Multiple-access Network Information-flow and Correction Codes*

Theodoros K. Dikaliotis**, Tracey Ho**, Sidharth Jaggi**, Svitlana Vyetrenko**, Hongyi Yao**
Michelle Effros, Joerg Kliewer, Elona Erez

Abstract

This work considers the multiple-access multicast error-correction scenario over a packetized network with z malicious edge adversaries. The network has min-cut m and packets of length ℓ, and each sink demands all information from the set of sources $\mathcal{S}$. In this paper we look at both the "side-channel" model (where sources and sinks share some random bits that are secret from the adversary) and the "omniscient" adversarial model (where we do not assume limitations on the adversary's knowledge). For both adversarial models, we provide outer bounds on the achievable rate-region for communication, and give corresponding communication schemes that operate at rates matching any point satisfying the outer bounds. In the "side-channel" adversarial model, the use of a secret channel allows higher rates to be achieved compared to the "omniscient" adversarial model, and a polynomial-time code to achieve the optimal rates is provided. For the "omniscient" adversarial model, we develop two capacity-achieving communication schemes: the first approach is based on random subspace code design of complexity that grows exponentially in ℓm, whereas, the second approach uses a novel multiple-field-extension technique to provide an algorithm that is polynomial-time in the network size, having an $O(\ell m^{|\mathcal{S}|})$ complexity. Our codes are "end-to-end", that is, all nodes except the sources and the sinks are oblivious to the adversaries present in the network and may simply implement predesigned linear network codes (random or otherwise). The codes are also distributed in that each source does not require knowledge of the data transmitted by other sources.

* In other words, MANIAC codes.

** The first five authors had equal contribution to this work and they are named in alphabetical order.

Theodoros K. Dikaliotis, Tracey Ho, Svitlana Vyetrenko and Michelle Effros are with California Institute of Technology, email: {tdikal, tho, svitlana, effros}@caltech.edu. Sidharth Jaggi is with the Chinese University of Hong Kong, email: jaggi@ie.cuhk.edu.hk. Hongyi Yao is with Tsinghua University, email:yaohongyi03@gmail.com. Joerg Kliewer is with New Mexico State University, email:jkliewer@nmsu.edu. Elona Erez is with Yale University, email:elona.erez@caltech.edu.

The work of Theodoros Dikaliotis, Svitlana Vyetrenko and Tracey Ho was supported by subcontract #069153 issued by BAE Systems National Security Solutions, Inc. and by the Defense Advanced Research Projects Agency (DARPA) and the Space and Naval Warfare System Center (SPAWARSYSCEN), San Diego under Contract No. N66001-08-C-2013, AFOSR under Grant 5710001972, Caltech's Lee Center for Advanced Networking, and NSF grant CNS-0905615. The work of Sidharth Jaggi was supported by the RGC GRF grants 412608 and 412809, the CUHK MoE-Microsoft Key Laboratory of Human-centric Computing and Interface Technologies, the Institute of Theoretical Computer Science and Communications, and Project No. AoE/E-02/08 from the University Grants Committee of the Hong Kong Special Administrative Region, China. The work of Hongyi Yao was supported by the National Natural Science Foundation of China Grant 61033001 and 61073174, the National Basic Research Program of China Grant 2007CB807900 and 2007CB807901, the Hi-Tech research & Development Program of China Grant 2006AA10Z216. The work of Joerg Kliewer was supported by NSF grant CCF-0830666.

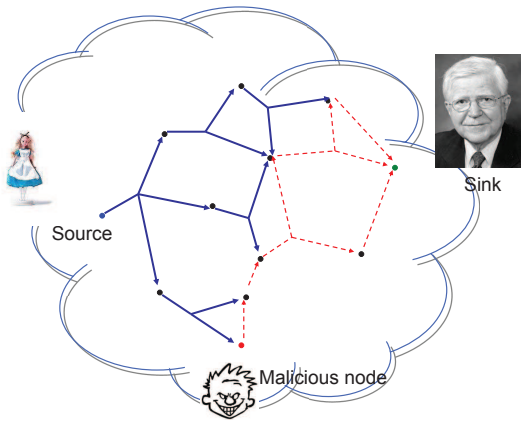

Fig. 1. Propagation of network errors via network coding. The action of a single malicious node contaminates all incoming links of the sink node due to packet mixing at downstream nodes.

Index Terms

Subspace codes, random linear network coding, network error-correction, double extended field, Gabidulin codes.

I. Introduction

Information dissemination can be optimized with the use of network coding. Network coding maximizes the network throughput in multicast transmission scenarios [1]. For this scenario, it was shown in [2] that linear network coding suffices to achieve the max-flow capacity from the source to each receiving node. An algebraic framework for linear network coding was presented in [3]. Further, the linear combinations employed at network nodes can be randomly selected in a distributed manner; if the coding field size is sufficiently large the max-flow capacity is achieved with high probability [4].

However, network coding is vulnerable to malicious attacks from rogue users. Due to the mixing operations at internal nodes, the presence of even a small number of adversarial nodes can contaminate the majority of packets in a network, preventing sinks from decoding. In particular, an error on even a single link might propagate to multiple downstream links via network coding, which might lead to the extreme case in which all incoming links at the sink are in error. This is shown in Fig. 1, where the action of a single malicious node contaminates all incoming links of the sink node due to packet mixing at downstream nodes. In such a case, network error-correction (introduced in [5]) rather than classical forward error-correction (FEC) is required, since the former exploits the fact that the errors at the sinks are correlated, whereas the latter assumes independent errors.

A number of papers e.g. [6], [7], [8] have characterized the set of achievable communication rates over networks containing hidden malicious jamming and eavesdropping adversaries, and given corresponding communication schemes. The latest code constructions (for instance [8] and [9]) have excellent parameters – they have low computational complexity, are distributed, and are asymptotically rate-optimal. However, in these papers the focus has been on single-source multicast problems, where a single source wishes to communicate all its information to all sinks.

In this work we examine the problem of multiple-access multicast, where multiple sources wish to communicate all their information to all sinks. We characterize the optimal rate-region for several variants of the multiple-access network error-correction problem and give matching code constructions, which have low computational complexity when the number of sources is small.

We are unaware of any straightforward application of existing single-source network error-correcting subspace codes that achieve the optimal rate regions. This is because single-source network error-correcting codes such as those of [9] and [8] require the source to judiciously insert redundancy into the transmitted codeword; however, in the distributed source case the codewords are constrained by the independence of the sources.

II. Background and related work

For a single-source single-sink network with min-cut C, the capacity of the network under arbitrary errors on up to z links is given by

$$R \leq C - 2z \tag{1}$$

and can be achieved by a classical end-to-end error-correction code over multiple disjoint paths from source to the sink. This result is a direct extension of the Singleton bound (see, *e.g.*, [10]). Since the Singleton bound can be achieved by a maximum distance separable code, as for example a Reed-Solomon code, such a code also suffices to achieve the capacity in the single-source single-sink case.

In the network multicast scenario, the situation is more complicated. For the single-source multicast the capacity region was shown ([5], [6], [7]) to be the same as (1), with C now representing the minimum of the min-cuts [6]. However, unlike single-source single-sink networks, in the case of single-source multicast, network error correction is required: network coding is required in general for multicast even in the error-free case [1], and with the use of network coding errors in the sink observations become dependent and cannot be corrected by end-to-end codes.

Two flavors of the network error correction problem are often considered. In the *coherent* case, it is assumed that there is centralized knowledge of the network topology and network code. Network error correction for this case was first addressed by the work of Cai and Yeung [5], [6], [7] for the single source scenario by generalizing classical coding theory to the network setting. However, their scheme has decoding complexity which is exponential in the network size.

In the harder *non-coherent* case, the network topology and/or network code are not known *a priori* to any of the honest parties. In this setting, [9], [11] provided network error-correcting codes with a design and implementation complexity that is only polynomial in the size of network parameters. Reference [11] introduced an elegant approach where information transmission occurs via the space spanned by the received packets/vectors, hence any generating set for the same space is equivalent to the sink [11]. Error-correction techniques for this case were proposed in [11] and [8] in the form of constant dimension and rank metric codes, respectively, where the codewords are defined as subspaces of some ambient space. These works considered only the single source case.

For the non-coherent multi-source multicast scenario *without* errors, the scheme of [4] achieves any point inside the rate-region. An extension of subspace codes to multiple sources, for a non-coherent multiple-access channel model without errors, was provided in [12], which gave practical achievable (but not rate-optimal) algebraic code constructions, and in [13], which derived the capacity region and gave a rate-optimal scheme for two sources. For the multi-source case with errors, [14] provided an efficient code construction achieving a strict subregion of the capacity region.

III. Challenges

In this work we address the capacity region and the corresponding code design for the multiple-source multicast communication problem under different adversarial scenarios. The issues which arise in this problem are best explained with a simple example for a single sink, which is shown in Fig. 2. Suppose that the sources $\mathcal{S}_1$ and $\mathcal{S}_2$ encode their information independently from each other. We can allocate one part of the network to carry only information from $\mathcal{S}_1$, and another part to carry only information from $\mathcal{S}_2$. In this case only one source is able to communicate reliably under one link error. However, if coding at the middle nodes N_1 and N_2 is employed, the two sources are able to share network capacity to send redundant information, and each source is able to communicate reliably at capacity 1 under a single link error. This shows that in contrast to the single source case, coding across multiple sources is required, so

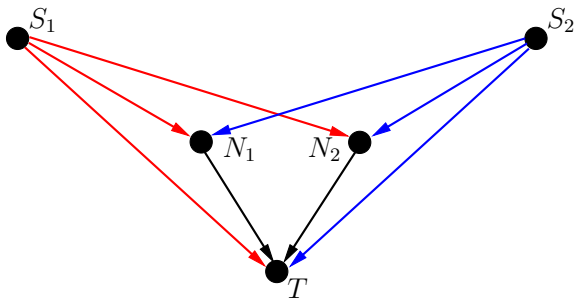

Fig. 2. A simple example to show that in the multiple source case in-network coding is required to achieve the network error correction capacity.

that sources can simultaneously use shared network capacity to send redundant information, even for a single sink.

