

# Network Coding with Myopic Adversaries

Sijie Li, Rawad Bitar, Sidharth Jaggi and Yihan Zhang

## Abstract

We consider the problem of reliable communication over a network containing a hidden *myopic* adversary who can eavesdrop on some  $z_{ro}$  links, jam some  $z_{wo}$  links, and do both on some  $z_{rw}$  links. We provide the first information-theoretically tight characterization of the optimal rate of communication possible under all possible settings of the tuple  $(z_{ro}, z_{wo}, z_{rw})$  by providing a novel coding scheme/analysis for a subset of parameter regimes. In particular, our vanishing-error schemes bypass the Network Singleton Bound (which requires a zero-error recovery criteria) in a certain parameter regime where the capacity had been heretofore open. As a direct corollary we also obtain the capacity of the corresponding problem where information-theoretic secrecy against eavesdropping is required in addition to reliable communication.

**A short video describing this work can be found in [1].**

## I. INTRODUCTION

Network coding is a network communication paradigm wherein nodes in a network non-trivially combine incoming packets to generate information on outgoing packets. It has been shown [2] that such combination operations are necessary and sufficient to attain information-theoretically optimal communication rates for many classes of network communication problems – in particular, for *multicast* problems, if the smallest source-destination *min-cut* equals  $C$ , network codes are able to attain this rate. Further, it was shown [3]–[5] that linear codes suffice for this purpose. Applications of network coding now abound in a variety of disparate fields, such as wireless systems [6], distributed storage [7], and router designs [8].

One complication in the network coding paradigm is the potential problem of errors – due to the mixing operations in the network even a single corrupted packet may end up tainting the majority of the information flowing in the network; as such, a malicious jammer hiding in the network may be able inflict disproportionate damage. To combat this problem, network error-correcting codes were proposed by Cai and Yeung [9], [10], followed by a plethora of computationally efficient code designs [11]–[15].

The focus of this paper is on a complete characterization of the optimal throughput possible in the presence of a *myopic* jammer. Initial works on network error-correction (for instance [9], [10], [15]) assumed the presence of an *omniscient* adversary – an adversary who is able to observe *all* transmissions in a network, and then tailor his jamming scheme as a function of his observations. In such scenarios, it was shown as a consequence of the Network Singleton bound [9], [10] that each of the adversary’s injected corrupted packets can do “double damage”, i.e., the optimal throughput obtainable is  $C - 2z_w$ , where  $z_w$  equals the number of packets the adversary can inject into the network. In contrast, it was observed in [11] that if the adversary is able to observe only  $z_r$  packets and must design its jamming strategy as a function of these observations, then for the parameter regime  $z_r + 2z_w < C$  (whence the adversary was said to be *limited*) in fact a throughput of  $C - z_w$  is obtainable, effectively making the jamming no more damaging than the relatively benign scenario of random noise.<sup>1</sup> Extensions beyond this parameter regime were made in the setting where the adversary’s noise is *additive* [16], [17]. Such adversarial models arise naturally in a variety of settings wherein the adversary can only control (eavesdrop on and/or jam) a subset of network links due to its physical constraints. However, a complete information-theoretic characterization of the capacity region, especially for the important and physically relevant model of *overwrite* adversaries (see Remark 3) was heretofore open.

In this work we focus on a more granular model parametrization that subsumes the limited adversary model of [11] as a special case. For this generalized setting we provide a complete characterization of the information-theoretically optimal communication rate possible. In our model, there are:

- **Read-Only links:**  $z_{ro}$  links that the adversary can only observe but not jam.
- **Write-Only links:**  $z_{wo}$  links that the adversary can only jam but not observe.
- **Read-Write links:**  $z_{rw}$  links that the adversary can both observe and jam.

As ancillary parameters, we also define

- **Read links:**  $z_r$  denotes the overall number of links  $z_{ro} + z_{rw}$  that the adversary can observe.
- **Write links:**  $z_w$  denotes the overall number of links  $z_{wo} + z_{rw}$  that the adversary can jam.

Sijie Li is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong. Email: sijieli@link.cuhk.edu.hk.

Rawad Bitar is with the Institute for Communications Engineering, Technical University of Munich, Munich, Germany. Email: rawad.bitar@tum.de.

Sidharth Jaggi is with the School of Mathematics, University of Bristol, Bristol, United Kingdom, and the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong. Email: sid.jaggi@bristol.ac.uk.

Yihan Zhang is with the Faculty of Computer Science, Technion Israel Institute of Technology, Haifa, Israel. Email: yihanzhang@cuhk.edu.hk.

<sup>1</sup>It is important to highlight that such results attaining rates higher than  $C - 2z_w$  are possible only if one accepts a vanishing probability of error metric rather than a zero-probability of error metric.

Our main result is that if  $z_{r_o} + 2z_{r_w} + 2z_{w_o} < C$  (the so-called “weak adversary” regime), then a rate of  $C - z_w$  is attainable. The optimality of this rate can be seen by noting that if James were to just add random noise on  $z_w$  links in the min-cut, direct information-theoretic cutset arguments imply that no higher rate is possible without resulting in a probability of error approaching one. Our results are quite strong – they hold even in a distributed network coding setting, i.e., if none of the legitimate parties communicating have prior information neither about the network topology or linear network coding operations performed by internal nodes nor about which network links are being eavesdropped/jammed by the adversary. In contrast, the malicious adversary is assumed to know the network topology, coding operations of each network node (including the source and sink) in advance, and as a function of this knowledge is allowed to choose an arbitrary subset of  $z_r$  links to eavesdrop on. On a basis of these observations the adversary may also choose  $z_w$  links to jam (of which at most  $z_{r_w}$  may be from among the  $z_r$  eavesdropped links), and additionally may base the contents of the corrupted packets he injects on all this information. Also, no computational restrictions are assumed on the adversary.

On the other hand if  $z_{r_o} + 2z_{r_w} + 2z_{w_o} \geq C$  (the so-called “strong adversary” regime), prior work [18] has already shown that even in particularly simple networks (“parallel-edge networks”) no rate higher than  $(C - 2z_w)^+$  is attainable, and indeed such a rate is already obtainable even against omniscient adversaries, for instance by the codes in [11]–[15]. Indeed, our main result may be viewed as the network coding generalization of [18]. A comparison of our work with related prior works is listed in Table I.

