\mathbf{Z}, \bar{\mathbf{Z}})$. Let $\mathbf{M}_s^{k-w}$ denote a set of $k-w$ messages, and $\mathbf{M}_s^w$ denote the remaining w. We will show that reliability, that is $H(\mathbf{M}_s|\mathbf{Y}_d) = 0$, and individual secrecy, that is, $I(\mathbf{M}_s^{k-w};\mathbf{Z}) = 0$, imply that $H(\mathbf{M}_s)$ is upper bounded by the term in Theorem 2.

$$
\begin{aligned}
&H(\mathbf{M}_s)\\
&= H(\mathbf{M}_s^{k-w}|\mathbf{M}_s^w) + H(\mathbf{M}_s^w)\\
&\overset{(a)}{\leq} I(\mathbf{M}_s^{k-w};\mathbf{Y}_d|\mathbf{M}_s^w) + H(\mathbf{M}_s^{k-w}|\mathbf{Y}_d) + w\\
&\overset{(b)}{=} I(\mathbf{M}_s^{k-w};\mathbf{Z},\bar{\mathbf{Z}}|\mathbf{M}_s^w) + w\\
&= I(\mathbf{M}_s^{k-w};\mathbf{Z}|\mathbf{M}_s^w) + I(\mathbf{M}_s^{k-w};\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) + w\\
&= I(\mathbf{M}_s^{k-w};\mathbf{Z}) + I(\mathbf{M}_s^w;\mathbf{Z}|\mathbf{M}_s^{k-w}) - I(\mathbf{Z};\mathbf{M}_s^w)\\
&\qquad + I(\mathbf{M}_s^{k-w};\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) + w\\
&\overset{(c)}{=} I(\mathbf{M}_s^w;\mathbf{Z}|\mathbf{M}_s^{k-w}) - I(\mathbf{Z};\mathbf{M}_s^w) + I(\mathbf{M}_s^{k-w};\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) + w\\
&= I(\mathbf{M}_s^w;\mathbf{Z}|\mathbf{M}_s^{k-w}) - I(\mathbf{Z};\mathbf{M}_s^w)\\
&\qquad + H(\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) - H(\bar{\mathbf{Z}}|\mathbf{M}_s^{k-w},\mathbf{Z},\mathbf{M}_s^w) + w\\
&= I(\mathbf{M}_s^w;\mathbf{Z}|\mathbf{M}_s^{k-w}) - I(\mathbf{Z};\mathbf{M}_s^w) + H(\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) + w\\
&= H(\mathbf{M}_s^w|\mathbf{M}_s^{k-w}) - H(\mathbf{M}_s^w|\mathbf{Z},\mathbf{M}_s^{k-w}) - H(\mathbf{M}_s^w)\\
&\qquad + H(\mathbf{M}_s^w|\mathbf{Z}) + H(\bar{\mathbf{Z}}|\mathbf{Z},\mathbf{M}_s^w) + H(\bar{\mathbf{Z}}) - H(\bar{\mathbf{Z}}) + w\\
&= I(\mathbf{M}_s^w;\mathbf{M}_s^{k-w}|\mathbf{Z}) - I(\bar{\mathbf{Z}};\mathbf{Z},\mathbf{M}_s^w) + H(\bar{\mathbf{Z}}) + w\\
&= I(\mathbf{M}_s^w;\mathbf{M}_s^{k-w}|\mathbf{Z}) - I(\bar{\mathbf{Z}};\mathbf{M}_s^w|\mathbf{Z}) - I(\bar{\mathbf{Z}};\mathbf{Z}) + H(\bar{\mathbf{Z}}) + w\\
&\leq I(\mathbf{M}_s^w;\mathbf{M}_s^{k-w}|\mathbf{Z}) - I(\bar{\mathbf{Z}};\mathbf{M}_s^w|\mathbf{Z}) + H(\bar{\mathbf{Z}}) + w\\
&= H(\mathbf{M}_s^w|\mathbf{Z}) - H(\mathbf{M}_s^w|\mathbf{Z},\mathbf{M}_s^{k-w}) - H(\mathbf{M}_s^w|\mathbf{Z})\\
&\qquad + H(\mathbf{M}_s^w|\mathbf{Z},\bar{\mathbf{Z}}) + H(\bar{\mathbf{Z}}) + w\\
&\overset{(d)}{\leq} H(\bar{\mathbf{Z}}) + w\\
&\overset{(e)}{\leq} \rho(s_i;d_i) - \rho(s_i;z) + w,
\end{aligned}
$$

where (a) is since conditioning reduces entropy. Note that this inequality is tight if the messages are independent. (b) is due to the reliability constraint, that is, $H(\mathbf{M}_s^{k-w}|\mathbf{Y}_d) = 0$ since all messages, and $\mathbf{M}_s^{k-w}$ specifically, are decodable at the destination using $\mathbf{Y}_d = (\mathbf{Z}, \bar{\mathbf{Z}})$. (c) follows since we assume that Eve is kept ignorant regarding any group of $w-k$ messages, hence $I(\mathbf{M}_s^{k-w};\mathbf{Z}) = 0$. That is, it uses the security constraint. (d) is since $H(\mathbf{M}_s^w|\mathbf{Z},\bar{\mathbf{Z}}) = 0$. However, since the converse turns out to be tight, and it turns out that removing the positive term $H(\mathbf{M}_s^w|\mathbf{Z},\mathbf{M}_s^{k-w})$ does not change much, we conclude that $H(\mathbf{M}_s^w|\mathbf{Z},\mathbf{M}_s^{k-w})$ is negligible, meaning, *given the messages Eve is interested in*, and her captured links, she is actually able to decode the rest of the messages/randomness as well. This is a returning theme in such wiretap-like coding schemes. (e) follows since $\rho(s_i;d_i) - \rho(s_i;z)$ is the maximum amount that may not be available to Eve, if she has a min-cut $\rho(s_i;z)$. Again, we assume unit capacity links and normalize the information in a message to "1" accordingly.

VI. Linear Code Construction for Individual-SMSM

The code given in Section IV relies on random coding, for which the individual secrecy constraint holds only asymptotically, that is, $H(M_{s,j}|\mathbf{Z}_w)/H(M_{s,j}) \to 1$ as k grows. In this section, we provide a structured linear code, which results in zero mutual information, not constrained by the number of messages (i.e., no requirement for k to grow), without any decrease in the rate or any message "blow-up" by extra randomness. Yet, the code requires a field size greater than or equal to q^u at the sources and destinations, where $u = c/\log_2(q) \geq k$. Note that this means we regard packets as symbols over a finite field F_{q^u}, where $F_q^{1\times u} \cong F_{q^u}$. Hence, the code is compatible with the network code given in Section IV since F_{q^u} is a vector space over F_q. Furthermore, note that the increased alphabet size is only at the sources and destinations. The network code at intermediate nodes can remain small. The structured linear code provided in this section adopts the linear code given in [21], [27] for single-source multicast to multi-source multicast. Even though most of the results and proofs in this subsection follow the techniques given in [43], for completeness we provide the adapted proofs herein, adopting the scope, terminology and notations to the multi-source multicast problem considered in this study. Note, however, that in the information leakage proof, Eve's observation $\mathbf{Z}_w$ may include a linear combination of packets from several sources, rather than only one source as in [27], hance maybe confusing Eve even further. We do not exploit this confusion here, and the proof holds even for

the case where Eve may see w packets unmixed with other sources, yet it creates a difference compared to single-source multicast. Moreover, if one could *guarantee* Eve's observation include mixtures of packets from several sources, the field size of the code may have been decreased. The current literature includes several examples analyzing the security achieved compared to the level of mixing in the network [22].