In Section VII we show that for the example network in Fig. 2, the capacity region is given by

$$\begin{aligned} R_1 &\leq m_{\mathcal{S}_1} - 2z \\ R_2 &\leq m_{\mathcal{S}_2} - 2z \\ R_1 + R_2 &\leq m_{\mathcal{S}_1,\mathcal{S}_2} - 2z, \end{aligned} \tag{2}$$

where for $i = 1, 2$, rate R_i is the information rate of $\mathcal{S}_i$, min-cut $m_{\mathcal{S}_i}$ is the minimum cut capacity between $\mathcal{S}_i$ and sink T, min-cut $m_{\mathcal{S}_1,\mathcal{S}_2}$ is the minimum cut capacity between $\mathcal{S}_1$, $\mathcal{S}_2$ and T and z is the known upper bound on the number of link errors. Hence, similarly to single-source multicast, the capacity region of a multi-source multicast network is described by the cut-set bounds. From that perspective, one may draw a parallel with point-to-point error-correction. However, for multi-source multicast networks point-to-point error-correcting codes do not suffice and a careful network code design is required. For instance, the work of [14], which applies single-source network error-correcting codes for this problem, achieves a rate-region that is strictly smaller than the capacity region (2) when $m_{\mathcal{S}_1} + m_{\mathcal{S}_2} \neq m_{\mathcal{S}_1,\mathcal{S}_2}$ [15].

IV. Our results

In this paper we consider a "side-channel" model and an "omniscient" adversarial model. In the former, the adversary does not have access to all the information available in the network, for example as in [9], [16] where the sources share a secret with the sink(s) in advance of the network communication. Let $\mathcal{S}$ be the set of sources in the network, s be the number of sources, R_i be the multicast transmission rate from source $\mathcal{S}_i$, $1 \leq i \leq s$, to every sink, and for any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$ let $m_{\mathcal{S}'}$ be the minimum min-cut capacity between any sink and $\mathcal{S}'$.

In Section VI we prove the following theorem:

Theorem 1. *Consider a multiple-source multicast network error-correction problem on network $\mathcal{G}$–possibly with unknown topology–where each source shares a random secret with each of the sinks. For any errors on up to z links, the capacity region is given by:*

$$\sum_{i\in\mathcal{I}(\mathcal{S}')} R_i \leq m_{\mathcal{S}'} - z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{3}$$

and every point in the rate region can be achieved with a polynomial-time code.

By capacity region we mean the closure of all rate tuples $(R_1, \ldots, R_s)$ for which there is a sequence of codes of length ℓ, message sets $\mathcal{J}_\ell^i = \{1, \ldots, J_\ell^i\}$ and encoding and decoding functions $\{f_\ell^i\}, \{\phi_\ell^j\}$ for every node i in the network and every sink j, so that for every $\epsilon > 0$ and $\delta > 0$ there is integer $L(\epsilon, \delta) > 0$ such that for every $\ell > L(\epsilon, \delta)$ we have $\frac{1}{\ell} \log |\mathcal{J}^i| \geq R_i - \epsilon$ and the probability of decoding error at any sink is less than δ regardless of the message.

In "omniscient" adversarial model, we do not assume any limitation on the adversary's knowledge, i.e. decoding should succeed for *arbitrary* error values. In Section VII-A we derive the multiple-access network error-correction capacity for both the coherent and non-coherent case. We show that network error-correction coding allows redundant network capacity to be shared among multiple sources, enabling the sources to simultaneously communicate reliably at their individual cut-set capacities under adversarial errors. Specifically, we prove the following theorem:

Theorem 2. *Consider a multiple-source multicast network error-correction problem on network $\mathcal{G}$ whose topology may be unknown. For any errors on up to z links, the capacity region is given by:*

$$\sum_{i\in\mathcal{I}(\mathcal{S}')} R_i \leq m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{4}$$

The rate-regions are, perhaps not surprisingly, larger for the side-channel model than for the omniscient adversarial model.

Finally, in Section VII-B we provide computationally efficient distributed schemes for the non-coherent case (and therefore for the coherent case too) that are rate-optimal for correction of network errors injected by computationally unbounded adversaries. In particular, our code construction achieves decoding success probability at least $1 - |s||\mathcal{E}|/p$ where p is the size of the finite field $\mathbb{F}_p$ over which coding is performed, with complexity $O(\ell m^{|\mathcal{S}|})$, which is polynomial in the network size.

The remainder of the paper is organized as follows: In Section V we formally introduce our problem and give some mathematical preliminaries. In Section VI we derive the capacity region and construct multi-source multicast error-correcting codes for the side-channel model. In Section VII, we consider two network error-correction schemes for omniscient adversary models which are able to achieve the full capacity region in both the coherent and non-coherent case. In particular, we provide a general approach based on minimum distance decoding, and then refine it to a practical code construction and decoding algorithm which has polynomial complexity (in all parameters except the number of sources). Furthermore, our codes are fully distributed in the sense that different sources require no knowledge of the data transmitted by their peers, and end-to-end, *i.e.* all nodes are oblivious to the adversaries present in the network and simply implement random linear network coding [17]. A remaining bottleneck is that while the implementation complexity (in terms of packet-length, field-size, and computational complexity) of our codes is polynomial in the size of most network parameters, it increases exponentially with the number of sources. Thus, the design of efficient schemes for a large number of sources is still open. Portions of this work were presented in [18] and in [19].

V. Preliminaries

A. Model

We consider a delay-free acyclic network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges. The capacity of each edge is normalized to be one symbol of the finite field $\mathbb{F}_p$ per unit time where p is a power of a prime. Edges with non-unit capacity are modeled as parallel edges.

There are two subsets $\mathcal{S}, \mathcal{T} \subseteq \mathcal{V}$ of nodes where $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_s\}$ is a set of s sources and $\mathcal{T}$ is a set of sinks within the network. Let R_i be the multicast transmission rate from $\mathcal{S}_i$, $1 \leq i \leq s$, to every sink. For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $\mathcal{I}(\mathcal{S}') \subseteq \{1, 2, \ldots, s\}$ be the indices of the source nodes that belong to $\mathcal{S}'$. Let $m_{\mathcal{S}'}$ be the minimum min-cut capacity between $\mathcal{S}'$ and any sink. For each i, let $\mathcal{C}_i$ be the code used by source i. Let $\mathcal{C}_{\mathcal{S}'}$ be the Cartesian product of the individual codes of the sources in $\mathcal{S}'$.

Within the network there is a computationally unbounded adversary who can observe all the transmissions and inject its own packets on up to z links that may be chosen as a function of his knowledge of the network, the message, and the communication scheme. The location of the z adversarial links is fixed

Note that since each transmitted symbol in the network is from a finite field, modifying symbol x to symbol y is equivalent to injecting/adding symbol $y - x$ into x.

but unknown to the communicating parties. In case of a *side-channel model*, there additionally exists a random secret shared between all sources and each of the sinks as in [9], [16].

The sources on the other hand do not have any knowledge about each other's transmitted information or about the links compromised by the adversary. Their goal is to judiciously add redundancy into their transmitted packets so that they can achieve any rate-tuple within the capacity region.

B. Random Linear Network Coding

In this paper, we consider the following well-known distributed random linear coding scheme [17].

Sources: All sources have incompressible data which they wish to deliver to all the destinations over the network. Source $\mathcal{S}_i$ arranges its data into batches of b_i packets and insert these packets into a $b_i \times \ell$ *message matrix* M_i over $\mathbb{F}_p$ (the *packet-length* ℓ is a network design parameter). Each source $\mathcal{S}_i$ then takes independent and uniformly random linear combinations over $\mathbb{F}_p$ of the rows of M_i to generate the packets transmitted on each outgoing edge.

Network nodes: Each internal node similarly takes (uniformly) random linear combinations of the packets on its incoming edges to generate packets transmitted on its outgoing edges.

Adversary: The adversarial packets are defined as the difference between the received and transmitted packets on each link. They are similarly arranged into a matrix Z of size $z \times \ell$.

Sink: Each sink $t \in \mathcal{T}$ constructs a $B \times \ell$ matrix Y over $\mathbb{F}_p$ by treating the received packets as consecutive length-ℓ row vectors of Y. Since all the operations in the network are linear, each sink has an incoming matrix Y that is given by

$$Y = T_1 M_1 + T_2 M_2 + \ldots + T_s M_s + T_z Z, \tag{5}$$

where T_i, $1 \leq i \leq s$, is the overall transform matrix from $\mathcal{S}_i$ to $t \in \mathcal{T}$ and T_z is the overall transform matrix from the adversary to sink $t \in \mathcal{T}$.

C. Finite Field Extensions

In the analysis below denote by $\mathbb{F}_p^{m \times n}$ the set of all $m \times n$ matrices with elements from $\mathbb{F}_p$. The identity matrix with dimension $m \times m$ is denoted by I_m, and the zero matrix of any dimension is denoted by O. The dimension of the zero matrix will be clear from the context stated. For clarity of notation, vectors are in bold-face (*e.g.* $\mathbf{A}$).

Every finite field $\mathbb{F}_p$, where p can be *algebraically extended* [20] to a larger finite field $\mathbb{F}_q$, where $q = p^n$ for any positive integer n. Note that $\mathbb{F}_q$ includes $\mathbb{F}_p$ as a subfield; thus any matrix $A \in \mathbb{F}_p^{m\times\ell}$ is also a matrix in $\mathbb{F}_q^{m\times\ell}$. Hence throughout the paper, multiplication of matrices from different fields (one from the base field and the other from the extended field) is allowed and is computed over the extended field.

The above extension operation defines a bijective mapping between $\mathbb{F}_p^{m\times n}$ and $\mathbb{F}_q^m$ as follows:

- For each $A \in \mathbb{F}_p^{m\times n}$, the folded version of A is a vector $\mathbf{A}^f$ in $\mathbb{F}_q^m$ given by $A\mathbf{a}^{\mathsf{T}}$ where $\mathbf{a} = \{a_1, \ldots, a_n\}$ is a basis of the extension field $\mathbb{F}_q$ with respect to $\mathbb{F}_p$. Here we treat the i^{th} row of A as a single element in $\mathbb{F}_q$ to obtain the i^{th} element of $\mathbf{A}^f$.
- For each $\mathbf{B} \in \mathbb{F}_q^m$, the unfolded version of $\mathbf{B}$ is a matrix $B^u \in \mathbb{F}_p^{m\times n}$. Here we treat the i^{th} element of $\mathbf{B}$ as a row in $\mathbb{F}_p^{1\times n}$ to obtain the i^{th} row of B^u.