	Adversary power	Network type	Rate	Decoding Complexity
Jaggi et.al. [11]	Strong Adv. $C < z_{r_o} + 2z_{r_w} + 2z_{w_o}$	General Network	$C - 2z_w$	$\mathcal{O}((nC)^3)$
Jaggi et.al. [11]	Weak Adv. $C > z_r + 2z_w$	General Network	$C - z_w$	$\mathcal{O}(nC^2)$
Zhang et.al. [18]	Weak Adv. $C > z_{r_o} + 2z_{r_w} + 2z_{w_o}$	Parallel Edges	$C - z_w$	$\mathcal{O}(\text{poly}(n))$
<b>This work</b>	Weak Adv. $C > z_{r_o} + 2z_{r_w} + 2z_{w_o}$	General Network	$C - z_w$	–

TABLE I: *Related Works.* Our work fills the gap of information-theoretical characterization for general network with the optimal rate  $C - z_w$ . With the converse from [18], there now is a full characterization of network error-correction under myopic adversary.

Our techniques rely on those developed for point-to-point myopic adversarial settings in [19], carefully coupled with the appropriate *subspace metric* for the problem at hand [14]. In the weak adversary regime, by the myopic nature of the adversary and the choice of the coding rate, the adversary has a considerable amount of uncertainty regarding the codeword transmitted through the network. Our analysis critically leverages such uncertainty and shows that under any adversarial action, only a small fraction of codewords may suffer from decoding errors.

We extend our results to the case where the message must also be secured, in an information theoretic sense, from the adversary’s observation. We show that by coupling our coding techniques with coset codes [20], a rate of  $C - z_r - z_w$  can be achieved for the weak adversary regime. The optimality of this rate follows from meeting the converse derived in [18] for parallel-edge networks. For the strong adversary regime, it is shown [18] that no positive rate can be achieved while requiring secrecy of the transmitted message.

There are potential applications of such codes in the presence of myopic adversaries in a variety of settings beyond vanilla network coding – for instance, distributed storage [21], secret-sharing [22], private information retrieval [23], and coded computing [24].

## II. PRELIMINARIES

For ease of presentation, in this paper we consider a unicast network coding problem in the presence of a myopic adversary – as is common in the network error-correction literature, the techniques we develop directly translate to multicast settings as well.

### A. Channel Model

We consider the problem of communicating reliably through a network in the presence of a myopic adversary. In a nutshell, a sender Alice wants to send a message to a receiver Bob through the network. An adversary James eavesdrops on a subset of the links in the network and can jam another subset of the links – in particular, James can decide which subset of links to jam, and how to jam them, based on his observations from the eavesdropped links. The goal is for Bob to be able to reliably reconstruct Alice’s message despite James’ jamming action. The network model is depicted in Figure 1. The detailed model is explained next.

**Notational conventions:** We use  $\mathbb{F}_q$  to denote finite fields of size  $q$  for prime powers  $q$ , and  $\mathbb{F}_q^n$  or  $(\mathbb{F}_q)^n$  to denote the vector space of  $n$ -tuples over  $\mathbb{F}_q$ . Scalars and scalar functions will be denoted by lower-case alphabets (e.g.  $m$ ). Matrices will be denoted by upper-case alphabets (e.g.  $X$ ) – two exceptions as nods to firmly established convention will be the scalar quantity  $C$  denoting the min-cut of a graph of interest, and  $U(\cdot)$  denoting the uniform distribution over a set. The row-space of any given matrix  $X$  will be denoted  $V(X)$ , and  $\oplus$  and  $\cap$  respectively denote the direct sum and intersection (of vector spaces). Sets and graphs will be denoted by calligraphic letters (e.g.  $\mathcal{C}$ ). The notation  $\mathbb{1}(\cdot)$  indicates the indicator function of

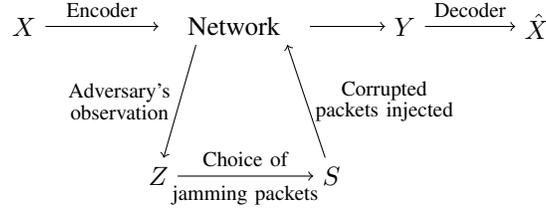


Fig. 1: *Network Model*: The sender inputs packets corresponding to the rows of matrix  $X$  into the network. The adversary eavesdrops on a set of  $z_r$  links leading to his observation matrix  $Z$ . Based on  $Z$ , he jams another set of links by injecting into the network a matrix  $S$ . The receiver receives the corrupted packets  $Y$ , corresponding to linear combinations of  $X$  and  $S$ . The communication goal is for the receiver to recover the transmitted  $X$  with high probability.

Symbol	Meaning
$C$	Min-cut of the Network
$n$	Length of the packet
$q$	Size of the finite field
$R$	Rate
$z_{ro}$	Eavesdropping-only power
$z_{rw}$	Eavesdropping and Overwriting power
$z_{wo}$	Overwriting-only power
$z_r$	Total eavesdropping power = $z_{ro} + z_{rw}$
$z_w$	Total overwriting power = $z_{wo} + z_{rw}$
$\epsilon$	Rate slack – small positive constant
$\mathcal{C}$	Codebook

TABLE II: Important notation

the corresponding event, and the notation  $(x)^+$  denotes  $\max\{x, 0\}$ . Frequently used notation throughout this paper is listed in Table II for reference.

**Network model:** The network  $\mathcal{N}$  is a directed acyclic graph<sup>2</sup> comprising of a *vertex-set*  $\mathcal{V}$  of nodes and an *edge-set*  $\mathcal{E}$  of directed links. Each node in  $\mathcal{V}$  can manipulate information on incoming links to generate messages on outgoing links. Each link in  $\mathcal{E}$  is assumed to have unit capacity, corresponding to the ability to transmit a single length- $n$  vector over some finite field  $\mathbb{F}_q$  over a suitable period of time.<sup>3</sup> The *block/packet-length*  $n$ , and *field-size*  $q$  are design parameters to be specified later. Nodes in the network may perform arbitrary arithmetic operations on incoming packets to generate outgoing packets. The min-cut of the network is denoted by  $C$ .

**Encoder model:** The sender Alice, situated at the *source node*, has a *message*  $m$  that is uniformly distributed over the set  $[q^{nR}]$  (the *rate*  $R$  is a design parameter to be specified later).

Alice's goal is to reliably communicate her message  $m$  to the receiver Bob situated at the *sink node*. To instantiate this communication she uses her *encoder*  $Enc : [q^{nR}] \rightarrow (\mathbb{F}_q)^{C \times n}$  to choose a *codeword*  $X$  (a  $C \times n$  matrix over  $\mathbb{F}_q$ ) for each message  $m \in [q^{nR}]$ .<sup>4</sup> The collection of all such codewords  $X$  comprises the *codebook*  $\mathcal{C}$ . Prior to communication, this codebook  $\mathcal{C}$  and the corresponding encoding (mapping from messages  $m$  to codewords  $X$ ) is known to each of Alice, Bob, and the adversary James described below.