Corollary 2. *With a (k, w) linear code over a field F_{q^u}, k_s-*individual security *holds in SMSM networks over a field F_q, keeping an eavesdropper which observes $w \geq \rho(s; z)$ links ignorant with respect to any set of $k_s \leq k - w$ messages, if $u \geq k$, form each source $s \in \mathcal{S}$ to each destination $d \in \mathcal{D}$, $\rho(s, d) \geq k$, for all $d \in \mathcal{D}$, $\rho(S, d) \geq (k)|S|$ and k satisfies*

$$k \geq \left\lceil \frac{\rho(s,d)}{\rho(s,d) - \rho(s;z)} \right\rceil \geq 2.$$

We may now turn to the detailed construction and proof of the Individual-SMSM structured linear code.

1) Codebook Generation: Let $\mathcal{C}$ be a linear code over F_{q^u} of length k and dimension w, and set $k' = k - w$. Then, let

$$\mathbf{H} = [\vec{H}_1; \vec{H}_2; \ldots; \vec{H}_{k'}] \in F_{q^u}^{k' \times k}$$

be a parity check matrix for the code. This linear code defines $q^{u(k-w)}$ cosets, one of them is the code itself. We denote the cosets by $\{A_m\}$, $1 \leq m \leq q^{u(k-w)}$. Note that each coset is of size q^{uw}. Hence, the cosets of this code correspond to the bins we used in Section IV, yet over a field F_{q^u}, such that there are many more cosets, and each is larger.

Let $\mathbf{G}$ be a generator matrix for $\mathcal{C}$. We thus denote

$$\mathbf{G} = [\vec{G}_1; \vec{G}_2; \ldots; \vec{G}_w] \in F_{q^u}^{w \times k},$$

and we select a matrix

$$\mathbf{G}^\star = [\vec{G}_1^\star; \vec{G}_2^\star; \ldots; \vec{G}_{k'}^\star] \in F_{q^u}^{k' \times k},$$

with k' linearly independent rows from $F_{q^u}^k \setminus \mathcal{C}$. That is, $\mathbf{G}^\star$ spans the null space of $\mathcal{C}$.

The linear code we consider herein is from the class of linear Maximum Rank Distance (MRD) codes [45], [46]. The norm of a vector $\mathbf{X}_s \in F_{q^u}^k$ is defined as the column rank of $\mathbf{X}_s$ over F_q, denoted by $rank_{F_q}(\mathbf{X}_s)$. The *rank distance* of two vectors over $F_{q^u}^k$ is defined as

$$d_R(\mathbf{X}_s(1), \mathbf{X}_s(2)) \triangleq rank_{F_q}(\mathbf{X}_s(1) - \mathbf{X}_s(2)).$$

The *minimum rank distance* of a code $\mathcal{C} \subseteq F_{q^u}^k$ is defined as the minimum distance of all pairs of distinct codewords in $\mathcal{C}$. Rank metric codes adhere to a Singleton bound, that is, the size of a code is bounded by $|\mathcal{C}| \leq q^{\max\{k,u\}(\min\{k,u\}-d+1)}$. For linear codes this becomes $d \leq \min\{1, u/k\}(k-k')+1$. We use the requirements in [27, Theorem 7], that is, for $u \geq k$, we use a code over F_{q^u}, defined by a parity check matrix $\mathbf{H} \in F_{q^u}^{k' \times k}$, which is MRD and the matrix **PHT** is nonsingular for all full rank $\mathbf{P} \in F_q^{k' \times k'}$ and all full rank $\mathbf{T} \in F_q^{k \times k'}$.

2) Source and legitimate nodes encodings: At each source node, s, the encoder selects a codeword $x^k(e)$ out of the q^{uw} members of the coset A_m, where m is given by the index $M_{s,1}; \ldots; M_{s,k'}$ and $e = M_{s,k'+1}; \ldots; M_{s,k}$ over a field $F_{q^u}^k$. That is, similar to Section IV, $k' = k - w$ symbols choose the coset, and the remaining w symbols choose the codeword within the coset. This is equivalent to letting $\mathbf{X}_s$ be a choice from the q^{uw} solutions of

$$(M_{s,1}; \ldots; M_{s,k'}) = \mathbf{H}\mathbf{X}_s. \tag{1}$$

Again, note that $\mathbf{X}_s$ is of the same size as $\mathbf{M}_s$. Proposition 1 below shows that, in fact, $\mathbf{X}_s$ can be easily computed using matrix multiplication.

Proposition 1. *At each source node, s, the encoding operation for the symbols $M_{s,1}; \ldots; M_{s,k} \triangleq \boldsymbol{M}_s$, is given by*

$$\begin{aligned} \boldsymbol{X}_s^T &= M_{s,1}\vec{G}_1^\star + \ldots + M_{s,k'}\vec{G}_{k'}^\star \\ &\quad + M_{s,k'+1}\vec{G}_1 + \ldots + M_{s,k}\vec{G}_w \\ &= \boldsymbol{M}_s^T \begin{bmatrix} \boldsymbol{G}^\star \\ \boldsymbol{G} \end{bmatrix}. \end{aligned} \tag{2}$$

Proof. Define $\mathbf{X}_s^T$ according to (2). We wish to show that this definition is indeed consistent with (1), that is, using the definition in (2) the symbols $M_{s,1}; \ldots; M_{s,k'}$ define the coset in which $\mathbf{X}_s$ resides, and, furthermore, the remaining w symbols, $M_{s,k'+1}; \ldots; M_{s,k}$, uniquely define the word within the coset.

To this end, take the transposed of equation (2), and multiply it by $\mathbf{H}$. We have:

$$\begin{aligned} \mathbf{H}\mathbf{X}_s &= \mathbf{H}M_{s,1}(\vec{G}_1^\star)^T + \ldots + \mathbf{H}M_{s,k'}(\vec{G}_{k'}^\star)^T \\ &\quad + \mathbf{H}M_{s,k'+1}(\vec{G}_1)^T + \ldots + \mathbf{H}M_{s,k}(\vec{G}_w)^T \\ &= \mathbf{M}_{s,1}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \mathbf{M}_{s,k'}\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \\ &\quad + M_{s,k'+1}\underline{0} + \ldots + M_{s,k}\underline{0} \\ &= \begin{pmatrix} \mathbf{M}_{s,1} \\ \vdots \\ \mathbf{M}_{s,k'} \end{pmatrix}, \end{aligned}$$

where the second inequality is since the row vectors $\vec{G}^\star$ are our choice of a basis to the null space of the code, hence, we can take $\mathbf{G}^\star$ such that $\mathbf{H}\mathbf{G}^{\star T} = \mathbf{I}$ [43, Section V.C]; Moreover, since $\mathbf{H}$ is a parity check matrix for the code, it is orthogonal to all codewords. Thus, the first k' rows define the coset.