We can also extend these operations to include more general scenarios. Specifically any matrix $A \in \mathbb{F}_p^{m\times\ell n}$ can be written as a concatenation of matrices $A = [A_1 \ldots A_\ell]$, where $A_i \in F_p^{m\times n}$. The folding operation is defined as follows: $A^f = [\mathbf{A}_1^f \ldots \mathbf{A}_\ell^f]$. Similarly the unfolding operation u can be applied to a number of submatrices of a large matrix, e.g., $[\mathbf{A}_1^f \ldots \mathbf{A}_\ell^f]^u = [(\mathbf{A}_1^f)^u \ldots (\mathbf{A}_\ell^f)^u] = [A_1 \ldots A_\ell]$.

In this paper *double algebraic extensions* are also considered. More precisely let $\mathbb{F}_Q$ be an algebraic extension from $\mathbb{F}_q$, where $Q = q^N = p^{nN}$ for any positive integer N. Table I summarizes the notation of the fields considered.

TABLE I
SUMMARY OF FIELD NOTATIONS

Field	$\mathbb{F}_p$	$\mathbb{F}_q$	$\mathbb{F}_Q$
Size	p	$q = p^n$	$Q = q^N$

Note: Of the three fields $\mathbb{F}_p$, $\mathbb{F}_q$ and $\mathbb{F}_Q$ defined above, two or sometimes all three appear simultaneously in the same equation. To avoid confusion, unless otherwise specified, the superscript f for folding is from $\mathbb{F}_p$ to $\mathbb{F}_q$, and the superscript u for unfolding is from $\mathbb{F}_q$ (or $\mathbb{F}_Q$) to $\mathbb{F}_p$.

D. Subspace codes

In [11] an algebraic framework was developed for the non-coherent network scenario in the single-source case. The idea behind it is to treat the fixed-length packets as the vector subspaces spanned by

Let $\mathbb{F}_p[x]$ be the set of all polynomials over $\mathbb{F}_p$ and $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Then $\mathbb{F}_p[x]/f(x)$ defines an algebraic extension field $\mathbb{F}_{p^n}$ by a homomorphic mapping [20].

them. Then what really matters at the decoder is the subspace spanned by the received packets rather than the individual packets.

Let V be the vector space of length-ℓ vectors over the finite field $\mathbb{F}_p$, representing the set of all possible values of packets transmitted and received in the network. Let $\mathcal{P}(V)$ denote the set of all subspaces of V. A code $\mathcal{C}$ consists of a nonempty subset of $\mathcal{P}(V)$, where each codeword $U \in \mathcal{C}$ is a subspace of constant dimension.

Subspace errors are defined as additions of vectors to the transmitted subspace and subspace erasures are defined as deletions of vectors from the transmitted subspace. Note that depending on the network code rate and network topology, network errors and erasures translate differently to subspace errors and erasures. For instance, subject to the position of adversary in the network, one network error can result in both dimension addition and deletion (i.e., both subspace error and subspace erasure in our terminology). Let ρ be the number of subspace erasures and let t be the number of subspace errors caused by z network errors.

The subspace metric [11] between two vector spaces $U_1, U_2 \in \mathcal{P}(V)$ is defined as

$$\begin{aligned} d_S(U_1, U_2) &\doteq \dim(U_1 + U_2) - \dim(U_1 \cap U_2) \\ &= \dim(U_1) + \dim(U_2) - 2\dim(U_1 \cap U_2). \end{aligned}$$

In [11] it shown that the minimum subspace distance decoder can successfully recover the transmitted subspace from the received subspace if

$$2(\rho + t) < D_S^{\min},$$

where $D_S^{\min}$ is the minimum subspace distance of the code. Note that d_S treats insertions and deletions of subspaces symmetrically. In [21] the converse of this statement for the case when information is transmitted at the maximum rate was shown.

In [22] a different metric on V, namely, the injection metric, was introduced and shown to improve upon the subspace distance metric for decoding of non-constant-dimension codes. The injection metric between two vector spaces $U_1, U_2 \in \mathcal{P}(V)$ is defined as

$$\begin{aligned} d_I(U_1, U_2) &\doteq \max(\dim(U_1), \dim(U_2)) - \dim(U_1 \cap U_2) \\ &= \dim(U_1 + U_2) - \min(\dim(U_1), \dim(U_2)). \end{aligned}$$

d_I can be interpreted as the number of error packets that an adversary needs to inject in order to transform input space U_1 into an output space U_2. The minimum injection distance decoder is designed to decode the received subspace as with as few error injections as possible. Note that for constant-dimensional codes d_S and d_I are related by

$$d_I(U_1, U_2) = \frac{1}{2} d_S(U_1, U_2).$$

E. Gabidulin Codes and Rank Metric Codes

Gabidulin in [23] introduced a class of error correcting codes over $\mathbb{F}_p^{m\times n}$. Let $\mathbf{X} \in \mathbb{F}_q^R$ be the information vector, $G \in \mathbb{F}_q^{m\times R}$ be the generator matrix, $(G\mathbf{X})^u \in \mathbb{F}_p^{m\times n}$ be the transmitted matrix, $Z \in \mathbb{F}_p^{m\times n}$ be the error matrix, and $(G\mathbf{X})^u + Z \in \mathbb{F}_p^{m\times n}$ be the received matrix. Then decoding is possible if and only if $\text{rank}(Z) \leq \lfloor \frac{d}{2} \rfloor$, where $d = m - R + 1$ is the minimum distance of the code.

The work of [8] utilizes the results of [23] to obtain network error-correcting codes with the following properties:

Theorem 3 (Theorem 11 in [8])**.** *Let Z be expressed as $Z = \sum_{i\in[1,\tau]} \mathbf{L}_i \mathbf{E}_i$, such that:*

- *For each $i \in [1, \tau]$, $\mathbf{L}_i \in \mathbb{F}_p^{m\times 1}$ and $\mathbf{E}_i \in \mathbb{F}_p^{1\times n}$;*
- *For each $i \in [1, \mu]$, $\mathbf{L}_i$ is known a priori by the sink;*
- *For each $i \in [\mu + 1, \mu + \delta]$, $\mathbf{E}_i$ is known a priori by the sink;*
- *$2\tau - \mu - \delta \leq d - 1$,*

using Gabidulin codes the sink can decode $\mathbf{X}$ with at most $\mathcal{O}(mn)$ operations over $\mathbb{F}_q$.

When $\mu = \delta = 0$, Theorem 3 reduces to the basic case where the sink has no prior knowledge about Z.

For any matrices $B_1 \in \mathbb{F}_p^{m_1\times m}$ and $B_2 \in \mathbb{F}_p^{m_2\times m}$ the following proposition holds and is a direct consequence of Corollary 3 in [8]:

Proposition 1. $d_S(\langle B_1\rangle, \langle B_2\rangle) \leq 2\textit{rank}(B_1 - B_2)$

where $\langle B_1\rangle$, $\langle B_2\rangle$ are the row-spaces of matrices B_1, B_2 respectively.

VI. Side-Channel Model

The side-channel model is an extension of the random secret model considered in [16] to the case of multiple sources. In that model every source shares a uniformly distributed random secret with each of

the sinks. For each source the "secret" consists of a set of symbols drawn uniformly at random from the base field $\mathbb{F}_p$ and the adversary does not have access to these secret symbols. This set of uniformly random symbols can be shared between each source and the sinks either before the transmission starts or during the transmission through a low capacity channel that is secret from the adversary and cannot be attacked by it. Each source has a different secret from all the other sources which makes this scheme distributed.

Proof of Theorem 1: Converse: Let $l_{i,j}, j = 1, \ldots, n_i$, be the outgoing links of each source $S_i, i = 1, \ldots, s$. Take any $\mathcal{S}' \subseteq \mathcal{S}$. We construct the graph $\mathcal{G}_{\mathcal{S}'}$ from $\mathcal{G}$ by adding a virtual super source node $w_{\mathcal{S}'}$, and n_i links $l'_{i,j}, j = 1, \ldots, n_i$, from $w_{\mathcal{S}'}$ to source S_i for each $i \in \mathcal{I}(\mathcal{S}')$. Note that the minimum cut capacity between $w_{\mathcal{S}'}$ and any sink is at least $m_{\mathcal{S}'}$. Any network code that multicasts rate R_i from each source $S_i, i \in \mathcal{I}(\mathcal{S}')$ over $\mathcal{G}$ corresponds to a network code that multicasts rate $\sum_{i \in \mathcal{I}(\mathcal{S}')} R_i$ from $w_{\mathcal{S}'}$ to all sinks over $\mathcal{G}_{\mathcal{S}'}$; the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}$ and $\mathcal{G}_{\mathcal{S}'}$. For the case of a single source, the adversary can choose the z links on the min-cut and set their outputs equal to zero. Therefore in this case the maximum possible achievable rate R is

$$R \leq C - z \tag{6}$$

where C is the multicast min-cut capacity of the network. The converse follows from applying inequality (6) to $w_{\mathcal{S}'}$ for each $\mathcal{S}' \subseteq \mathcal{S}$. ■

Achievability: In the case of the side-channel model, for notational convenience, we will restrict ourselves to the analysis of the situation where there are only two sources $\mathcal{S}_1, \mathcal{S}_2 \in \mathcal{V}$ transmitting information to one sink $t \in \mathcal{V}$, since the extension of our result to more sources and sinks is straightforward and analyzed briefly in Section VIII.