We assume that prior to communication, Alice, Bob and the intermediate nodes do not know the network topology (though they know the value of the min-cut  $C$ ), nor do they know the network coding operations performed by intermediate nodes.<sup>5</sup> In the scheme we present these intermediate nodes perform *random linear network coding* [26], though the matching converse argument we outline in Section III-C does not rely on specific coding scheme.

**Network communication scheme:** The *network communication scheme*  $\mathcal{S}$  comprises of Alice's encoder  $Enc$ , the (linear) coding operations of nodes in  $\mathcal{V}$ , and Bob's decoder  $Dec$  as described below.

**Adversarial model:** In addition to knowing Alice's encoding strategy/codebook  $\mathcal{C}$ , the malicious adversary James knows the network topology, Bob's decoding strategy, and the coding performed at intermediate nodes. James' goal is to try to disrupt the communication from Alice to Bob in a manner so that Bob is unable to reliably estimate Alice's message  $m$ . To instantiate

<sup>2</sup>The scenario where the network has cycles is considerably more complex [25], as it involves some level of feedback – we do not consider it here.

<sup>3</sup>Again, as is standard in the network coding, if links have unequal capacities, this can be handled by splitting such links into parallel links of unit capacity.

<sup>4</sup>Note that in contrast to some prior work in the secure/reliable network coding literature (for instance [11]), this is a *deterministic* mapping from each message  $m$  to corresponding codeword  $X$  – it turns out that our schemes do not need to rely on additional stochasticity/randomness.

<sup>5</sup>We make these model choices to demonstrate that our coding scheme is able to operate despite knowing very little about the network setting *a priori*. In addition, the converse argument we outline in Section III-C goes through even if Alice/Bob/intermediate nodes had prior knowledge of the topology/intermediate coding operations, so such an assumption is not unduly restrictive.

this disruption, as a function of his knowledge, he can pick a subset of links to control in the manner described below. James's power is parametrized by his *adversarial power-tuple*  $(z_{ro}, z_{wo}, z_{rw})$ , characterized as the following:

- First, he can read (without changing) the data transmitted on the set of  $z_{ro}$  “read-only” links of his choice.
- Next, on another set of  $z_{rw}$  “read-write” links of his choice, he can read the transmitted data, and then overwrite the transmissions on these links with an arbitrary set of  $z_{rw}$  length- $n$  vectors (these vectors may depend on James' observations on all  $z_{ro} + z_{rw}$  links).
- Finally, on a set of  $z_{wo}$  “write-only” links of his choice, James can replace the contents of these links with an arbitrary set of  $z_{wo}$  length- $n$  vectors (these vectors may depend on James' observations on all  $z_{ro} + z_{rw}$  links, but *not* on the contents of the  $z_{wo}$  write-only links).

For notational convenience, we also define the ancillary parameters  $z_r$ ,  $z_w$  and  $z$  as follows:

- The *number of eavesdropped links*  $z_r$  is set to equal  $z_{ro} + z_{rw}$ , corresponding to the total number of links James can eavesdrop on.
- The *number of jammed links*  $z_w$  is set to equal  $z_{wo} + z_{rw}$ , corresponding to the total number of links James can jam.
- The *number of corrupted links*  $z$  is set to equal  $z_{ro} + z_{wo} + z_{rw}$ , corresponding to the total number of links James can read and/or write on.

In more detail, let the *eavesdropper's observation matrix*  $Z$  be the  $z_r \times n$  matrix over  $\mathbb{F}_q$  whose rows comprise of James' observations on the  $z_r$  links he can eavesdrop on. As noted above, since in this model it suffices to restrict the operations performed by intermediate nodes to (random) linear network coding operations,  $Z$  equals  $T_{AJ}X$ . Here the *network transform from Alice to James*  $T_{AJ}$  is a  $z_r \times C$  matrix over  $\mathbb{F}_q$  corresponding to the linear transform of  $X$  instantiated by the network coding operations by nodes upstream of James.

Further, let the *jamming matrix*  $S$  be the  $z_w \times n$  matrix over  $\mathbb{F}_q$  which comprises of James' jamming patterns  $S_{wo} \in \mathbb{F}_q^{z_{wo} \times n}$  on the  $z_{wo}$  links he can jam and  $S_{rw} \in \mathbb{F}_q^{z_{rw} \times n}$  on the  $z_{rw}$  links he can eavesdrop on and jam. Then  $S$  is a function of  $Z$  (and in addition James' knowledge of the network topology, and Alice's encoder  $Enc$  above, the network coding operations, and Bob's decoder  $Dec$  described below). On a few occasions below we use the notation  $S = Jam_S(Z)$  instead of  $S$ , to make explicit the dependence of the jamming matrix  $S$  on the eavesdropper's observation matrix  $Z$  – here  $Jam_S : (\mathbb{F}_q)^{z_r \times n} \rightarrow (\mathbb{F}_q)^{z_w \times n}$  can be interpreted as James' *jamming function*. James is unconstrained in his choice of jamming functions.<sup>6</sup>

**Remark 1.** *Strictly speaking, the jamming matrix  $S \in \mathbb{F}_q^{z'_w \times n}$  can have smaller dimension  $z'_w \leq z_w$ . In particular, it can comprise of two sub-matrices  $S_{wo} \in \mathbb{F}_q^{z'_{wo} \times n}$  and  $S_{rw} \in \mathbb{F}_q^{z'_{rw} \times n}$  for some  $z'_{wo} \leq z_{wo}$  and  $z'_{rw} \leq z_{rw}$ . However, we focus on the worst case where the adversary uses his full power. Other cases can be reduced to this case by treating  $(z'_{ro}, z'_{wo}, z'_{rw})$  that James truly used as the new adversarial power tuple.*

Prior to communication, the locations of these  $z_{ro}$ ,  $z_{wo}$ , and  $z_{rw}$  links among the edge-set  $\mathcal{E}$  are unknown to Alice/Bob/intermediate nodes (though the *values* of  $z_{ro}$ ,  $z_{wo}$ , and  $z_{rw}$ , or good upper bounds on these, are available to Alice and Bob).

Following the lead of [18], James is called a *weak adversary* if the condition in Eqn. (1) is satisfied.

$$C > z_{ro} + 2z_w \quad (1)$$

A pictorial explanation of the adversarial model considered in this work is shown in Fig. 2.