Now, since the rows $M_{s,k'+1}; \ldots; M_{s,k}$ create a linear combination of *codewords*, the addition of such a linear combination does not change the coset. $\mathbf{X}_s^T$ remains in the same coset regardless of these rows. Yet, as $(\vec{G}_1; \ldots; \vec{G}_w)$ is of rank w, all q^{uw} possibilities for the linear combination are distinct, creating distinct vectors $\mathbf{X}_s^T$ within the coset. □

Then, since each symbol over F_{q^u} of the encoded codeword $X_{s,1}; \ldots; X_{s,k} \triangleq \mathbf{X}_s$ at the source is a vector over F_q of length $c = u/\log_2(q)$, the network code is still compatible with Section IV. That is, the sources transmit linear combinations

of the rows, with random coefficients. Nodes transmit random linear combinations of the messages they received.

A. Reliability

As for the reconstruction of $\mathbf{X}_s$ at the destinations, it is almost a direct consequence of [2]. Again, the min-cut is given by Theorem 1, and the legitimate nodes can easily reconstruct $\mathbf{X}_s$ for each s. Now, each destination can map $\mathbf{X}_s$ back to $\mathbf{M}_s$. First, compute the bin index according to $(M_{s,1};\ldots;M_{s,k'}) = \mathbf{H}\mathbf{X}_s$. Then, $M_{s,k'+1};\ldots;M_{s,k}$ are simply the index of $\mathbf{X}_s$ within that bin. They can be computed using $(M_{s,k'+1};\ldots;M_{s,k}) = \tilde{\mathbf{G}}\mathbf{X}_s$, where $\tilde{\mathbf{G}}$ is any basis for the code such that $\tilde{\mathbf{G}}\mathbf{G}^\star = 0$ yet $\tilde{\mathbf{G}}\mathbf{G} = I$.[2]

B. Information Leakage at the Eavesdropper

Denoted by $\mathcal{C}$ the code and by $\mathbf{X}_s$ the codeword corresponding to $\vec{M}_{s,1}\ldots\vec{M}_{s,k}$. We assume that the eavesdropper has full knowledge of the code $\mathcal{C}$. As given in Section IV-B, to analyze the information leakage at the eavesdropper, note that Eve has access to at most w linear combinations on the elements of $\mathbf{X}_s$.

Next, using techniques given in [27], [43], we calculate the eavesdropper's uncertainty. Let $\underline{\mathbf{M}}_s^{k-w} = \mathbf{P}\mathbf{M}_s^{k-w}$ for a full rank $\mathbf{P} \in F_q^{k'\times k'}$. Let $\mathbf{Z}_w = \mathbf{W}\mathbf{X}_s$, where $\mathbf{W}$ is an arbitrary encoding matrix due to network links observed by the eavesdropper. Then, we have

$$\begin{aligned} I(\underline{\mathbf{M}}_s^{k-w};\mathbf{Z}_w) &= I(\underline{\mathbf{M}}_s^{k-w},\mathbf{X}_s;\mathbf{Z}_w) - I(\mathbf{X}_s;\mathbf{Z}_w|\underline{\mathbf{M}}_s^{k-w}) \\ &\overset{(a)}{\leq} H(\mathbf{Z}_w) - H(\mathbf{X}_s|\underline{\mathbf{M}}_s^{k-w}) \\ &\qquad + H(\mathbf{X}_s|\underline{\mathbf{M}}_s^{k-w},\mathbf{Z}_w) \\ &\leq rank(\mathbf{W}) + rank(\mathbf{PH}) - rank\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix}, \end{aligned}$$

where (a) is since given the network coefficients and $\mathbf{X}_s$, $H(\mathbf{Z}_w|\underline{\mathbf{M}}_s^{k-w},\mathbf{X}_s) \geq 0$, and the last inequality follows directly from the proof of Lemma 6 in [43]. Note that the above inequality, $H(\mathbf{Z}_w|\underline{\mathbf{M}}_s^{k-w},\mathbf{X}_s) \geq 0$, is a key difference compared to single source multicast. In single source multicast, $H(\mathbf{Z}_w|\underline{\mathbf{M}}_s^{k-w},\mathbf{X}_s) = 0$, as the output at Eve's side is determined by the source input. However, in MSM this entropy might be positive, if Eve's observation includes a mixture with other sources and not only the source s.

Now, if $\langle\cdot\rangle$ denotes the row space of a matrix, we have

$$rank(\mathbf{PH}) + rank(\mathbf{W}) - rank\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix} = dim(\langle\mathbf{PH}\rangle \cap \langle\mathbf{W}\rangle).$$

Let $r = dim(\langle\mathbf{PH}\rangle\cap\langle\mathbf{W}\rangle)$. Then, there exist full rank matrices $\mathbf{R}_1 \in F_{q^u}^{r\times w}$ and $\mathbf{R}_2 \in F_{q^u}^{r\times k'}$, such that $\mathbf{R}_1\mathbf{W} = \mathbf{R}_2\mathbf{PH}$ and $rank(\mathbf{R}_2\mathbf{PH}) = r$, and we have $\mathbf{R}_1\mathbf{Z}_w = \mathbf{R}_1\mathbf{W}\mathbf{X}_s = \mathbf{R}_2\mathbf{PH}\mathbf{X}_s = \mathbf{R}_2\underline{\mathbf{M}}_s^{k-w}$. On the other hand, the mutual information is at least the linear common part, that is, $I(\underline{\mathbf{M}}_s^{k-w};\mathbf{Z}_w) \geq H(\mathbf{R}_2\underline{\mathbf{M}}_s^{k-w})$. By the uniformity of the messages and the full ranks of $\mathbf{P}$ and $\mathbf{R}_2$, $H(\mathbf{R}_2\underline{\mathbf{M}}_s^{k-w}) = r$, hence

$$I(\underline{\mathbf{M}}_s^{k-w};\mathbf{Z}_w) \geq rank(\mathbf{PH}) + rank(\mathbf{W}) - rank\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix}.$$

To conclude,

$$I(\underline{\mathbf{M}}_s^{k-w},\mathbf{Z}_w) = rank(\mathbf{PH}) + rank(\mathbf{W}) - rank\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix}.$$

Now, if $\mathcal{C}$ is an MRD code over a field of $F_{q^u}^k, u \geq k$, for any full rank $\mathbf{P} \in F_q^{k'\times k'}$ the matrix $\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix}$ is nonsingular for any full rank $\mathbf{W} \in F_q^{w\times k}$. Thus, $rank\begin{bmatrix}\mathbf{PH}\\ \mathbf{W}\end{bmatrix} = rank(\mathbf{PH}) + rank(\mathbf{W})$, and the mutual information is zero.