Encoding: Source $\mathcal{S}_1$ encodes its data into matrix $X_1 \in \mathbb{F}_p^{R_1 \times (\ell - \alpha)}$ of size $R_1 \times (\ell - \alpha)$, where $\alpha = m^2_{\mathcal{S}_1,\mathcal{S}_2} + 1$, with symbols from $\mathbb{F}_p$ and arranges its message into $M_1 = \begin{bmatrix} L_1 & X_1 \end{bmatrix}$ where $L_1 \in \mathbb{F}_p^{R_1 \times \alpha}$ is a matrix that will be defined below. Similarly, source $\mathcal{S}_2$ arranges its data into matrix $M_2 = \begin{bmatrix} L_2 & X_2 \end{bmatrix}$ where $L_2 \in \mathbb{F}_p^{R_2 \times \alpha}$ will be defined below and $X_2 \in \mathbb{F}_p^{R_2 \times (\ell - \alpha)}$.

The shared secret between source $\mathcal{S}_i$ and sink t is composed of a length–α vector $W_i = \begin{bmatrix} w_{i1} & \ldots & w_{i\alpha} \end{bmatrix} \in \mathbb{F}_p^{1 \times \alpha}$ and a matrix $H_i \in \mathbb{F}_p^{R_i \times \alpha}$, where the elements of both W_i and H_i are drawn uniformly at random from $\mathbb{F}_p$. The vector W_i defines a *parity-check* matrix $P_i \in \mathbb{F}_p^{\ell \times \alpha}$ whose (m, n)-th entry equals $(w_{in})^m$,

i.e., the element w_{in} taken to the m^{th} power. The matrix L_i is defined so that the following equality holds

$$H_i \;=\; M_iP_i = \begin{bmatrix} L_i & X_i \end{bmatrix} \begin{bmatrix} V_i \\ -- \\ \tilde{P}_i \end{bmatrix} = L_iV_i + X_i\tilde{P}_i \tag{7}$$

where V_i, $\tilde{P}_i$ correspond to rows $\{1,\ldots,\alpha\}$ and $\{\alpha+1,\ldots,\ell\}$ of matrix P_i respectively. Matrix $V_i \in \mathbb{F}_p^{\alpha\times\alpha}$ is a Vandermonde matrix and is invertible whenever vector W_i contains pairwise different non-zero elements from $\mathbb{F}_p$, else W_i is non-invertible which happens with probability at most α^2/p (each of the elements w_{ij} is zero or identical to another element with probability at most α/p). Whenever the matrix V_i is invertible source $\mathcal{S}_i$ solves equation (7) to find L_i and substitutes it into matrix M_i. When the matrix V_i is non-invertible then L_i is substituted with the zero matrix.

Linear Coding: Once matrices M_1, M_2 are formed then both sources and the internal nodes perform random linear network coding operations and therefore sink t gets

$$\begin{aligned} Y &= T_1M_1 + T_2M_2 + T_zZ \\ \Leftrightarrow Y &= \begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix} \begin{bmatrix} M_1 \\ -- \\ M_2 \\ -- \\ Z \end{bmatrix} \end{aligned} \tag{8}$$

where $T_i \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2}\times R_i}$ and $T_z \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2}\times z}$.

Decoding: Assume that matrix $Y \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2}\times\ell}$ has column rank equal to r and matrix $Y^s \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2}\times r}$ contains r linearly independent columns of Y. Since all the columns of Y can be written as linear combinations of columns of Y^s, then $Y = Y^sF$ where $F \in \mathbb{F}_p^{r\times\ell}$. The columns of M_1, M_2 and Z corresponding to those in Y^s are denoted as $M_1^s \in \mathbb{F}_p^{R_1\times r}$, $M_2^s \in \mathbb{F}_p^{R_2\times r}$ and $Z^s \in \mathbb{F}_p^{z\times r}$ respectively.

Therefore

$$Y^s = \begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix} \begin{bmatrix} M_1^s \\ -- \\ M_2^s \\ -- \\ Z^s \end{bmatrix} \tag{9}$$

and by using equations (8), (9) we have

$$Y = Y^s F \underset{(9)}{\overset{(8)}{\Rightarrow}} \begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix} \begin{bmatrix} M_1 \\ -- \\ M_2 \\ -- \\ Z \end{bmatrix} = \begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix} \begin{bmatrix} M_1^s \\ -- \\ M_2^s \\ -- \\ Z^s \end{bmatrix} F.$$

Therefore $M_1 = M_1^s F$ and $M_2 = M_2^s F$ since for large enough p, matrix $\begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix}$ is invertible with high probability [9]. Consequently, equation (7) can be written as $M_1^s(FP_1) = H_1$ where matrices F, P_1 and H_1 are known and matrix M_1^s is unknown and can be found using standard Gaussian elimination.

As in [9] it can be proved that the solution obtained by the Gaussian elimination is with high probability the unique solution to equation $M_1 P_1 = H_1$. Indeed, using Claim 5 of [9], for any $\hat{M}_1^s \neq M_1^s$ the probability (over $w_{11}, \ldots, w_{1\alpha}$) that $\hat{M}_1^s(FP_1) = H_1$ is at most $\left(\frac{\ell}{p}\right)^{\alpha}$. Since there are $p^{R_1 \cdot r}$ different matrices $\hat{M}_1$ ($\hat{M}_1 = \hat{M}_1^s F$ and $\hat{M}_1^s \in \mathbb{F}_p^{R_1 \times r}$) by taking the union bound over all different $\hat{M}_1$ (Corollary 6 in [9]) we conclude that the probability of having more than one solution for equation $M_1 P_1 = H_1$ is at most $p^{R_1 \cdot m_{\mathcal{S}_1, \mathcal{S}_2}} \left(\frac{\ell}{p}\right)^{\alpha} < \frac{\ell^{\alpha}}{p}$. Decoding of X_2 is similar.

Probability of error analysis: In order for the decoding to fail one or more of the following three events should occur:

1) At least one of the network transform matrices $\begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix}$ is not full column rank. According to [17], this happens with probability less than $\binom{|\mathcal{E}|}{z} \frac{|\mathcal{E}||\mathcal{T}|}{p}$, where $|\mathcal{E}|$, $|\mathcal{T}|$ is the number of edges and the number of sinks in the network. Term $\binom{|\mathcal{E}|}{z}$ is the number of different sets of z links the adversary can attack and $\frac{|\mathcal{E}|}{p}$ is an upper bound for the probability that matrix $\begin{bmatrix} T_1 & T_2 & T_z \end{bmatrix}$ is not full column rank when the adversary has attacked a specific set of links.

2) Either of the Vandermonde matrices V_1 or V_2 are not invertible. By using the union bound this happens with probability at most $2\alpha^2/p$.
3) There are more than one solutions for equations $\hat{M}_i^s(FP_i) = H_i$ for $i \in \{1, 2\}$. This happens with probability at most $2\ell^\alpha/p = 2\ell^{(m^2_{\mathcal{S}_1,\mathcal{S}_2}+1)}/p$.

Hence, it is not difficult to see that the probability of decoding failure can be made arbitrarily small as the size p of the finite field increases. Moreover increasing ℓ without bound we can approach any point inside the rate-region. The decoding complexity of the algorithm is dominated by the complexity of the Gaussian elimination that is $O(\ell m^3_{\mathcal{S}_1,\mathcal{S}_2})$.

VII. Omniscient Adversarial Model

A. General approach

In this section we construct capacity-achieving codes for the multiple-source multicast non-coherent network scenario. We use the algebraic framework of subspace codes developed in [11], which provides a useful tool for network error and erasure correction over general unknown networks. In Section V-D, we gave basic concepts and definitions of subspace network codes needed for further discussion.

In the proof of Theorem 2 we show how to design non-coherent network codes that achieve upper bounds given by (4) when a minimum (or bounded) injection distance decoder is used at the sink nodes. Our code construction uses random linear network coding at intermediate nodes, single-source network error-correction capacity-achieving codes at each source, and an overall global coding vector. Our choice of decoder relies on the observation that subspace erasures are not arbitrarily chosen by the adversary, but also depend on the network code. Since, as we show below, with high probability in a random linear network code, subspace erasures do not cause confusion between transmitted codewords, the decoder focuses on the discrepancy between the sent and the received codewords caused by subspace errors. The error analysis shows that injection distance decoding succeeds with high probability over the random network code. On the other hand, the subspace minimum distance of the code is insufficient to account for the total number of subspace errors and erasures that can occur. This is in contrast to constant dimension single-source codes, where subspace distance decoding is equivalent to injection distance decoding [22].

Proof of Theorem 2: Converse: The proof is similar to the converse of the proof of Theorem 1 with the exception that after connecting any subset of sources $\mathcal{S}' \subseteq \mathcal{S}$ by a virtual super-source node $w_{\mathcal{S}'}$, we apply the network Singleton bound [6] to $w_{\mathcal{S}'}$ for each $\mathcal{S}' \subseteq \mathcal{S}$.

From the three probability events the third one dominates the other two when packet size is large.

Achievability: 1) *Code construction:* Consider any rate vector $(R_1, \ldots, R_s)$ such that

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} R_i < m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{10}$$

Let each $\mathcal{C}_i$, $i = 1, \ldots, s$ be a code consisting of codewords that are k_i-dimensional linear subspaces. The codeword transmitted by source $\mathcal{S}_i$ is spanned by the packets transmitted by $\mathcal{S}_i$. From the single source case, for each source $i = 1, \ldots, s$ we can construct a code $\mathcal{C}_i$ where

$$k_i > R_i + z \tag{11}$$

that corrects any z additions [9]. This implies that by [21], $\mathcal{C}_i$ has minimum subspace distance greater than $2z$, i.e. for any pair of distinct codewords V_i, $V_i' \in \mathcal{C}_i$

$$d_S(V_i, V_i') = \dim(V_i) + \dim(V_i') - 2\dim(V_i \cap V_i') > 2z.$$

Hence,

$$\dim(V_i \cap V_i') < k_i - z \quad \forall \ V_i, V_i' \in \mathcal{C}_i. \tag{12}$$

By (11), we have:

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i > \sum_{i \in \mathcal{I}(\mathcal{S}')} R_i + |\mathcal{S}'|z.$$

Therefore, by combining it with (10) and scaling all source rates and link capacities by a sufficiently large integer if necessary, we can assume without loss of generality that we can choose k_i satisfying

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i \leq m_{\mathcal{S}'} + (|\mathcal{S}'| - 2)z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{13}$$

We can make vectors from one source linearly independent of vectors from all other sources by prepending a length–$(\sum_{i \in \mathcal{I}(\mathcal{S})} k_i)$ global encoding vector, where the jth global encoding vector, $j = 1, 2, \ldots, \sum_{i \in \mathcal{I}(\mathcal{S})} k_i$, is the unit vector with a single nonzero entry in the jth position. This adds an overhead that becomes asymptotically negligible as packet length grows. This ensures that

$$\dim(V_i \cap V_j) = 0 \ \forall i \neq j, V_i \in \mathcal{C}_i, V_j \in \mathcal{C}_j. \tag{14}$$

Error analysis: Let $X \in \mathcal{C}_{\mathcal{S}}$ be the sent codeword, and let R be the subspace received at a sink. Consider any $\mathcal{S}' \subseteq \mathcal{S}$. Let $\overline{\mathcal{S}'} = \mathcal{S} \backslash \mathcal{S}'$. Let $X = V \oplus W$, where $V \in \mathcal{C}_{\mathcal{S}'}, W \in \mathcal{C}_{\overline{\mathcal{S}}'}$ and V is spanned by the codeword V_i from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. We will show that with high probability over the random network code, there does not exist another codeword $Y = V' \oplus W$, such that V' is spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$, which could also have produced R under arbitrary errors on up to z links in the network.