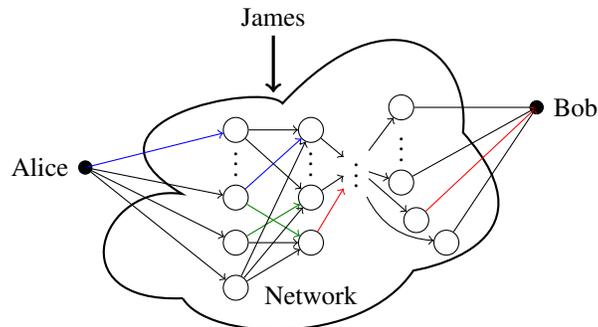


Fig. 2: *James' attack in view of the network. The blue edges represent those that James can eavesdrop. The red edges represent those that James can jam. The green edges represent those that James can both eavesdrop and jam.*

<sup>6</sup>Indeed, he can even choose probabilistic jamming functions. However, as shown in [19], given any probabilistic jamming function  $Jam_S$  with a given probability of decoding error (as defined in (2)), there exists a deterministic jamming function  $Jam'_S$  with at least the same probability of decoding error. Hence, without loss of generality, we focus here on deterministic jamming functions.

**Remark 2.** As noted in Section I, the significance of the inequality in Eqn. (1) is that this is precisely the parameter regime where the following happens – say Alice chooses a random code of rate  $C - z_w - \epsilon$ , then there is still an exponentially large set of codewords in  $\mathcal{C}$  that are consistent with James’ observation  $Z$ . Roughly speaking, in [19], whose approach we adapt in this work, the corresponding parameter regime is called the *sufficiently myopic regime*.

**Remark 3.** The distinction between the additive error models in [16], [17], and the overwrite model considered in this work (wherein James can replace the contents of packets on the links he can jam with whatever he wishes) shows itself in the  $z_{wo}$  links. In additive models, if James has uncertainty about what is being transmitted on a link, he will still have uncertainty after he jams this link. In contrast, in the overwrite model we consider in this work, the content of packets on links James corrupts is always precisely known to him, since he replaces the prior contents with his injected corruptions (even if he has uncertainty about the contents of the links he is corrupting). Arguably, the overwrite error model of this paper is a more natural fit for a variety of wired/distributed computing/storage models than the additive model (which can perhaps be motivated more in wireless settings).

**Remark 4.** We wish to emphasize that anything that Alice and Bob (and/or intermediate nodes) know prior to communication, James also knows – hence no shared keys/common randomness is shared privately between Alice and Bob – in this regard we differ from some models in the literature, such as the “Shared Secret” model in [11], or the model of [27]. Also, we do not assume computational bounds on James (unlike, for instance, the models of [28] or [29]).

**Decoder model:** We represent the information on the links incoming to the sink by the *network output*  $Y$ , a  $\mathbb{C} \times n$  matrix over  $\mathbb{F}_q$ .<sup>7</sup> Given this  $Y$  and his knowledge of Alice’s codebook  $\mathcal{C}$ , the goal of Bob’s decoder  $Dec : (\mathbb{F}_q)^{\mathbb{C} \times n} \rightarrow [q^{nR}]$  is to ensure that its output  $\hat{m}$  is a “reliable estimate” (as made precise next) of Alice’s message  $m$ .

**Code properties:** Bob’s decoder  $Dec$  is said to make an error if the decoder output  $\hat{m}$  differs from Alice’s message  $m$ .

For a given network communication scheme  $\mathcal{S}$ , the (average) *probability of decoding error* is defined as in Eqn. (2) where the expectation is over Alice’s uniformly distributed message  $m \sim U([q^{nR}])$  and the random linear network coding operations at the intermediate nodes.

$$\max_{Jam_{\mathcal{S}}} \mathbb{E} \left( \frac{\sum_{X' \in \mathcal{C}: T_{AJ} X' = Z} \mathbb{1}(Dec(Y(X', Jam_{\mathcal{S}}(Z))) \neq m)}{|\{X' \in \mathcal{C} : T_{AJ} X' = Z\}|} \right) \quad (2)$$

In words, the meaning (2) can be unwrapped as follows. Say Alice has message  $m$  (the notation  $m \sim U([q^{nR}])$  means that  $m$  is uniformly distributed among all possible messages), resulting in the codeword  $X = Enc(m)$ . For the given network communication scheme  $\mathcal{S}$  (that James knows) his observation matrix equals  $Z = T_{AJ} X$ , and based on this observation and the communication scheme James chooses a corresponding jamming function  $Jam_{\mathcal{S}}$ , resulting in the jamming matrix  $S = Jam_{\mathcal{S}}(Z)$ . Note that there will in general be multiple possible codewords  $X'$  in Alice’s codebook  $\mathcal{C}$  such that  $T_{AJ} X'$  equals James’ observation  $Z$  – call them *Z-compatible* codewords. Then, for a specific jamming function  $Jam_{\mathcal{S}}$  and message  $m$ , the fraction of *Z-compatible* codewords  $X'$  that result in Bob’s decoder making an error is the probability of error. For a specific jamming function  $Jam_{\mathcal{S}}$ , the average probability of error is the average of the previous quantity over all messages  $m$ . Finally, since James’ jamming function  $Jam_{\mathcal{S}}$  can be arbitrary (he is after all a malicious adversary), this probability of error quantity is maximized over all possible jamming functions.

A rate  $R$  is said to be *achievable* if for any  $\epsilon > 0$  there exists a network communication scheme over some (sufficiently large)  $n$  and  $q$  such that the probability of decoding error is no more than  $\epsilon$ . The *network error-correction capacity*  $R^*$  for a given network  $\mathcal{N}$  and adversarial power-tuple  $(z_{ro}, z_{wo}, z_{rw})$  is then the supremum (over network communication schemes) of achievable rates.

**Secrecy model:** When secrecy is to be satisfied, our codes attain perfect secrecy [20], [30]. Let  $m$  be the transmitted message, let  $X$  be the symbols communicated through the network and let  $Z$  be James’ observation. *Information theoretic secrecy* (a.k.a. *perfect secrecy*) requires that James’ uncertainty about the message  $m$  is not reduced after his observation, i.e.,  $H(m|Z) = H(m)$ , where  $H(\cdot)$  is the entropy function and all logarithms are base  $q$ . This is in contrast to *strong* and *weak secrecy* in which it is required that  $H(m|Z) = H(m) - \epsilon_n$  for a small  $\epsilon_n$  that either goes to 0 when the block length  $n$  goes to infinity (strong secrecy) or  $\epsilon_n/n$  goes to 0 when  $n$  goes to infinity (weak secrecy).

A rate  $R_{\text{sec}}$  is said to be *securely achievable* if for any  $\epsilon > 0$  there exists a network communication scheme over some (sufficiently large)  $n$  and  $q$  such that the probability of decoding error is no more than  $\epsilon$  and perfect secrecy of the transmitted message is maintained. The *secure network error-correction capacity*  $R_{\text{sec}}^*$  for a given secure network  $\mathcal{N}$  and adversarial power-tuple  $(z_{ro}, z_{wo}, z_{rw})$  is then the supremum (over network communication schemes) of securely achievable rates.