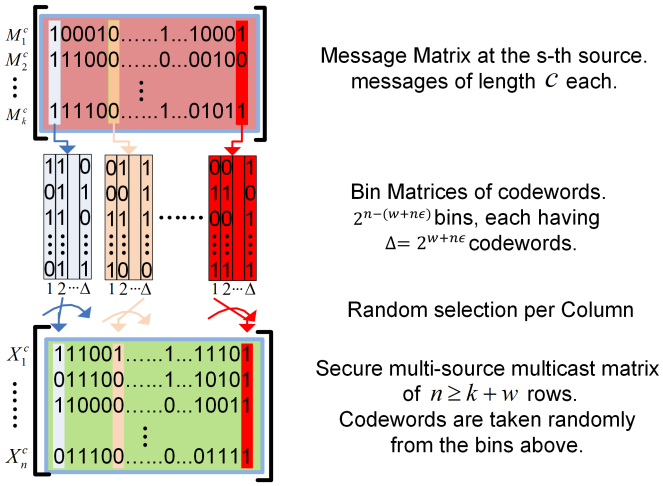

Figure 4: Binning and source encoding process for Strong-SMSM.

VII. Code Construction and a Proof for Strong-SMSM

In this section, we design a random code, which results with strong-secrecy, i.e., requiring Eve's mutual information *with all messages simultaneously* to be zero, yet, at price of rate as given in [5]. However, using the suggested random code herein, the field size is determined only by the network coding scheme, that is, only by the requirement for reliability, and is not increased by the strong-security constraints.

At each source node $s \in \{1,\ldots,|S|\}$, we *randomly* map each column of the message matrix $\mathbf{M}_s$. As depicted in Figure 4, in the code construction phase, for each *possible column* of the s-th message matrix we generate a bin, containing several columns. The number of such columns *corresponds* to w, the number of packets that the eavesdropper can wiretap, in a relation that will be made formal in the sequel. Then, to encode, for each column of the message matrix, we randomly select a column from its corresponding bin. This way, a new, $n \times c$ message matrix $\mathbf{X}_s$ is created. Specifically, a Strong-SMSM code at the s-th source node consists of a messages matrix $\mathbf{M}_s$ of $\vec{M}_{s,1}\ldots\vec{M}_{s,k}$ messages of length c bits over the binary field, we denote the set of matrices by $\mathcal{M}_s$; A discrete

[2] In the same way, using a gossip protocol, the reliability proof is almost a direct consequence of [33, Theorem 1]. Hence, the number of rounds required is given by Theorem 3.

memoryless source of randomness over the alphabet $\mathcal{R}$ and some known statistics p_R; An encoder,

$$f : \mathcal{M}_s \times \mathcal{R} \to \mathcal{X}_s \in \{0,1\}^{n\times c}$$

which maps each message matrix $\mathbf{M}_s$ to a matrix $\mathbf{X}_s$ of codewords. This message matrix contains $n \geq k + w + n\epsilon$ new messages of size c, where, here as well, $n\epsilon \geq 1$ is a small integer.

The need for a *stochastic encoder* is similar to most encoders ensuring information theoretic security, as randomness is required to confuse the eavesdropper about the actual information [39]. Hence, we define by R_k the random variable encompassing the randomness required *for the k messages at the source node*, and by Δ the number of columns in each bin. We may now turn to the detailed construction and analysis.

1) Codebook Generation: Set $\Delta = 2^{w+n\epsilon}$. Where $P(x) \sim Bernoulli(1/2)$, using a distribution $P(X^n) = \prod_{j=1}^{n} P(x_j)$, for each possible column in the message matrix generate Δ independent and identically distributed codewords $x^n(e)$, $1 \leq e \leq \Delta$.

2) Source and legitimate node encodings: For each column i of the s-th message matrix $\mathbf{M}_s$, the s-th source node selects uniformly at random one codeword $x^n(e)$ from the i-th bin. Therefore, the s-th source Strong-SMSM matrix $\mathbf{X}_s$ contains c randomly selected codewords of length n, one for each column of the s-th message matrix. Then, the sources transmit linear combinations of the rows, with random coefficients. Nodes transmit random linear combinations of the vectors in $\mathcal{S}_v$, which is maintained by each node according to the messages received at the node.

The reliability in the Strong-SMSM algorithm is inherited from the reliability in RLNC. That is, if min-cuts are $\rho(s,d) \geq k+w$ and $\rho(S,d) \geq (k+w)|S|$ for each $s \in \mathcal{S}$ and $d \in \mathcal{D}$ then $k + w = n$ messages can be transmitted reliably from each source to all destinations. Since the transformation $\mathbf{M}_s$ to $\mathbf{X}_s$ can be inverted as given in Section IV-A, the destinations can decode the original messages.

A. Information Leakage at the Eavesdropper

We now prove the strong-security constraint is met. In particular, for the strong constraint, we wish to show that $I(\mathbf{M}_s; \mathbf{Z}_w)$ is small for all $s \in \mathcal{S}$. We will do that by showing that given $\mathbf{Z}_w = \mathbf{W}[\mathbf{X}_1, \cdots, \mathbf{X}_{|S|}]$ where $\mathbf{W}$ is arbitrary encoding matrix due to network, Eve's information, all possibilities for $\mathbf{M}_s$ are equally likely, hence Eve has no intelligent estimation for $\mathbf{M}_s$.

Denote by $\mathcal{C}_n$ the random codebook and by $\mathbf{X}_s$ the set of codewords corresponding to $\vec{M}_{s,1} \dots \vec{M}_{s,k}$. To analyze the information leakage at the eavesdropper, note that Eve has access to at most w linear combinations on the rows of $\mathbf{X}_s$.

Next, note that the columns of $\mathbf{X}_s$ are independent (by the construction of the codebook, creating $\mathbf{X}_s$ is done independently per-column; c columns are used only to reduce the NC overhead). Hence, it suffices to consider the information leakage for each column $i \in \{1, \dots, c\}$ from $\mathbf{X}_s$ separately. For each column i of $\mathbf{M}_s$, the encoder has Δ independent and identically distributed codewords, out of which one is selected. Hence, there is an exponential number of codewords, from the eavesdropper's perspective, that can generate a column in $\mathbf{X}_s$, and we require that Eve is still confused even given the w linear combinations from each column. Hence, when the number of codewords is 2^n, given the w linear combinations from each column in $\mathbf{Z}_w(i)$, the eavesdropper has $2^n(1/2)^w = 2^{(n-w)}$ possible codewords. We now denote $l = n - w$ and define the shell $\mathcal{S}h(\mathbf{Z}_w(i), l)$, the set of all n-tuples consistent with $\mathbf{Z}_w(i)$. Clearly, there are 2^l tuples in $\mathcal{S}h(\mathbf{Z}_w(i), l)$.