Fix any sink t. Let $\mathcal{R}$ be the set of packets (vectors) received by t, i.e. R is the subspace spanned by $\mathcal{R}$. Each of the packets in $\mathcal{R}$ is a linear combination of vectors from V and W and error vectors, and can be expressed as $\mathbf{p} = \mathbf{u_p} + \mathbf{w_p}$, where $\mathbf{w_p}$ is in W and the global encoding vector of $\mathbf{u_p}$ has zero entries in the positions corresponding to sources in set $\mathcal{I}(\overline{\mathcal{S}'})$.

The key idea behind our error analysis is to show that with high probability subspace deletions do not cause confusion, and that more than z additions are needed for X be decoded wrongly at the sink, i.e we will show that

$$d_I(R, V' \oplus W) = \dim(R) - \dim(R \cap (V' \oplus W)) > z.$$

Let $P = \text{span}\{\mathbf{u_p} : \ \mathbf{p} \in \mathcal{R}\}$. Let M be the matrix whose rows are the vectors $\mathbf{p} \in \mathcal{R}$, where the jth row of M corresponds to the jth vector $\mathbf{p} \in \mathcal{R}$. Similarly, let $M_{\mathbf{u}}$ be the matrix whose jth row is the vector $\mathbf{u_p}$ corresponding to the jth vector $\mathbf{p} \in \mathcal{R}$, and let $M_{\mathbf{w}}$ be the matrix whose jth row is the vector $\mathbf{w_p}$ corresponding to the jth vector $\mathbf{p} \in \mathcal{R}$. Consider matrices A, B such that the rows of $AM_{\mathbf{u}}$ form a basis for $P \cap V'$ and, together with the rows of $BM_{\mathbf{u}}$, form a basis for P. The linear independence of the rows of $\begin{bmatrix} AM_{\mathbf{u}} \\ BM_{\mathbf{u}} \end{bmatrix}$ implies that the rows of $\begin{bmatrix} AM \\ BM \end{bmatrix}$ are also linearly independent, since otherwise there would be a nonzero matrix D such that

$$D \begin{bmatrix} AM \\ BM \end{bmatrix} = 0 \Rightarrow D \begin{bmatrix} AM_{\mathbf{w}} \\ BM_{\mathbf{w}} \end{bmatrix} = 0$$
$$\Rightarrow D \begin{bmatrix} AM_{\mathbf{u}} \\ BM_{\mathbf{u}} \end{bmatrix} = 0,$$

a contradiction. For $\mathbf{w_p}$ in W, $\mathbf{u_p} + \mathbf{w_p}$ is in $V' \oplus W$ only if $\mathbf{u_p}$ is in V', because the former implies $\mathbf{u_p} = \mathbf{u_p} + \mathbf{w_p} - \mathbf{w_p}$ is in $V' \oplus W$ and since $\mathbf{u_p}$ has zero entries in the positions of the global encoding vector corresponding to $\mathcal{I}(\overline{\mathcal{S}'})$ it must be in V'. Thus, since any vector in the row space of $BM_{\mathbf{u}}$ is not in

V', any vector in the row space of BM is not in $V' \oplus W$. Since the row space of BM is a subspace of R, it follows that the number of rows of B is equal to $\dim(P) - \dim(P \cap V')$ and is less than or equal to $\dim(R) - \dim(R \cap (V' \oplus W))$. Therefore,

$$\begin{aligned} d_I(R, V' \oplus W) &= \dim(R) - \dim(R \cap (V' \oplus W)) \\ &\geq \dim(P) - \dim(P \cap V'). \end{aligned} \tag{15}$$

We next show that for random linear coding in a sufficiently large field, with high probability

$$\dim(P) - \dim(P \cap V') > z \tag{16}$$

for all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Consider first the network with each source i in $\mathcal{S}'$ transmitting k_i linearly independent packets from V_i, sources in $\overline{\mathcal{S}'}$ silent, and no errors. From the maxflow-mincut bound, any rate vector $(h_1, \ldots, h_{|\mathcal{S}'|})$, such that

$$\sum_{i \in \mathcal{S}''} h_i \leq m_{\mathcal{S}''} \quad \forall \mathcal{S}'' \subseteq \mathcal{S}'$$

can be achieved. Combining this with (13), we can see that in the error-free case, each $s_i \in \mathcal{S}'$ can transmit information to the sink at rate $k_i - \frac{(|\mathcal{S}'|-2)z}{|\mathcal{S}'|}$ for a total rate of

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z. \tag{17}$$

With sources in $\overline{\mathcal{S}'}$ still silent, consider the addition of z unit-rate sources corresponding to the error links. The space spanned by the received packets corresponds to P. Consider any V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Let Z be the space spanned by the error packets, and let $z' \leq z$ be the minimum cut between the error sources and the sink. Let $P = P_V \oplus P_Z$, where $P_Z = P \cap Z$ and P_V is a subspace of V. There exists a routing solution, which we distinguish by adding tildes in our notation, such that $\dim \tilde{P}_Z = z'$ and, from (17), $\dim \tilde{P} \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z$, so

$$\dim(\tilde{P}_V) \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z - z'. \tag{18}$$

Note that, by (14), a packet from V_i is not in any $V_j' \in \mathcal{C}_j, j \neq i$, and hence is in V' if and only if it is in V_i'. Therefore, by (12)

$$\dim(\tilde{P}_V \cap V') \leq \sum_{i \in \mathcal{I}(\mathcal{S}')} \dim(V_i \cap V_i') < \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - |\mathcal{S}'|z.$$

Therefore, using (18) we have

$$\begin{aligned}
\dim(\tilde{P}_V \cup V') &= \dim(\tilde{P}_V) + \dim(V') - \dim(\tilde{P}_V \cap V') \\
&> \dim(\tilde{P}_V) + \dim(V') + |\mathcal{S}'|z - \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i \\
&\geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z - z' + |\mathcal{S}'|z \\
&= \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + 2z - z' \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z.
\end{aligned}$$

Then

$$\dim(\tilde{P} \cup V') > \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z.$$

For random linear coding in a sufficiently large field, with high probability by its generic nature

$$\dim(P \cup V') \geq \dim(\tilde{P} \cup V') > \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z,$$

and this also holds for any z or fewer errors, all sinks, and all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. Then, (16) follows by

$$\dim(P) - \dim(P \cap V') = \dim(P \cup V') - \dim(V').$$

Hence, using (16) and (15),

$$\begin{aligned}
d_I(R, V' \oplus W) &= \dim(R) - \dim(R \cap (V' \oplus W)) \\
&\geq \dim(P) - \dim(P \cap V') > z.
\end{aligned}$$

Thus, more than z additions are needed to produce R from $Y = V' \oplus W$. By the generic nature of random linear coding, with high probability this holds for any $\mathcal{S}'$. Therefore, at every sink the minimum injection distance decoding succeeds with high probability over the random network code.

Decoding complexity: Take any achievable rate vector $(R_1, R_2, \ldots, R_s)$. For each $i = 1, \ldots, s$, S_i can transmit at most $p^{R_i \ell}$ independent symbols. Decoding can be done by exhaustive search, where the decoder checks each possible set of codewords to find the one with minimum distance from the observed set of packets, therefore, the decoding complexity of the minimum injection distance decoder is upper bounded by $O(p^{l \sum_{i=1}^{s} R_i})$. ■

B. Polynomial-time construction

Similar to the side-channel model, we will describe the code for the case where there are only two sources $\mathcal{S}_1, \mathcal{S}_2 \in \mathcal{V}$ transmitting information to one sink $t \in \mathcal{V}$, since the extension of our results to more sources and sinks is straightforward and analyzed briefly in Section VIII. To further simplify the discussion we show the code construction for rate-tuple (R_1, R_2) satisfying $R_1 \leq m_{\mathcal{S}_1} - 2z$, $R_2 \leq m_{\mathcal{S}_2} - 2z$, $R_1 + R_2 + 2z = m_{\mathcal{S}_1, \mathcal{S}_2}$ and exactly $m_{\mathcal{S}_1, \mathcal{S}_2}$ edges incident to sink t (if more do, redundant information can be discarded).

Encoding: Each source $\mathcal{S}_i$, $i \in \{1, 2\}$, organizes its information into a matrix $X_i \in \mathbb{F}_p^{R_i \times knN}$ with elements from $\mathbb{F}_p$, where $n = R_1 + 2z$, $N = R_2 + 2z$ and k is an integer (and a network parameter). In order to correct adversarial errors, redundancy is introduced through the use of Gabidulin codes (see Section V-E for details).