<sup>7</sup>A natural question pertains to scenarios where there are more than  $C$  packets incoming to the sink. It can be shown via standard arguments that with high probability over the random linear network code design, there are at least  $C$  linearly independent vectors on the links incoming to the sink. As is common in the network error-correction literature (see for instance [11]), if there are more than  $C$  linearly independent vectors, we choose an arbitrary subset of size  $C$  and discard the remainder. As we show, in the weak adversary regime when Alice is transmitting at rate  $C - z_w - \epsilon$ , Bob is still able to reconstruct Alice’s message with high probability. Conversely, via standard information-theoretic arguments, if Alice is transmitting at rate higher than  $C - z_w + \epsilon$  and James injects random noise on  $z_w$  links situated in a min-cut, every communication scheme will have a probability of error converging to 1. Hence no loss of performance arises from this discarding operation.

To prove the strongest possible results, we provide perfect secrecy when constructing codes, and consider weak secrecy for proving a converse on the error-correction capacity of secure networks. We show that those values are equal, i.e., the converse that holds even for weak secrecy can be achieved while maintaining perfect secrecy.

### B. Subspace Codes

In our scheme, Alice's encoder and Bob's decoder will depend critically on certain properties of the row-spaces of the matrices  $X$  in  $\mathcal{C}$ . It will therefore help to quickly review the extensive literature on *subspace codes* (see for instance the review in [15]).

The set of all subspaces of  $\mathbb{F}_q^n$  is called the projective space of order  $n$  over  $\mathbb{F}_q$ , denoted as  $\mathcal{P}_q(n)$ . The set of all  $k$ -dimensional subspaces of  $\mathbb{F}_q^n$  is called a Grassmannian, denoted as  $\mathcal{G}_q(n, k)$ , where  $0 \leq k \leq n$ . A graph representation of the Grassmannian is shown in Fig. 3.

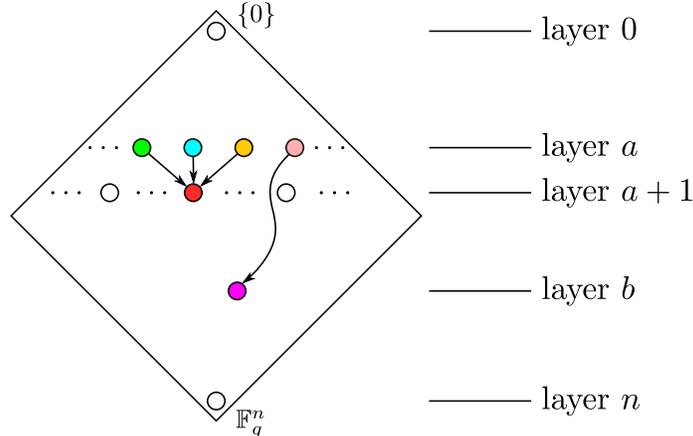


Fig. 3: A graph representation of the Grassmannian. Nodes in layer  $a$  are  $a$ -dimensional subspaces. An arrow connecting two subspaces in two adjacent layers means that the  $(a + 1)$ -dimensional subspace in layer  $a + 1$  contains the  $a$ -dimensional subspace in layer  $a$ . For example, the *red* subspace contains the *green*, *blue* and *yellow* subspaces. We say two subspaces in layers  $a$  (the subspace in *light pink*) and  $b$  (the subspace in *dark pink*),  $b > a + 1$ , are connected if there exists a path (series of arrows) connecting the subspace in layer  $a$  to the subspace in layer  $b$ .

It is known [14] that the Gaussian coefficient defined as

$$\binom{n}{k}_q \triangleq \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i},$$

measures the cardinality of the Grassmannian  $\mathcal{G}_q(n, k)$ . The value of  $\binom{n}{k}_q$  is bounded between  $q^{kn-k^2}$  and  $4q^{kn-k^2}$  [15, Lemma 4]. Throughout the paper, we will use those values to bound the Gaussian coefficient from below and from above, respectively.

A subspace code is a non-empty collection of subspaces of  $\mathbb{F}_q^n$ . Hence a subspace codeword is a subspace in the collection. However, in the network communication model outlined in the previous section, codewords correspond to  $\mathbb{C} \times n$  matrices. To be able to use the nice machinery of subspace codes, we identify any given subspace of dimension  $k$  with the unique Reduced Row Echelon Form (RREF)  $k \times n$  matrix  $X$  whose row-space  $V(X)$  equaling the given subspace. Subspace codes such that each subspace in the code is of the same dimension is called a constant-dimension code. The distance function  $d(\cdot, \cdot)$  we use is the *injection distance* between subspaces [14], where the distance between any two subspaces  $V$  and  $V'$  is expressed as

$$d(V, V') = \max\{\dim(V), \dim(V')\} - \dim(V \cap V'). \quad (3)$$

It is shown in [14] that this definition results in a metric. The injection distance is depicted in view of the Grassmannian in Fig. 4.

### C. Communication Scheme

We now describe the specific encoding and decoding strategies in our scheme, and James' possible eavesdropping/jamming actions, all in the context of subspace codes over Grassmannians.

1) *Random code construction/Encoder*: We construct the codebook  $\mathcal{C}$  by sampling  $q^{nR}$  codewords (subspaces) uniformly at random from the Grassmannian  $\mathcal{G}_q(n, \mathbb{C})$ . Given a message  $m$  and the corresponding codeword/subspace, Alice's encoder then merely transmits the RREF matrix  $X$  with row-space equaling the given subspace.

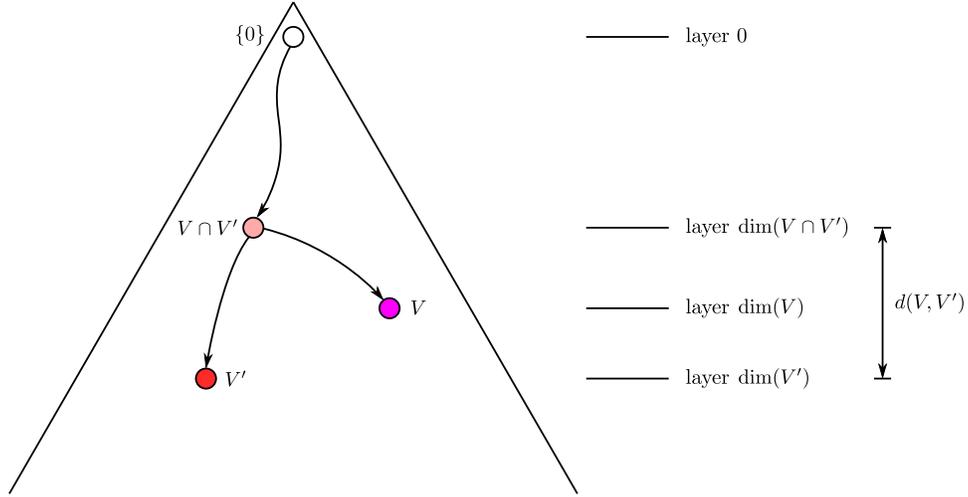


Fig. 4: Injection distance in the context of the Grassmannian graph.