We assume Eve has the codebook, yet does not know which column from each bin is selected to be the codeword. Hence, we wish to show that given $\mathbf{Z}_w(i)$, Eve will have at least one candidate per bin. Now,

$$Pr(\mathbf{X}_s^n(i) \in \mathcal{C}_n \cap \mathbf{X}_s^n(i) \in \mathcal{S}h(\mathbf{Z}_w(i), l)) = \frac{\mathcal{V}ol(\mathcal{S}h(\mathbf{Z}_w(i), l))}{2^n} = \frac{2^{(n-w)}}{2^n}.$$

In each bin of $\mathcal{C}_n$, we have $\Delta = 2^{w+n\epsilon}$ codewords. Thus, the *expected* number of codewords Eve sees in her shell, *per bin* is

$$\mathbf{E}\left[|\{m(i) : X^n(i) \in \mathcal{S}h(Z(i), l)\}|\right] = \frac{2^{w+n\epsilon} * 2^{n-w}}{2^n} = 2^{n\epsilon}.$$

Again, we can conclude that on average, and if $n\epsilon$ is not too small, for every column in $\mathbf{M}_s$ Eve has a few possibilities *in each bin*, hence cannot locate the right bin. We need to show that all bins have (asymptotically) equally likely number of candidate codewords. Similarly to the individual security proof, we wish to show that the probability that the actual number of options deviates from the average by more than ε is small. We define $\mathcal{E}_{C_1}(Z(i), l)$ similarly to Section IV-B and by the Chernoff bound, we have

$$Pr(\mathcal{E}_{C_1}(Z(i), l)) \geq 1 - 2^{-\varepsilon' 2^{n\epsilon}}.$$

The reminder of the leakage proof follows the exact same steps as the one in Section IV-B, yet with $\mathbf{M}_s(i)$ replacing $\mathbf{M}_s^{k_s}(i)$ and k replacing k_s.

VIII. Applications

In previous sections we suggested an SMSM code and proved that under the suggested code an eavesdropper which can capture a subset of the packet's traversing the network (up to w packets) is kept ignorant regarding each packet's content, under the *Individual Security* constraint, without compromising the rate (i.e., achieving full network capacity). In this section, we show several common applications which exemplify the applicability of the suggested code to a diverse range of protocols and applications. The first two examples include only a single source, merely to show the applicability of the *individual secrecy* setup. The third example is multi-source in nature, and includes all aspects of our solution.

A. Data Centers

One of the most prominent facilities characterizing our new "information explosion" era are distributed *Data Centers*. Such facilities, which aim to cope with the rapidly increasing

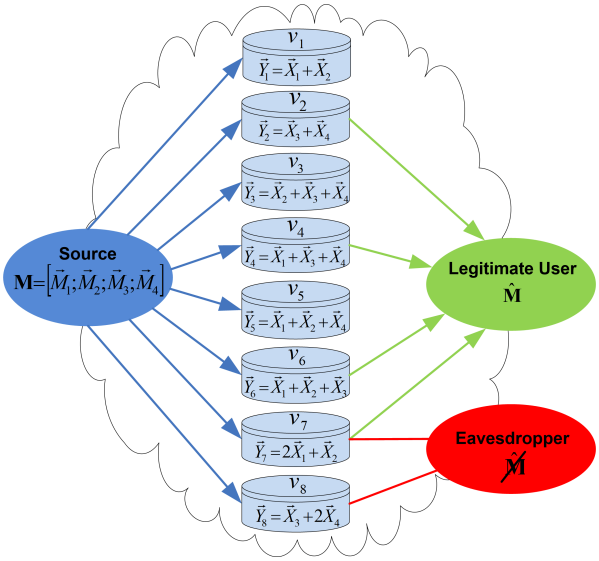

Figure 5: Individual Secure Data Center, with 8 servers. The source needs to store a file $\mathbf{M}$ with 4 messages, where any legitimate user (destination) which is connected to 4 servers should be able to decode the 4 original messages. In the individual secure coding scheme of this application, we assume the existence of an eavesdropper, which is able to obtain information from any 2 servers. We wish that this eavesdropper will not gain any information on each specific message.

volumes of data generated, archived and expected to be accessible, are vital to many services such as video sharing, social networks, peer-to-peer cloud storage and many more. Google's GFS [47], Amazon's Dynamo [48], Google's BigTable [49], Facebook's Apache Hadoop [50], Microsoft's WAS [51] and LinkedIn's Voldemort [52] are just a few examples of such ubiquitous applications. Obviously, the security and reliability of such *Data Centers* are critical for such applications to be adopted by users and organizations.

In the basic non-secure model [53], [54], a source s needs to store a file $\mathbf{M}$, which is decomposed into k messages, in v servers (nodes), such that any legitimate user d (destination) can reconstruct the file by collecting the stored information from any l servers ($l = \rho(s, d_i) \geq k$). With one source, as considered in [24]–[26], the secured version constraints the stored chunks such that an eavesdropper, which can observe the information stored at any w servers, will be kept ignorant regarding the actual file stored (see Figure 5). In these works, which consider only one source, a source code to obtain weak secrecy is considered as an outer code, with a loss of a small factor of storage secrecy capacity. Then, *Regenerating Codes* [53]–[55] are used. These are usually suggested to store data in distributed storage.

For the secured multi-source version, we can leverage the individual-SMSM coding scheme suggested herein to enhance the non-secure solution suggested in [28], [56]–[59], which consider each node in the network as a server which maintains pieces of data using RLNC. We will be able to guarantee that any eavesdropper that can access any w servers will

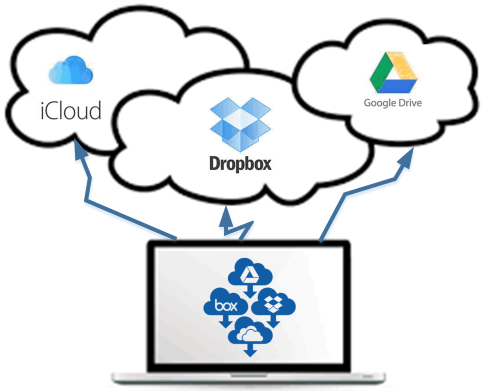

Figure 6: Individual Secure Cloud Storage, with various cloud storage providers. The source encodes the original data using the individual security coding scheme suggested and then uploads w encoded packets to different $\lceil k/w \rceil$ cloud storage providers, such that, each provider not only will not be able to decode the original data, but will also have zero information regarding any of the $k - w$ stored messages individually.

have no information regarding any stored message individually (zero mutual information regarding each message separately). Specifically, each source s encodes the original data file $\mathbf{M}$ using the individual security coding scheme suggested herein (Sections IV and VI) and then uploads the encoded packets to the v servers. The number and the size of packets uploaded to the servers in the secure solution suggested are as in the non-secure model; thus, we obtain the full capacity of the system.

It is important to note that utilizing the individual security coding scheme suggested in this paper, one not only ensures individual secrecy from potential eavesdroppers, but also can guarantee privacy from the hosting servers themselves, such that, each server not only will not be able to decode the original data but will have zero information regarding any of the stored message individually. For example, assume that in the example depicted in Figure 6, the source s (private user) wants to store a file $\mathbf{M}$ in the cloud. To do that, the source can utilize 3 different cloud storage providers, such as Google Drive, Microsoft OneDrive, Dropbox, etc. However, the source wants to keep the original information private. Hence, by encoding the original data using the individual security coding scheme suggested at the source, and then uploading at most 3 encoded packets $\vec{Y}_{i_1}, \ldots, \vec{Y}_{i_3}$ to any provider, the provider will store the packets in their servers v, but these will be kept ignorant of the original file.