More precisely the information of $\mathcal{S}_1$ can be viewed as a matrix $X_1 \in \mathbb{F}_q^{R_1 \times kN}$, where $\mathbb{F}_q$ is an algebraic extension of $\mathbb{F}_p$ and $q = p^n$ (see Section V-C for details). Before transmission X_1 is multiplied with a generator matrix, $G_1 \in \mathbb{F}_q^{n \times R_1}$, creating $G_1 X_1 \in \mathbb{F}_q^{n \times kN}$ whose unfolded version $M_1' = (G_1 X_1)^u$ is a matrix in $\mathbb{F}_p^{n \times knN}$. The information of $\mathcal{S}_2$ can be viewed as a matrix $X_2 \in \mathbb{F}_Q^{R_2 \times k}$, where $\mathbb{F}_Q$ is an algebraic extension of $\mathbb{F}_q$ where $Q = q^N = p^{nN}$. Before transmission X_2 is multiplied with a generator matrix, $G_2 \in \mathbb{F}_Q^{N \times R_2}$, creating $G_2 X_2 \in \mathbb{F}_Q^{N \times k}$ whose unfolded version $M_2' = (G_2 X_2)^u$ over $\mathbb{F}_p$ is a matrix in $\mathbb{F}_p^{N \times knN}$. Both G_1 and G_2 are chosen as generator matrices for Gabidulin codes and have the capability of correcting errors of rank at most z over $\mathbb{F}_p$ and $\mathbb{F}_q$ respectively.

In the scenario where sink t does not know T_1 and T_2 *a priori* the two sources append headers on their transmitted packets to convey information about T_1 and T_2 to the sink. Thus source $\mathcal{S}_1$ constructs message matrix $M_1 = \begin{bmatrix} I_n & O & M_1' \end{bmatrix}$ with the zero matrix O having dimensions $n \times N$, and source $\mathcal{S}_2$ constructs a message matrix $\begin{bmatrix} O & I_N & M_2' \end{bmatrix}$ with the zero matrix O having dimension $N \times n$. Each row of matrices M_1, M_2 is a packet of length $\ell = knN + n + N$.

Before we continue with the decoding we need to prove the following two Lemmas:

Lemma 1. *Folding a matrix does not increase its rank.*

Proof: Let matrix $H \in \mathbb{F}_p^{m \times kn}$ has rank$(H) = r$ in field $\mathbb{F}_p$. Thus $H = WZ$, where $Z \in \mathbb{F}_p^{r \times kn}$ is of full row rank and $W \in \mathbb{F}_p^{m \times r}$ is of full column rank. After the folding operation H becomes $H^f = WZ^f$ and therefore has rank in the extension field $\mathbb{F}_q$, where $q = p^n$, is at most r, *i.e.* rank$(H^f) \leq r$. ■

Lemma 2. *Matrix* $\begin{bmatrix} T_1 G_1 & T_2 \end{bmatrix} \in \mathbb{F}_q^{m_{\mathcal{S}_1,\mathcal{S}_2} \times m_{\mathcal{S}_1,\mathcal{S}_2}}$ *is invertible with probability at least* $1 - |\mathcal{E}|/p$.

Proof: Let $\mathcal{X}$ be the set of random variables over $\mathbb{F}_p$ comprised of the local coding coefficients used in the random linear network code. Thus the determinant of $\begin{bmatrix} T_1 G_1 & T_2 \end{bmatrix}$ is a polynomial $\mathbf{f}(\mathcal{X})$ over $\mathbb{F}_q$ of degree at most $|\mathcal{E}|$ (see Theorem 1 in [17] for details). Since the variables $\mathcal{X}$ in $\mathbf{f}(\mathcal{X})$ are evaluated over $\mathbb{F}_p$, $\mathbf{f}(\mathcal{X})$ is equivalent to a vector of polynomials $(f_1(\mathcal{X}), f_2(\mathcal{X}), \ldots, f_n(\mathcal{X}))$, where $f_i(\mathcal{X}) \in \mathbb{F}_p[\mathcal{X}]$ is a polynomial over $\mathbb{F}_p$ with variables in $\mathcal{X}$. Note that $f_i(\mathcal{X})$ also has degree no more than $|\mathcal{E}|$ for each $i \in \{1, \ldots, n\}$. Thus once we prove that there exists an evaluation of $\mathcal{X}$ such that $\mathbf{f}$ is a nonzero vector over $\mathbb{F}_p$, we can show that matrix $\begin{bmatrix} T_1 G_1 & T_2 \end{bmatrix}$ is invertible with probability at least $1 - |\mathcal{E}|/p$ by the Schwartz-Zippel lemma [24] (Proposition 98).

Since $R_1 + N = m_{\mathcal{S}_1,\mathcal{S}_2}$, $R_1 \leq m_{\mathcal{S}_1}$ and $N \leq m_{\mathcal{S}_2}$, there exist $R_1 + N$ edge-disjoint-paths:$\mathcal{P}_1^1, \mathcal{P}_2^1, \ldots, \mathcal{P}_{R_1}^1$ from $\mathcal{S}_1$ to t and $\mathcal{P}_1^2, \mathcal{P}_2^2, \ldots, \mathcal{P}_N^2$ from $\mathcal{S}_2$ to t. The variables in $\mathcal{X}$ are evaluated in the following manner:

1) Let O be the zero matrix in $F_q^{n \times N}$. We choose the variables in $\mathcal{X}$ so that the R_1 independent rows of $\begin{bmatrix} G_1 & O \end{bmatrix} \in \mathbb{F}_q^{n \times m_{\mathcal{S}_1,\mathcal{S}_2}}$ correspond to routing information from $\mathcal{S}_1$ to t via $\mathcal{P}_1^1, \ldots, \mathcal{P}_{R_1}^1$.
2) Let $\{\mathbf{u}_{R_1+1}, \mathbf{u}_{R_1+2}, \ldots, \mathbf{u}_{m_{\mathcal{S}_1,\mathcal{S}_2}}\}$ be N distinct rows of the identity matrix in $\mathbb{F}_q^{m_{\mathcal{S}_1,\mathcal{S}_2} \times m_{\mathcal{S}_1,\mathcal{S}_2}}$ such that for each $i \in \{1, \ldots, N\}$, $\mathbf{u}_{R_1+i}$ has the element 1 located at position $R_1 + i$. Then these N vectors correspond to routing information from $\mathcal{S}_2$ to sink t via $\mathcal{P}_1^2, \mathcal{P}_2^2, \ldots, \mathcal{P}_N^2$.

Under such evaluations of the variables in $\mathcal{X}$, matrix $\begin{bmatrix} T_1 G_1 & T_2 \end{bmatrix}$ equals $\begin{bmatrix} G_1' & O \\ O & I_N \end{bmatrix}$, where $G_1' \in \mathbb{F}_q^{R_1 \times R_1}$ consists of the R_1 independent rows of G_1. Hence $\mathbf{f}$ is non-zero. Using the Schwartz-Zippel Lemma $\mathbf{f} \neq 0$ and thus $\begin{bmatrix} T_1 G_1 & T_2 \end{bmatrix}$ is invertible with probability at least $1 - |\mathcal{E}|/p$ over the choices of $\mathcal{X}$. ■

Decoding: The two message matrices M_1, M_2 along with the packets inserted by the adversary are transmitted to sink t through the network with the use of random linear network coding (see Section V-B)

and therefore sink t gets:

$$\begin{aligned} Y &= T_1 M_1 + T_2 M_2 + T_z Z \\ \Leftrightarrow Y &= \begin{bmatrix} Y_1 & Y_2 & Y_3 \end{bmatrix} = \begin{bmatrix} T_1 & T_2 & A \end{bmatrix} + E, \end{aligned} \tag{19}$$

where $A = T_1 M_1' + T_2 M_2' \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2} \times knN}$ and $E \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2} \times \ell}$ has rank no more than z over field $\mathbb{F}_p$. Let $E = \begin{bmatrix} E_1 & E_2 & E_3 \end{bmatrix}$, where $E_1 \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2} \times n}$, $E_2 \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2} \times N}$ and $E_3 \in \mathbb{F}_p^{m_{\mathcal{S}_1,\mathcal{S}_2} \times knN}$. Sink t will first decode M_2 and then M_1.

Stage 1: Decoding X_2: Let $Y_a = \begin{bmatrix} Y_1 G_1 & Y_2 & Y_3^f \end{bmatrix}$ be a matrix in $\mathbb{F}_q^{m_{\mathcal{S}_1,\mathcal{S}_2} \times (R_1 + N + kN)}$. To be precise:

$$Y_a = \begin{bmatrix} T_1 G_1 & T_2 & A^f \end{bmatrix} + \begin{bmatrix} E_1 G_1 & E_2 & E_3^f \end{bmatrix}. \tag{20}$$

Sink t uses invertible row operations over $\mathbb{F}_q$ to transform Y_a into a row-reduced echelon matrix $\begin{bmatrix} T_{RRE} & M_{RRE} \end{bmatrix}$ that has the same row space as Y_a, where T_{RRE} has $m_{\mathcal{S}_1,\mathcal{S}_2} = R_1 + N$ columns and M_{RRE} has kN columns. Then the following propositions are from the results proved in [8]:

Proposition 2. 1) *The matrix $\begin{bmatrix} T_{RRE} & M_{RRE} \end{bmatrix}$ takes the form $\begin{bmatrix} T_{RRE} & M_{RRE} \end{bmatrix} = \begin{bmatrix} I_C + \hat{L} U_\mu^T & r \\ O & \hat{E} \end{bmatrix}$, where $U_\mu \in \mathbb{F}_q^{C \times \mu}$ comprises of μ distinct columns of the $C \times C$ identity matrix such that $U_\mu^T r = 0$ and $U_\mu^T \hat{L} = -I_\mu$. In particular, $\hat{L}$ in $\mathbb{F}_q^{C \times \mu}$ is the "error-location matrix", $r \in \mathbb{F}_q^{C \times kN}$ is the "message matrix", and $\hat{E} \in \mathbb{F}_q^{\delta \times kN}$ is the "known error value" (and its rank is denoted δ).*

2) *Let $X = \begin{bmatrix} X_1 \\ M_2^f \end{bmatrix}$ and $e = r - X$ and $\tau = rank \begin{bmatrix} \hat{L} & e \\ 0 & \hat{E} \end{bmatrix}$. Then $2\tau - \mu - \delta$ is no more than $d_S(\left\langle \begin{bmatrix} T_{RRE} & M_{RRE} \end{bmatrix} \right\rangle, \left\langle \begin{bmatrix} I_{m_{\mathcal{S}_1,\mathcal{S}_2}} & X \end{bmatrix} \right\rangle)$, i.e., the subspace distance between $\left\langle \begin{bmatrix} T_{RRE} & M_{RRE} \end{bmatrix} \right\rangle$ and $\left\langle \begin{bmatrix} I_{m_{\{\mathcal{S}_1,\mathcal{S}_2\}}} & X \end{bmatrix} \right\rangle$.*

3) *There exist τ column vectors $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_\tau \in \mathbb{F}_q^C$ and τ row vectors $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_\tau \in \mathbb{F}_q^{1 \times kN}$ such that $e = \sum_{i \in [1,\tau]} \mathbf{L}_i \mathbf{E}_i$. In particular, $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_\mu$ are the columns of $\hat{L}$, and $\mathbf{E}_{\mu+1}, \mathbf{E}_{\mu+2}, \ldots, \mathbf{E}_{\mu+\delta}$ are the rows of $\hat{E}$.*

In the following subscript d stands for the last N rows of any matrix/vector. Then we show the following for our scheme.