2) *Decoder*: Bob uses a “brute-force” injection-distance decoder. The decoder measures the injection distance given in Eqn. (3) between the received subspace  $V(Y)$  and each codeword  $V(X)$  in the codebook. If there is a unique codeword  $\hat{X}$  such that  $d(Y, \hat{X}) \leq z_w$ , then the decoder outputs  $\hat{X}$  as the transmitted codeword. Otherwise, the decoder outputs an error.

**Remark 5.** Using such an injection-distance decoder is not in general optimal for general codes (beyond subspace codes), since many different matrices may have the same row-space. Indeed, in some contexts, ignoring such degeneracy can result in loss of useful information. For instance, in [31] a scheme that does not collapse multiple matrices into a single subspace allows in some scenarios one to estimate the topology of a given network and adversarial location. However, for our purposes in this work, where we are focused solely on the problem of characterizing the information-theoretically optimal rate of communication over networks containing myopic adversaries, exploiting the non-degeneracy of general codes (rather than subspace codes) does not asymptotically improve the throughput. And on the flip side, as has been noted in the literature in the past (for instance [15]), subspace codes have the pleasing property that they allow one to ignore the role that specific network topologies/linear network coding operations play in how information is transformed in the network, enabling significantly cleaner and easier analysis.

3) *Adversarial Action*: James observes a  $z_r$ -dimensional subspace  $V(Z) = V(T_{AJ}X)$  of  $V(X)$  – for notational convenience we henceforth denote this  $V(Z)$  as  $V_r(X)$ . Based on this observation, he designs a subspace  $V(S)$  of dimension not exceeding his jamming power  $z_w = z_{wo} + z_{rw}$  to inject in the network. Let  $V(S) = V_{wo}(S_{wo}) \oplus V_{rw}(S_{rw})$ , where  $V_{wo}(S_{wo})$  and  $V_{rw}(S_{rw})$  respectively denote the subspaces inserted on the  $z_{wo}$  write-only links and the  $z_{rw}$  read-write links controlled by James. We represent the subspace  $V(Y)$  received by Bob as  $V_{ro}(X) \oplus V_u(X) \oplus V_{wo}(S_{wo}) \oplus V_{rw}(S_{rw})$ . Here  $V_u(X)$  corresponds to the subspace in the direct-sum decomposition of the transmitted codeword  $V(X)$  that is neither seen nor overwritten by James. James’ adversarial action is depicted in Fig. 5 in view of (the graph representation of) the Grassmannian.

#### D. Error Event

We define the following to be the error event.

**Definition 1.** Consider a transmitted codeword  $V(X)$  and a received subspace  $V(Y)$ . We say that an error happens if for some jamming action  $V(S)$ , there exists a codeword  $V(\hat{X}) \in \mathcal{C}$  such that  $V(\hat{X}) \neq V(X)$  and  $d(V(\hat{X}), V(Y)) \leq z_w$  where  $V(Y)$  results from  $V(X)$  and  $V(S)$ .

The probability of decoding error is the probability of finding a suitable subspace  $V(S)$  among all feasible jamming matrices such that there exists a codeword  $\hat{X} \neq X$  that satisfies

$$d(V(\hat{X}), V(Y)) = d(V(\hat{X}), V_{ro}(X) \oplus V_u(X) \oplus V_{wo}(S_{wo}) \oplus V_{rw}(S_{rw})) \leq z_w.$$

#### E. Main results

With the preliminaries out of the way, our main result is summarized in the following theorem.

**Theorem 1.** The network error-correction capacity  $\mathcal{R}^*$  of a network  $\mathcal{N}$  with min-cut  $C$  and adversarial power-tuple  $(z_{ro}, z_{wo}, z_{rw})$  equals

$$\mathcal{R}^* = \begin{cases} C - z_w & \text{if } C > z_{ro} + 2z_w, \\ (C - 2z_w)^+ & \text{otherwise.} \end{cases} \quad (4)$$