B. Wireless Networks

The inherent broadcast nature of the wireless medium makes network coding techniques pertinent for wireless networks. Specifically, relying on network coding, instead of sending packets (unicast, multicast or broadcast packets) to each intended addressee individually, a source (or an intermediate node which needs to relay packets toward the destination) can transmit a manipulation (usually a linear combination) of the packets destined to the various receivers. A receiver collecting

sufficient number of such combinations (coded packets) can reconstruct (decode) the original packets. Relying on NC when

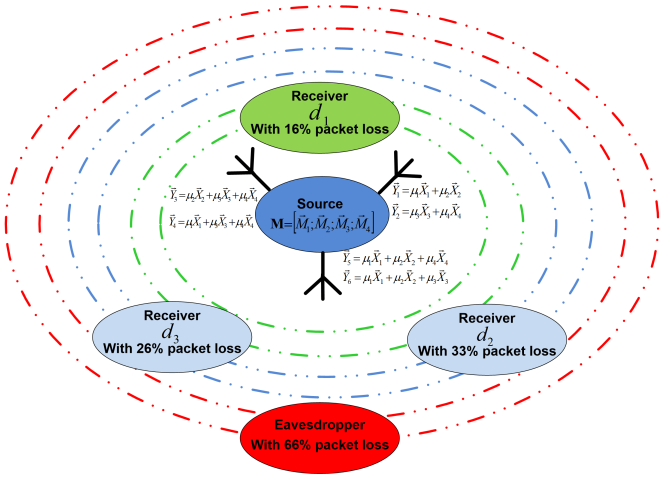

Figure 7: Individual Secure Wireless Network. The source needs to disseminate 4 message over a wireless network to 3 legitimate users. In the individual secure model, we assume the existence of an eavesdropper. However, due to interference, collisions (low SINR) or low SNR, each of the receivers has a different packet loss rate, according to the physical constraints in the wireless networks.

the channel is lossy, i.e., there is a probability that a sent packet will not be received (decoded) by its intended receiver (receivers), has great advantages as instead of resending each uncoded packet until received correctly by its intended receiver, a sender keeps sending combinations of the original packets until each receiver collects a sufficient number of combinations (e.g., [60]–[66]). Accordingly, a sender can *a priori* estimate the number of coded packets needed according to the most lossy channel and send coded packets accordingly, without relying on any feedbacks mechanism.

The secured version of this data dissemination problem requires that an eavesdropper with a degraded channel which can obtain only a subset of the transmitted packet will not be able to attain any information regarding any of the original packets. Utilizing the individual security coding scheme suggested in this paper, in which the source estimates the number of packets needed to be sent according to the estimated packet loss to each receiver, encodes the messages before the wireless transmission according to the procedure presented in Section IV and the anticipated packet loss to the eavesdropper and broadcast the coded packets ensures that the legitimate users will be available to obtain the original transmitted data while any eavesdropper with higher packet loss rate will be kept ignorant. A simple illustration is given in Figure 7: a transmitter utilizing MU-MIMO techniques to direct the beams toward its intended receivers such that eavesdroppers which are sparsely scattered are expected to experience a lower quality channel hence higher packet loss than the intended receivers; the transmitter is utilizing the individual-SMSM coding scheme suggested in Section IV, ensuring individual security as proved in this paper. In some sense, a similar application was suggested in [67], [68] for secure data exchange, where legitimate clients want to directly exchange information over a wireless channel in the presence of an eavesdropper. These works considered the matrix completion problem [69], and provided an MRD code, such that, given constraints on the number of messages that each legitimate client has and transmits, established bounds on the number of transmissions over broadcasting channel required for both reliability at the legitimate clients (of all the data exchanged), and weakly secrecy at the eavesdropper who obtains all transmitted data.

C. Live Broadcast of Video with Multi-Path Streaming

Multi-Path routing techniques which enable the use of multiple alternative paths between a source and a destination through the network, has been widely exploited over the years to provide a variety of benefits such as load balancing, fault tolerance, bandwidth enhancement, etc. One such ubiquitous example is LiveU innovative solution for distributing live video streams via wireless networks [70], [71]. In these systems, the real-time recorded video is encoded in packets by the source. These encoded packets include pieces of the data to be transmitted through different distributed media. For example, the pieces of the data transmitted over various technologies such as cellular networks, WiFi, satellite, fiber internet, etc. or various providers, e.g., Sprint, T-Mobile, AT&T Verizon, etc. A local server at the legitimate client decodes the data received from the different distributed media. This distributed streaming system maintains a high-quality viewer experience and cost-efficiency since the source can adapt the number of pieces dynamically to be transmitted by the different media. For example, if the connection using cellular or WiFi is lost during the real-time transmission, the source can route the pieces of the data dynamically by other connections or medias, taking into account the cost of each transmission by the optional connections.

In context to individual security suggested herein, we consider the case where there is an eavesdropper which has access to only a subset of the connections during the real-time distributed streaming (we assume that the eavesdropper can access any set of the streams unknown to the source, yet only a subset thereof). Utilizing the individual security coding scheme suggested in this paper, i.e., encoding the packets prior to the transmission, according to the coding scheme suggested in Section IV, guarantees Individual Secure Live Broadcast of Video with Multi-Path Streaming, such that an eavesdropper which can capture at most w streams transmitted over the different distributed medias is kept ignorant in the sense of having zero mutual information, regarding any set of k_s messages individually, yet may potentially obtain *insignificant* information about mixtures of packets transmitted. Figure 8 depicts a graphical representation of this system.

IX. Conclusions

In this paper, we proposed SMSM codes under an *Individual Security* constraint. In this model, the eavesdropper is kept ignorant, in the sense of having zero mutual information regarding each message separately, yet may potentially obtain

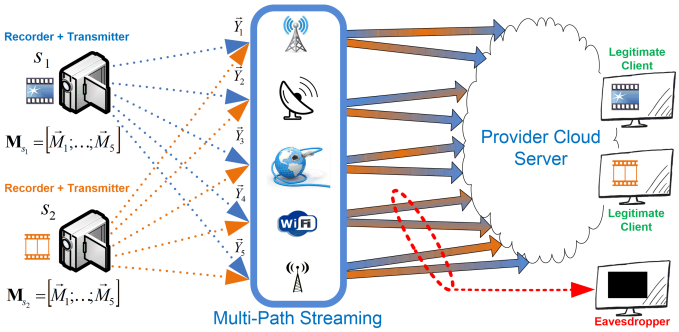

Figure 8: Individual Secure Live Broadcast of Video with Multi-Path Streaming. The sources s_1, s_2 needs to transmit the real-time recorded video $\mathbf{M}_{s_1}$, $\mathbf{M}_{s_2}$, respectively, encoded by LNC to 5 packets $\vec{Y}_1,\ldots,\vec{Y}_5$ from each source, over the different medias. The intermediate providers, such as cellular networks, WiFi, satellite, fiber internet, etc may use LNC before their routing transmission. Then, the legitimate clints which received from a local provider cloud server all the packets, can decodes all the data. In the individual secure model of this problem, we assume the existence of an eavesdropper, which is able to obtain information from any 4 connections. However, the individual secure code suggested herein, assure that the eavesdropper is not able to decode the original recorded information from the wiretapped connections.

insignificant information about mixtures of packets transmitted. In fact, it ensures Eve is kept ignorant of any *set of* $k-w$ *messages*. That is, guarantee zero mutual information, with respect to any set of $k-w$ messages.

We completely characterized the rate region for individually secure MSM. Specifically, we showed that secure communication is achievable up to the min-cut, that is, without any decrease in the rate or any message "blow-up" by extra randomness. Moreover, we provided a code for Strong-SMSM by extra randomness, i.e., requiring Eve's mutual information *with all messages simultaneously* to be zero. While this included a rate loss, it is important to note that in the code suggested the alphabet size did not increase with the network parameters due to the strong-security constraint.