Lemma 3. *1) Matrix $e_d = r_d - M_2^f$ can be expressed as $e_d = \sum_{i \in 1,2,\ldots,\tau} (\mathbf{L}_i)_d \mathbf{E}_i$, where $(\mathbf{L}_1)_d, (\mathbf{L}_2)_d, \ldots, (\mathbf{L}_\mu)_d$ are the columns of $\hat{L}_d$ and $\mathbf{E}_{\mu+1}, \mathbf{E}_{\mu+2}, \ldots, \mathbf{E}_{\mu+\delta}$ are the rows of $\hat{E}$.*

1) is from Prop. 7, 2) from Thm. 9, and 3) from Prop. 10 in [8].

2) *With probability at least* $1-|\mathcal{E}|/p$, $2\tau-\mu-\delta\leq 2z$

Proof: 1) It is a direct corollary from the third statement of Proposition 2.

2) Using the second statement of Proposition 2 it suffices to prove with probability at least $1-|\mathcal{E}|/p$, $d_S(\left\langle \begin{bmatrix} T_{RRE} & M_{RRE}\end{bmatrix}\right\rangle, \left\langle \begin{bmatrix} I_{m_{\mathcal{S}_1,\mathcal{S}_2}} & X\end{bmatrix}\right\rangle)\leq 2z$.

As shown in the proof of Lemma 1, the columns of E_3^f are in the column space of E_3 (and then of E) over $\mathbb{F}_q$. Thus $\begin{bmatrix} E_1 & E_2 & E_3^f\end{bmatrix}$ and therefore $\begin{bmatrix} E_1G_1 & E_2 & E_3^f\end{bmatrix}$ has rank at most equal to z over $\mathbb{F}_q$. Using Proposition 1 and (20), $d_S(\langle Y_a\rangle, \left\langle \begin{bmatrix} T_1G_1 & T_2 & A^f\end{bmatrix}\right\rangle)$ is no more than $2z$. Since $d_S(\left\langle \begin{bmatrix} T_{RRE} & M_{RRE}\end{bmatrix}\right\rangle, \langle Y_a\rangle)$ $=0$, we have $d_S(\left\langle \begin{bmatrix} T_{RRE} & M_{RRE}\end{bmatrix}\right\rangle, \left\langle \begin{bmatrix} T_1G_1 & T_2 & A^f\end{bmatrix}\right\rangle)\leq 2z$.

Using Lemma 2, matrix $D=\begin{bmatrix} T_1G_1 & T_2\end{bmatrix}$ is invertible with probability at least $1-|\mathcal{E}|/p$, so $\begin{bmatrix} I_{m_{\mathcal{S}_1,\mathcal{S}_2}} & X\end{bmatrix}$ has zero subspace distance from $\begin{bmatrix} D & DX\end{bmatrix}=\begin{bmatrix} T_1G_1 & T_2 & A^f\end{bmatrix}$. Thus,

$$d_S(\left\langle \begin{bmatrix} T_{RRE} & M_{RRE}\end{bmatrix}\right\rangle, \left\langle \begin{bmatrix} I_{m_{\mathcal{S}_1,\mathcal{S}_2}} & X\end{bmatrix}\right\rangle)\leq 2z.$$

■

In the end combining Lemma 3 and Theorem 3 sink t can take $(\hat{L}_d, \hat{E}, r)$ as the input for the Gabidulin decoding algorithm and decode X_2 correctly.

Stage 2: Decoding X_1*:* From (19) sink t gets $Y=\begin{bmatrix} T_1+E_1 & T_2+E_2 & A+E_3\end{bmatrix}$, computes $(T_2+E_2)M_2$, and then subtracts matrix $\begin{bmatrix} O & (T_2+E_2) & (T_2+E_2)M_2\end{bmatrix}$ from Y. The resulting matrix has N zero columns in the middle (column $n+1$ to column $n+N$). Disregarding these we get:

$$Y'=\begin{bmatrix} T_1 & T_1M_1\end{bmatrix}+\begin{bmatrix} E_1 & E_3-E_2M_2\end{bmatrix}.$$

The new error matrix $E'=\begin{bmatrix} E_1 & E_3-E_2M_2\end{bmatrix}$ has rank at most z over $\mathbb{F}_p$ since the columns of E' are simply linear combinations of columns of E whose rank is at most z. Therefore the problem degenerates into a single source problem and sink t can decode X_1 with probability at least $1-|\mathcal{E}|/p$ by following the approach in [8].

Summarizing the above decoding scheme for X_1 and X_2, we have the following main result:

Theorem 4. *Each* t *can efficiently decode the information from all sources correctly with probability at least* $1-|s||\mathcal{E}|/p$.

Decoding complexity: For both coherent and non-coherent cases the computational complexity of Gabidulin encoding and decoding of two source messages is dominated by the decoding of X_2, which

requires $\mathcal{O}(nNm_{\mathcal{S}}\ell \log(pnN))$ operations over $\mathbb{F}_p$ (see [8]).

To generalize our technique to more sources, consider a network with s sources $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_s$. Let R_i be the rate of $\mathcal{S}_i$ and $n_i = R_i + 2z$ for each $i \in [1, s]$. A straightforward generalization uses the multiple-field-extension technique so that $\mathcal{S}_i$ uses the generator matrix over finite field of size $p^{n_1 n_2 \ldots n_i}$. In the end the packet length must be at least $n_g = n_1 n_2 \ldots n_s$, resulting in a decoding complexity $\mathcal{O}(m_{\mathcal{S}} n_g^2 \log(pn_g))$ increasing exponentially in the number of sources s. Thus the multiple field-extension technique works in polynomial time only for a fixed number of sources.

Note that the intermediate nodes work in the base field $\mathbb{F}_p$ to perform random linear network coding. The multiple-field-extension is an end-to-end technique, *i.e.*, only the sources and sinks use the extended field.

C. Coherent case

Sections VI, VII-A and VII-B give code constructions for the non-coherent coding scenario. Note that a non-coherent coding scheme can also be applied in the coherent setting when the network is known. Hence, the capacity regions of coherent and non-coherent network coding for the same multi-source multicast network are the same. However, both the constructions of Sections VII-A and VII-B include an overhead of incorporating a global coding vector. Therefore, they achieve the outer bounds given by (4) only asymptotically in packet length. In contrast, in the coherent case, the full capacity region can be achieved exactly with packets of finite length, as shown in the following:

Proof of Theorem 2, coherent case achievability: We first construct a multi-source multicast network code $\mathcal{C}$ for $\mathcal{G}$ that can correct any $2z$ errors with known locations, called erasures in [25]. We can use the result of [26] for multi-source multicast network coding in an alternative model where on each link either an erasure symbol or error-free information is received, by observing the following correspondence between the two models. We form a graph $\mathcal{G}'$ by replacing each link l in $\mathcal{G}$ with two links in tandem with a new node v_l between them, and adding an additional source node u of rate $2z$ connected by a new link k_l to each node v_l. We use the result from [26] to obtain a multi-source network code that achieves a given rate vector under any pattern of erasure symbols such that the maxflow-mincut conditions are satisfied for every subset of sources in $\mathcal{G}'$. In particular, if erasure symbols (by the definition of [26]) are received on all but $2z$ of the new links k_l (corresponding to $2z$ erasures in $\mathcal{G}$ by the definition of [25]), all the original sources can be decoded.

Let $l_{i,j}, j = 1, \ldots, n_i$, be the outgoing links of each source $s_i, i = 1, \ldots, n$. Next, we construct the graph $\mathcal{G}_{\mathcal{S}}$ from $\mathcal{G}$ by adding a virtual super source node w, and n_i links $l'_{i,j}, j = 1, \ldots, n_i$, from w to each source s_i. Then the code $\mathcal{C}$ for the multi-source problem corresponds to a single-source network code $\mathcal{C}_{\mathcal{S}}$ on $\mathcal{G}_{\mathcal{S}}$ where the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}_{\mathcal{S}'}$ and $\mathcal{G}_{\mathcal{S}}$.

By [25] the following are equivalent in the single-source case:

1) a linear network code has network minimum distance at least $2z + 1$
2) the code corrects any error of weight at most z
3) the code corrects any erasure of weight at most $2z$.

This implies that $\mathcal{C}_{\mathcal{S}}$ has network minimum distance at least $2z+1$, and so it can correct any z errors. ■

VIII. Extension to more than two sources

When there are more than two sources the extension of our encoding and decoding techniques is straightforward both for the case of the side-channel and the omniscient model, and up to this point we have focused on the case of two sources simply for notational convenience. To clarify how our techniques can extend to multiple sources we will outline the encoding and decoding for an arbitrary number of sources equal to s and use results from the previous sections.

Side-channel model: For the case of the side-channel model each source encodes its data $X_i \in \mathbb{F}_p^{R_i \times (\ell - \alpha)}$, $i \in \{1, \ldots, s\}$, in a matrix $M_i = \begin{bmatrix} L_i & X_i \end{bmatrix}$ where $L_i \in \mathbb{F}_p^{R_i \times \alpha}$ will be such so that equation $H_i = M_i P_i$ holds. Source $\mathcal{S}_i$ shares with the receiver/receivers the random matrix $H_i \in \mathbb{F}_p^{R_i \times \alpha}$ along with the random vector $W_i = \begin{bmatrix} r_{i1} & r_{i2} & \ldots & r_{i\alpha} \end{bmatrix}$. The vector W_i defines matrix $P_i \in \mathbb{F}_p^{\ell \times \alpha}$ since its $(m, n) -$ th entry equals $(r_{in})^m$. Every receiver follows the decoding steps described in Section VI and gets equations $M_i P_i = M_i^s (F H_i) = H_i$, $i \in \{1, \ldots, s\}$, that can be solved with high probability using Gaussian elimination.