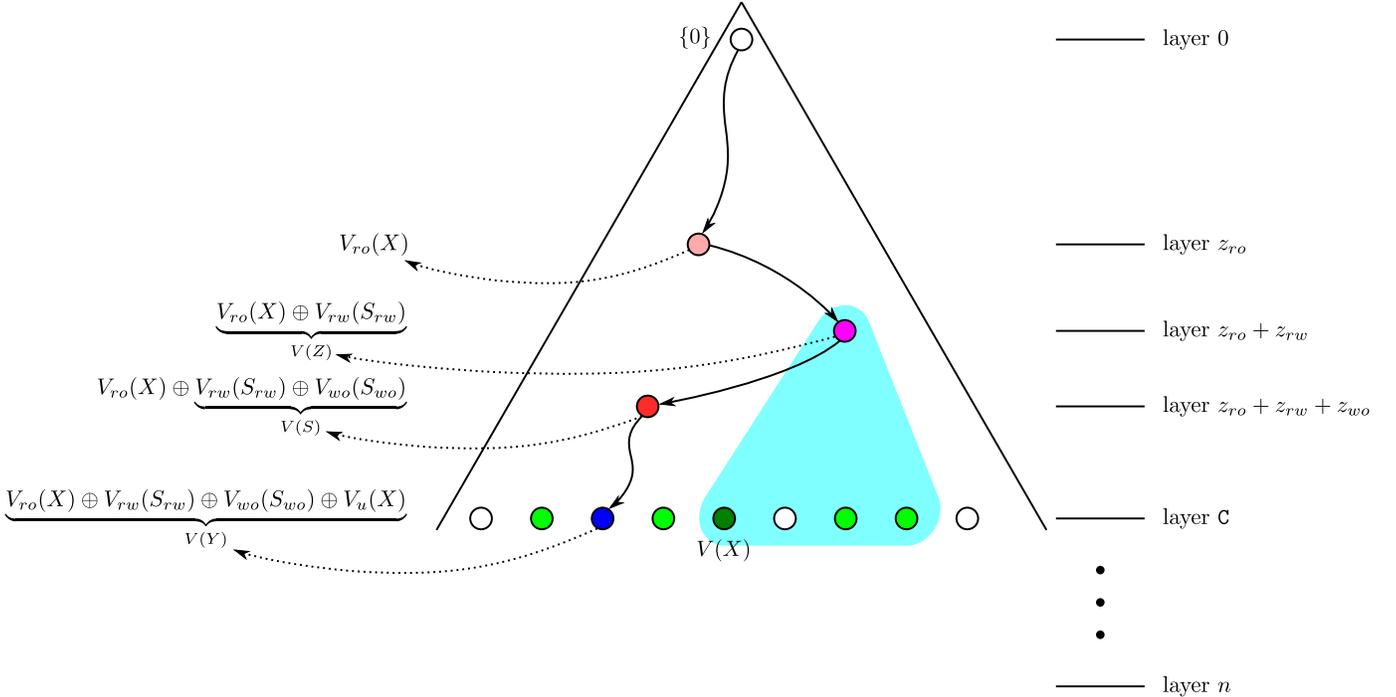


Fig. 5: James' attack in the context of the Grassmannian graph. Each layer here is a collection of subspaces over  $\mathbb{F}_q$  of the same dimension. The codebook consists of  $q^{nR}$  subspaces (the subspaces in light green and dark green) on layer C. The subspace in dark green denotes Alice's codeword  $V(X)$ . James has the power to first observe a subspace of Alice's codeword sitting on layer  $z_{r0} + z_{rw}$  (corresponding to the subspaces in light pink and dark pink). Then, the number of codewords in layer C (the green subspaces in the light blue shaded region) connected to James' observation  $V(Z)$  (the subspace in dark pink) is exponential by Lemma 1. James can choose to overwrite at most  $z_{rw}$  number of observed links (corresponding to the subspace in dark pink) and another  $z_{wo}$  links (corresponding to the red subspace). Overall, James can control the subspace  $V(Y)$  (the subspace in dark blue) received by Bob up to layer  $z_{r0} + z_{rw} + z_{wo}$  by Lemma 3. Our communication scheme works under the assumption given by Eqn. (1).

The rate converse of  $C - z_w$  in the weak adversary regime follows directly from information-theoretic arguments; the rate converse of  $(C - 2z_w)^+$  in the strong adversary regime relies on a myopic symmetrization attack that James can carry out. The proofs of these converses are presented in Sec. III-C. The achievability proof is more involved – a sketch is presented in Sec. III-A and a detailed proof is presented in III-B.

Further, the following corollary can be derived directly via a standard coset coding argument. A detailed explanation is given in Sec. III-D.

**Corollary 1.** *The secure network error-correction capacity  $R_{sec}^*$  of a network  $\mathcal{N}$  with min-cut  $C$  and adversarial power-tuple  $(z_{r0}, z_{wo}, z_{rw})$  equals*

$$R_{sec}^* = \begin{cases} C - z_w - z_r & \text{if } C > z_{r0} + 2z_w, \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

### III. ANALYSIS

We first prove Theorem 1 in two parts. In the first part we prove the achievability of the rate  $C - z_w - \epsilon$  using the proposed subspace codes. Then, we use the result of [18] to show that the optimal rate is indeed  $C - z_w$  if  $C > z_{r0} + 2z_w$  and is  $C - 2z_w$  otherwise. Then, Corollary 1 follows immediately by coupling our subspace code with a coset code [20] for the achievability part. We explain the idea of coset coding and how it is coupled with our subspace code in Section III-D. The converse follows from [18].

We start with a sketch of the achievability proof of Theorem 1 to provide intuition.

#### A. Sketch of the achievability proof

Recall that the codebook is constructed by choosing  $q^{nR}$  subspaces uniformly at random from the Grassmannian  $\mathcal{G}_q(n, C)$ . The decoder decodes the received  $V(Y)$  as explained in Section II-C2. We will show that with high probability, reliable communication in the presence of a weak adversary is possible using the subspace code with rate  $R = C - z_w - \epsilon$ .

Consider the subspace  $V(X)$  transmitted by Alice. James observes a random subspace  $V_r(X)$  of  $V(X)$  of dimension  $z_r$ . Since  $z_r + z_w < C - z_{wo}$ , we can show that approximately  $q^{n(z_{wo} + \delta_1)}$ , for some  $\delta_1 > 0$ , codewords are  $Z$ -compatible with James' observation  $V_r(X)$  (Lemma 1). In other words, from James' perspective, exponentially many codewords could have been transmitted by Alice.

*Oracle-given Set:* For the ease of analysis, we give James more power by giving him extra information about the  $Z$ -compatible codewords. After Alice decides on  $V(X)$ , an oracle reveals to James a random set of  $q^{n\epsilon_1}$   $Z$ -compatible codewords, which includes the correct one. This set is referred to as the oracle-given set and is denoted by  $\mathcal{M}_{og}$ . Note that this only increase James' power by reducing the number of  $Z$ -compatible codewords.

The oracle-given set is generated as follows. For each potential  $V_r(X)$  that may be seen by James, about  $q^{n(z_{wo} + \delta_1)}$  codewords are  $Z$ -compatible. The oracle partitions these compatible codewords into  $q^{n(z_{wo} + \delta_1 - \epsilon_1)}$  sets, each of size  $q^{n\epsilon_1}$ . After eavesdropping on  $z_r$  links, James is given one of the previously constructed sets denoted by  $\mathcal{M}_{og}$  that contains the true codeword. Since each codeword is generated randomly and each partition is constructed randomly, each codeword in  $\mathcal{M}_{og}$  can be viewed as generated uniformly at random conditioned on James' observation.

Now we show that for all jamming actions, Bob will be able to decode  $V(X)$  successfully with high probability. Consider a certain subspace  $V(X)$  transmitted by Alice. James can jam at most  $z_w$  dimensions of this subspace. Bob receives the subspace  $V(Y) = V_{ro}(X) \oplus V_u(X) \oplus V_{rw}(S_{rw}) \oplus V_{wo}(S_{wo})$ . A decoding error happens if and only if there is another codeword  $V(\hat{X}) \in \mathcal{C}$  such that  $d(V(\hat{X}), V(Y)) \leq z_w$ . In this case, we say that the transmitted codeword  $V(X)$  is confused by the codeword  $V(\hat{X})$ . We shall use the following terminology:  $V(X)$  is a *confusable* codeword and  $V(\hat{X})$  is a *confusing* codeword.