Finally, we showed a few examples out of many important applications, like data centers, wireless networks, gossip and live broadcasting of video, for which the individual security coding schemes suggested is applicable, and achieves the full capacity of these systems.

References

[1] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE transactions on information theory*, vol. 49, no. 2, pp. 371–381, 2003.

[2] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[3] N. Cai and R. W. Yeung, "Secure network coding," in *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*. IEEE, 2002, p. 323.

[4] T. Chan and A. Grant, "Capacity bounds for secure network coding," in *Communications Theory Workshop, 2008. AusCTW 2008. Australian*. IEEE, 2008, pp. 95–100.

[5] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *Information Theory, IEEE Transactions on*, vol. 57, no. 1, pp. 424–435, 2011.

[6] S. Y. El Rouayheb and E. Soljanin, "On wiretap networks II," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. IEEE, 2007, pp. 551–555.

[7] D. Silva and F. R. Kschischang, "Security for wiretap networks via rank-metric codes," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*. IEEE, 2008, pp. 176–180.

[8] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1361–1371, 2012.

[9] N. Cai and R. W. Yeung, "A security condition for multi-source linear network coding," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. IEEE, 2007, pp. 561–565.

[10] Z. Zhang and R. W. Yeung, "A general security condition for multi-source linear network coding," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 1155–1158.

[11] N. Cai, "Valuable messages and random outputs of channels in linear network coding," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 413–417.

[12] N. Cai and T. Chan, "Theory of secure network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[13] T. H. Chan and A. Grant, "Network coding capacity regions via entropy functions," *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5347–5374, 2014.

[14] D. Kobayashi, H. Yamamoto, and T. Ogawa, "Secure multiplex coding attaining channel capacity in wiretap channels," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8131–8143, 2013.

[15] A. S. Mansour, R. F. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *Information Theory Workshop (ITW), 2014 IEEE*. IEEE, 2014, pp. 426–430.

[16] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the individual secrecy rate region for the broadcast channel with an external eavesdropper," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 1347–1351.

[17] A. S. Mansour, R. F. Schaefer, and H. Boche, "The individual secrecy capacity of degraded multi-receiver wiretap broadcast channels," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 4181–4186.

[18] ——, "On the individual secrecy capacity regions of the general, degraded and gaussian multi-receiver wiretap broadcast channel," *IEEE Transactions on Information and Security, 2016*, vol. 11, no. 9, pp. 2107–2122, 2016.

[19] M. Goldenbaum, R. F. Schaefer, and H. V. Poor, "The multiple-access channel with an external eavesdropper: Trusted vs. untrusted users," in *2015 49th Asilomar Conference on Signals, Systems and Computers*. IEEE, 2015, pp. 564–568.

[20] Y. Chen, O. O. Koyluoglu, and A. H. Vinck, "On secure communication over the multiple access channel," *International Symposium on Information Theory and Its Applications (ISITA), 2016 IEEE*, 2016.

[21] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," *NetCod, Apr*, vol. 104, 2005.

[22] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. IEEE, 2007, pp. 546–550.

[23] J. Claridge and I. Chatzigeorgiou, "Probability of partially decoding network-coded messages," *IEEE Communications Letters*, vol. 21, no. 9, pp. 1945–1948, 2017.

[24] S. Kadhe and A. Sprintson, "Weakly secure regenerating codes for distributed storage," in *Network Coding (NetCod), 2014 International Symposium on*. IEEE, 2014, pp. 1–6.

[25] ——, "On a weakly secure regenerating code construction for minimum storage regime," in *Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on*. IEEE, 2014, pp. 445–452.

[26] N. Paunkoska, V. Kafedziski, and N. Marina, "Improved perfect secrecy of distributed storage systems using interference alignment," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2016 8th International Congress on*. IEEE, 2016, pp. 240–245.

[27] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *Networking and Information Theory, 2009. ITW 2009. IEEE Information Theory Workshop on*. IEEE, 2009, pp. 281–285.

[28] S. Deb, M. Médard, and C. Choute, "Algebraic gossip: A network coding approach to optimal multiple rumor mongering," *Information Theory, IEEE Transactions on*, vol. 52, no. 6, pp. 2486–2507, 2006.

[29] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, "Epidemic algorithms for replicated database maintenance," in *Proceedings of the sixth annual ACM Symposium on Principles of distributed computing*. ACM, 1987, pp. 1–12.

[30] S. Deb, M. Medard, and C. Choute, "On random network coding based information dissemination," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*. IEEE, 2005, pp. 278–282.

[31] B. Haeupler, "Analyzing network coding gossip made easy," in *Proceedings of the 43rd annual ACM symposium on Theory of computing*. ACM, 2011, pp. 293–302.

[32] A. S. Mansour, R. F. Schaefer, and H. Boche, "The individual secrecy capacity of the gaussian SISO and degraded gaussian MIMO multi-receiver wiretap channel," in *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2015, pp. 365–369.

[33] A. Cohen, B. Haeupler, C. Avin, and M. Médard, "Network coding based information spreading in dynamic networks with correlated data," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 2, pp. 213–224, 2015.

[34] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.

[35] R. Karp, C. Schindelhauer, S. Shenker, and B. Vocking, "Randomized rumor spreading," in *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*. IEEE, 2000, pp. 565–574.

[36] D. Kempe, A. Dobra, and J. Gehrke, "Gossip-based computation of aggregate information," in *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*. IEEE, 2003, pp. 482–491.

[37] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *Information Theory, IEEE Transactions on*, vol. 52, no. 6, pp. 2508–2530, 2006.

[38] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "Secure network coding via filtered secret sharing," in *42nd Annual Allerton Conf. Commun*, 2004.

[39] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[40] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[41] X. Zhou, Y. Zhang, and L. Song, *Physical layer security in wireless communications*. Crc Press, 2016.

[42] B. K. Dey, S. Jaggi, and M. Langberg, "Sufficiently myopic adversaries are blind," in *Information Theory (ISIT), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 1164–1168.

[43] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1124–1135, 2011.

[44] R. Matsumoto and M. Hayashi, "Universal secure multiplex network coding with dependent and non-uniform messages," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3773–3782, 2017.

[45] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[46] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[47] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The google file system," in *ACM SIGOPS operating systems review*, vol. 37, no. 5. ACM, 2003, pp. 29–43.

[48] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels, "Dynamo: amazon's highly available key-value store," *ACM SIGOPS operating systems review*, vol. 41, no. 6, pp. 205–220, 2007.

[49] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber, "Bigtable: A distributed storage system for structured data," *ACM Transactions on Computer Systems (TOCS)*, vol. 26, no. 2, p. 4, 2008.

[50] D. Borthakur, J. Gray, J. S. Sarma, K. Muthukkaruppan, N. Spiegelberg, H. Kuang, K. Ranganathan, D. Molkov, A. Menon, S. Rash *et al.*, "Apache hadoop goes realtime at facebook," in *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*. ACM, 2011, pp. 1071–1080.