Omniscient model: For the case of the omniscient adversary we will need to extend the field we work with s times. Assume that $n_i = R_i + 2z$ and the information from source $\mathcal{S}_i$ is organized into a matrix $X_i \in \mathbb{F}_p^{R_i \times k n_1 \ldots n_s}$. Before transmission matrix X_i, $i \in \{1, \ldots, s-1\}$, is viewed as matrix $X_i \in \mathbb{F}_{p_i}^{R_i \times k n_{i+1} \ldots n_s}$ in the larger field $\mathbb{F}_{p_i}$ where $p_i = p^{n_1 \ldots n_i}$ and X_s is viewed as a matrix $X_s \in \mathbb{F}_{p_s}^{R_s \times k}$ where $p_s = p^{n_1 \ldots n_s}$. Each matrix X_i is multiplied with a generator matrix $G_i \in \mathbb{F}_{p_i}^{n_i \times R_i}$, creating $G_i X_i$ whose unfolded version $M'_i = (G_i X_i)^u$ is a matrix in $\mathbb{F}_p^{n_i \times k n_1 \ldots n_s}$. All matrices G_i are chosen as generator matrices for Gabidulin codes and have the capability of correcting errors of rank at most z over field $\mathbb{F}_{p_i}$.

Source $\mathcal{S}_1$ create the message matrix M_1 by appending some header to M_1', specifically the message is $M_1 = \begin{bmatrix} I_{n_1} & O_{n_1\times n_2} & \dots & O_{n_1\times n_s} & M_1' \end{bmatrix}$ where I_{n_1} is the identity matrix with dimensions $n_1 \times n_1$ and $O_{n_i\times n_j}$ is the zero matrix with dimensions $n_i \times n_j$. Similarly $M_2 = \begin{bmatrix} O_{n_2\times n_1} & I_{n_2} & \dots & O_{n_2\times n_s} & M_2' \end{bmatrix}, \dots,$ $M_s = \begin{bmatrix} O_{n_s\times n_1} & O_{n_s\times n_2} & \dots & I_{n_s} & M_s' \end{bmatrix}$ and therefore the packet length is $\ell = \sum_{i=1}^{s} n_i + k\prod_{i=1}^{s} n_i$ over $\mathbb{F}_p$ the base field of network coding.

Similar to equation (19) the received matrix can be written as

$$\begin{aligned} Y &= T_1M_1 + \ldots + T_sM_s + T_zZ \\ \Leftrightarrow Y &= \begin{bmatrix} Y_1 & \dots & Y_s & Y_{s+1} \end{bmatrix} = \begin{bmatrix} T_1 & \dots & T_s & A' \end{bmatrix} + E \end{aligned}$$

where $A' = T_1M_1' + \ldots + T_sM_s'$ and $E \in \mathbb{F}_p^{m_{\mathcal{S}}\times \ell}$ has rank no more than z over field $\mathbb{F}_p$. For the decoding of information from source $\mathcal{S}_s$ we form the matrix $Y_\alpha' = \begin{bmatrix} Y_1G_1 & \dots & Y_{s-1}G_{s-1} & Y_s & Y_{s+1}^f \end{bmatrix}$ and transform it to a row-reduced echelon form as in Proposition 2. Since matrix $D' = \begin{bmatrix} T_1G_1 & \dots & T_{s-1}G_{s-1} & T_s \end{bmatrix}$ is invertible with high probability similar to Lemma 2 one can use Lemma 3 and decode X_s. By subtracting $\begin{bmatrix} O_{m_{\mathcal{S}}\times n_1} & \dots & O_{m_{\mathcal{S}}\times n_{s-1}} & Y_s & Y_sM_s' \end{bmatrix}$ from Y the problem reduces to $s-1$ number of sources and one can solve it recursively.

IX. Comparison of our code constructions

TABLE II
Comparison of performance metrics of the code constructions given in Sections VI, VII-A and VII-B for any achievable rate vector $(R_1, R_2, \dots, R_s)$

	decoding complexity	packet length
Side-channel model	$O(\ell m_{\mathcal{S}}^3)$	$\Theta(m_{\mathcal{S}}^2)$
Omniscient adversary: subspace codes	$O(p^{lm_{\mathcal{S}}})$	$\Theta(m_{\mathcal{S}})$
Omniscient adversary: field extension codes	$O(m_{\mathcal{S}}^{2s+1}\log(pm_{\mathcal{S}}^s))$	$\Theta(\prod_{i=1}^{s} m_{\mathcal{S}_i})$

In this section we compare some performance metrics of the code constructions given in Sections VI, VII-A and VII-B. For convenience, Table II summarizes the requirements on the decoding complexity and the packet length for each of the achievable schemes. For clarity of comparison, we approximate all quantities presented in Table II; the exact expressions are derived in the corresponding sections.

Based on Table II, we can make the following observations about the practicality of our constructions:

- If the secret channel is available, one should use the side-channel model construction since it not only achieves higher rates but also provides lower decoding complexity.

- Multiple-field extension codes have computational complexity that is polynomial in all network parameters, but exponential in the number of sources. Therefore, they are preferable when the number of sources is small.
- Random subspace codes become beneficial compared to multiple-field extension codes as the number of sources grows.

X. Conclusion

In this work we consider the problem of communicating messages from multiple sources to multiple sinks over a network that contains a hidden malicious adversary who observes and attempts to jam communication. We consider two models. In the first model, the sources share a small secret (that is unknown to the adversary) with the sink(s). In the second model, this resource is unavailable – no limitations on the adversary's knowledge are assumed. We prove upper bounds on the set of achievable rates in these settings. Since more resources are available to the honest parties in the first model, the rate-region corresponding to the upper bounds in the first model is larger than that in the second model. We also provide novel algorithms that achieve any point in the rate-regions corresponding to the two models. Our codes for the first model have computational complexity that is polynomial in network parameters. For the second model we have two algorithms. In our codes based on random subspace design, all sources code over the same field, and decoding is based on minimum injection distance. Our codes based on multiple-field extension have computational complexity that is polynomial in all network parameters, but exponential in the number of sources.

Our codes are end-to-end and decentralized – each interior node is oblivious to the presence of an adversary, and merely performs random linear network coding. They also do not require prior knowledge of the network topology or coding operations by any honest party. They work in the presence of a computationally unbounded adversary, even one who knows the network topology and coding operations and can decide where and how to jam the network on the basis of this information.

A problem that remains open is that of computationally efficient codes for the omniscient adversarial case with a large number of sources. This may require new insights in algebraic code design.

Besides multi-source multicast, our codes have implications for the much more common scenario of multiple unicasts. One class of codes (that is not rate-optimal) for this problem assumes that each sink treats information that it is uninterested in as noise, and decodes and successively cancels such messages

out. Since the code constructions provided here achieve higher rates than those available in prior work, they may aid in non-trivial achievability schemes (though in general still not rate-optimal) for this problem.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1204–1216, Jul. 2000.

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

[3] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. on Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[4] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 10, no. 52, pp. 4413–4430, Oct. 2006.

[5] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. of 2002 IEEE Information Theory Workshop (ITW)*, 2002.

[6] ——, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst*, vol. 6, no. 1, pp. 19–36, 2006.

[7] R. W. Yeung and N. Cai, "Network error correction, part II: Lower bounds," *Commun. Inf. Syst*, vol. 6, no. 1, pp. 37–54, 2006.

[8] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[9] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros, "Resilient network coding in the presence of Byzantine adversaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.

[10] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[11] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[12] M. J. Siavoshani, C. Fragouli, and S. Diggavi, "Noncoherent multisource network coding," in *Proc. IEEE Int. Symposium on Inform. Theory*, Toronto, Canada, Jul. 2008, pp. 817–821.

[13] S. Mohajer, M. Jafari, S. Diggavi, and C. Fragouli, "On the capacity of multisource non-coherent network coding," in *Proc. of the IEEE Information Theory Workshop*, 2009.

[14] M. Siavoshani, C. Fragouli, and S. Diggavi, "Code construction for multiple sources network coding," in *Proc. of the MobiHoc*, 2009.

[15] Personal Communication.

[16] L. Nutman and M. Langberg, "Adversarial models and resilient schemes for network coding," in *Proc. of IEEE International Symposium of Information Theory*, 2008, pp. 171–175.

[17] T. Ho, M. Médard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," in *Proc. of Allerton 2003*, 2003.

[18] S. Vyetrenko, T. Ho, M. Effros, J. Kliewer, and E. Erez, "Rate regions for coherent and noncoherent multisource network error correction," in *Proc. of IEEE International Symposium of Information Theory*, 2009.

[19] H. Yao, T. K. Dikaliotis, S. Jaggi, and T. Ho, "Multiple access network information-flow and correction codes*," submitted for publication into *Proc. of IEEE Information Theory Workshop*, Dublin, 2010, available online at http://www.its.caltech.edu/ tdikal/preprints/2010-preprint-itw-hdjh.pdf.

[20] M. Artin, *Algebra*. New Jersey: Prentice Hall, 1991.

[21] S. Vyetrenko, T. Ho, and E. Erez, "On noncoherent correction of network errors and erasures with random locations," in *Proc. of the IEEE International Symposium on Information Theory*, Jun. 2009.

[22] D.Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Transactions on Information Theory*, vol. 55, pp. 5479–5490, 2009.

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

[24] M. Agrawa and S. Biswas, "Primality and identity testing via chinese remaindering," *Journal of the ACM*, 2003.

[25] S. Yang and R. W. Yeung, "Characterizations of network error correction/detection and erasure correction," in *NetCod 2007*, Jan 2007.

[26] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Transactions on Information Theory*, vol. 52, pp. 789–804, 2006.