[51] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci *et al.*, "Windows azure storage: a highly available cloud storage service with strong consistency," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*. ACM, 2011, pp. 143–157.

[52] A. Auradkar, C. Botev, S. Das, D. De Maagd, A. Feinberg, P. Ganti, L. Gao, B. Ghosh, K. Gopalakrishna, B. Harris *et al.*, "Data infrastructure at linkedin," in *Data Engineering (ICDE), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 1370–1381.

[53] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[54] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[55] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.

[56] S. Acedanski, S. Deb, M. Médard, and R. Koetter, "How good is random linear coding based distributed networked storage," in *Workshop on Network Coding, Theory and Applications*, 2005, pp. 1–6.

[57] B. Haeupler and M. Médard, "One packet suffices-highly efficient packetized network coding with finite memory," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 1151–1155.

[58] B. Haeupler, M. Kim, and M. Médard, "Optimality of network coding with buffers," in *Information Theory Workshop (ITW), 2011 IEEE*. IEEE, 2011, pp. 533–537.

[59] F. H. Fitzek, T. Toth, A. Szabados, M. V. Pedersen, D. E. Lucani, M. Sipos, H. Charaf, and M. Medard, "Implementation and performance evaluation of distributed cloud storage solutions using random linear network coding," in *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 249–254.

[60] D. S. Lun, M. Médard, and R. Koetter, *Efficient operation of wireless packet networks using network coding*. IWCT, 2005, vol. 5.

[61] M. Kim, M. Médard, and J. Barros, "Algebraic watchdog: mitigating misbehavior in wireless network coding," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 1916–1925, 2011.

[62] R. A. Popa, A. Chiesa, T. Badirkhanli, and M. Médard, "Going beyond pollution attacks: Forcing byzantine clients to code correctly," *arXiv preprint arXiv:1108.2080*, 2011.

[63] V. N. Talooki, R. Bassoli, D. E. Lucani, J. Rodriguez, F. H. Fitzek, H. Marques, and R. Tafazolli, "Security concerns and countermeasures in network coding based communication systems: A survey," *Computer Networks*, vol. 83, pp. 422–445, 2015.

[64] U. Speidel, E. Cocker, P. Vingelmann, J. Heide, and M. Médard, "Can network coding bridge the digital divide in the pacific?" in *Network Coding (NetCod), 2015 International Symposium on*. IEEE, 2015, pp. 86–90.

[65] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "On coding for reliable communication over packet networks," *Physical Communication*, vol. 1, no. 1, pp. 3–20, 2008.

[66] J. Hansen, D. E. Lucani, J. Krigslund, M. Médard, and F. H. Fitzek, "Network coded software defined networking: enabling 5g transmission and storage networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 100–107, 2015.

[67] M. Yan and A. Sprintson, "Algorithms for weakly secure data exchange," in *Network Coding (NetCod), 2013 International Symposium on*. IEEE, 2013, pp. 1–6.

[68] M. Yan, A. Sprintson, and I. Zelenko, "Weakly secure data exchange with generalized reed solomon codes," in *Information Theory (ISIT), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 1366–1370.

[69] N. Cohen, C. R. Johnson, L. Rodman, and H. J. Woerdeman, "Ranks of completions of partial matrices," in *The Gohberg anniversary collection. Birkhäuser Basel*. Springer, 1989, pp. 165–185.

[70] LiveU. (2017) Live cellular uplinking for television and the web. [Online]. Available: Cellular-uplinking-white-paper-LiveU.doc

[71] ——. (2017) The Internet can be a scary place for your live video: don't let a bad stream cost you your audiences. [Online]. Available: http://www.pts.gr/files/LiveU-Live-Streaming-Whitepaper.pdf

Alejandro Cohen received the B.Sc. from the Department of Electrical Engineering, SCE college of engineering, Israel, in 2010 and M.Sc. degree at the communication system engineering, Ben-Gurion University of the Negev, Beer Sheva, Israel, in 2013. Currently pursuing the Ph.D. degree in communication system engineering. His main research interests are in the area of wireless communication, security, network information theory and network coding. From 2007 to 2014 he was with DSP Group in Herzelya where he worked on voice enhancement and signal processing. Currently he is with Intel in Petah-Tikva where he works in innovation group at mobile and wireless.

Asaf Cohen is a senior lecturer at the Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel. Before that, he was a post-doctoral scholar at the California Institute of Technology (Caltech). He received the B.Sc., M.Sc. (both with high honors) and Ph.D. from the Department of Electrical Engineering, Technion, Israel Institute of Technology, in 2001, 2003 and 2007, respectively. From 1998 to 2000 he was with the IBM Research Laboratory in Haifa where he worked on distributed computing. His areas of interest are information theory, learning andcoding. In particular, he is interested in sequential decision making, with applications to detection and estimation; Network security and anomaly detection; Network information theory and network coding; Statistical signal processing; Coding theory and performance analysis of codes. Dr. Cohen received several honors and awards, including the Viterbi post-doctoral scholarship, a student paper award at IEEE Israel 2006 and the Dr. Philip Marlin Prize for Computer Engineering, 2000.

Muriel Médard is the Cecil H. Green Professor in the Electrical Engineering and Computer Science (EECS) Department at MIT and leads the Network Coding and Reliable Communications Group at the Research Laboratory for Electronics at MIT. She has co-founded three companies to commercialize network coding, CodeOn, Steinwurf and Chocolate Cloud. She has served as editor for many publications of the Institute of Electrical and Electronics Engineers (IEEE), of which she was elected Fellow, and she has served as Editor in Chief of the IEEE Journal on Selected Areas in Communications. She was President of the IEEE Information Theory Society in 2012, and served on its board of governors for eleven years. She has served as technical program committee co-chair of many of the major conferences in information theory, communications and networking. She received the 2009 IEEE Communication Society and Information Theory Society Joint Paper Award, the 2009 William R. Bennett Prize in the Field of Communications Networking, the 2002 IEEE Leon K. Kirchmayer Prize Paper Award, the 2018 ACM SIGCOMM Test of Time Paper Award and several conference paper awards. She was co-winner of the MIT 2004 Harold E. Edgerton Faculty Achievement Award, received the 2013 EECS Graduate Student Association Mentor Award and served as Housemaster for seven years. In 2007 she was named a Gilbreth Lecturer by the U.S. National Academy of Engineering. She received the 2016 IEEE Vehicular Technology James Evans Avant Garde Award, the 2017 Aaron Wyner Distinguished Service Award from the IEEE Information Theory Society and the 2017 IEEE Communications Society Edwin Howard Armstrong Achievement Award.

Omer Gurewitz received the B.Sc. degree in Physics from Ben Gurion University, Beer Sheva, Israel, in 1991, and the M.Sc. and Ph.D. degrees in Electrical Engineering from the Technion Israel Institute of Technology, Haifa, Israel, in 2000 and 2005, respectively. He is an Assistant Professor with the Department of Communication Systems Engineering, Ben Gurion University. Between 2005 and 2007, he was a Post-doctoral Researcher with the Electrical and Computer Engineering (ECE) Department, Rice University, Houston, TX, USA. His research interests are in the field of performance evaluation of wired and wireless communication networks. His current projects include cross-layer design and implementation of medium access protocols for next generation wireless communication.