We show that for a fixed subspace  $V(S)$  that James injects, only a small fraction of codewords in  $\mathcal{M}_{og}$  can be confused by a codeword  $V(\hat{X}) \neq V(X)$  in  $\mathcal{C}$ . We divide the codebook into two parts: (i) the codewords outside the oracle-given set, i.e., in  $\mathcal{C} \setminus \mathcal{M}_{og}$ ; and (ii) the codewords inside the oracle-given set  $\mathcal{M}_{og}$ . Based on a careful analysis on the Principle of Deferred Decisions [32], we may assume that the codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$  are independent of those in  $\mathcal{M}_{og}$ . Then we can bound the number of confusing codewords in the two previously discussed parts. One more step is needed to conclude the analysis. We need to show that a confusing codeword in  $\mathcal{M}_{og}$  can confuse a small number of codewords. Thus, we can bound the total number of confusable codewords in  $\mathcal{M}_{og}$  which in turns bounds the probability of error. Note that the randomness of all the concentration analysis provided in the proof comes from the codebook construction.

For part (i), we bound the number of confusable codewords in  $\mathcal{M}_{og}$  with confusing codewords from  $\mathcal{C} \setminus \mathcal{M}_{og}$ . We first use a basic list-decoding argument to show that for a given  $V(Y)$ , the number of confusing codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$  that can confuse  $V(X)$  is no more than  $n^3$  with probability  $1 - e^{-\frac{n^3}{3}}$  over code design. Then, we analyze the best  $V(\hat{X})$  that James can hope for to confuse  $V(X)$ . We use the randomness in  $V_u(X)$  to show that the best confusing  $V(\hat{X}) \in \mathcal{C} \setminus \mathcal{M}_{og}$  can confuse at most  $n^3$  codewords in  $\mathcal{M}_{og}$  with probability  $1 - e^{-\frac{n^3}{3}}$ . Hence, in part (i) of the codebook at most  $n^3 \times n^3 = n^6$  of the  $q^{n\epsilon_1}$  possible  $Z$ -compatible codewords are confused by *any* choice of  $S$  by James.

For part (ii), we bound the number of confusable codewords in  $\mathcal{M}_{og}$  with confusing codewords from  $\mathcal{M}_{og}$ . In this case, we cannot use a basic list-decoding argument directly since it strongly relies on the independence between the set of confusing codewords and the set of confusable codewords. To overcome this difficulty, we randomly partition  $\mathcal{M}_{og}$  into a  $q^{n\epsilon_1} \times q^{n\epsilon_1}$  grid. We use the independence among the codewords in rows/columns of this grid to argue that only an exponentially small fraction of codewords can be confusing codewords. Therefore, we can use the same analysis we used for part (i) to bound the number of confusable codewords by  $2q^{n\epsilon_1/2}n^3$  for each confusing codeword (the  $2q^{n\epsilon_1/2}$  comes from taking a union bound over the  $2q^{n\epsilon_1/2}$  rows + columns in the grid). This analysis results in bounding the probability (over code design) of having a small fraction of confusable codewords in  $\mathcal{M}_{og}$  by  $1 - e^{-\frac{n^3}{3}}$ .

Overall, a code is said to be "bad" if there exists a transmitted matrix  $X$  and jamming matrix  $S$  such that more than  $n^6$  codewords are confused in part (i) of the codebook, or more than  $2n^6q^{n\epsilon_1/2}$  codewords are confused in part (ii).

The claimed arguments for the two parts will give us a super-exponentially small probability of a "bad code" for every fixed  $V(S)$  and  $V(X)$ . Therefore, taking a union bound over all possible  $V_r(X)$ ,  $V(S)$  and  $V(X)$ , we still have a small probability of error. Hence, we argue that with high probability, only a small fraction of codewords in  $\mathcal{M}_{og}$  are confusable codewords. Therefore the probability of error is also small since from James' perspective codewords from  $\mathcal{M}_{og}$  are each uniformly likely to have been transmitted.

## B. Detailed proof of the achievability

We prove that reliable communication can be achieved with a random subspace code with rate  $R = C - z_w - \epsilon$  for some sufficiently small  $\epsilon$ . The source of randomness in our analysis is the random generation of the codebook.

First, we argue that based on James' observation, there is at least  $\frac{1}{2}q^{n(z_{wo} + \delta_1)}$   $Z$ -compatible codewords with high probability.

**Lemma 1.** Consider a random subspace code  $\mathcal{C}$  of rate  $R = C - z_w - \epsilon$  used to transmit a message through a network. Let  $\delta_1 \geq 1 - \epsilon$ . For a given subspace  $V_r(X)$  of  $V(X)$  that a weak adversary obtains by observing a random set of  $z_r$  links of the

network, the following holds

$$\Pr \left( \# \text{ of } Z\text{-compatible codewords with a given } V_r(X) \leq \frac{1}{2} q^{n(z_{w_o} + \delta_1)} \right) \leq e^{-\frac{1}{8} q^{n(z_{w_o} + \delta_1)}}.$$

*Proof.* Since James observes a  $z_r$ -dimensional subspace, the remaining subspace is still uniformly distributed from his perspective. The cardinality of the remaining subspace is  $\binom{n}{c-z_r}_q$ . Thus, the probability of a codeword being compatible with James' observation is  $\frac{\binom{n}{c-z_r}_q}{\binom{n}{c}_q}$ , which is no larger than  $4q^{-nz_r+2Cz_r-z_r^2}$  (using the bounds on the Gaussian coefficient). We compute the expected number of  $Z$ -compatible codewords as

$$\begin{aligned} \mathbb{E} [\# \text{ of } Z\text{-compatible codewords}] &= \frac{\binom{n}{c-z_r}_q}{\binom{n}{c}_q} q^{nR} \\ &\geq 4q^{-nz_r+2Cz_r-z_r^2} q^{nR} \\ &= 4q^{n(C-z_{r_o}-2z_{r_w}-z_{w_o}-\epsilon)+2Cz_r-z_r^2} \\ &\geq q^{n(z_{w_o} + \delta_1)}. \end{aligned}$$

The last inequality holds for  $\delta_1 \geq 1 - \epsilon$ , since  $C > z_{r_o} + 2(z_{r_w} + z_{w_o})$  and  $C, z_{r_o}, z_{r_w}$  and  $z_{w_o}$  are integers. Then, by applying the lower tail of the Chernoff bound [33, Eqn. (1.10.12)], we can bound the number of  $Z$ -compatible codewords as given in the statement of the lemma.  $\square$

Lemma 1 quantifies the probability of obtaining more than  $\frac{1}{2} q^{n(z_{w_o} + \delta_1)}$   $Z$ -compatible codewords given a fixed observation  $V_r(X)$ . To bound the probability of obtaining more than  $\frac{1}{2} q^{n(z_{w_o} + \delta_1)}$   $Z$ -compatible codewords for all possible observations, we take the union bound over all  $\binom{c}{z_r}_q$  possible observations as follows

$$\begin{aligned} \Pr \left( \# \text{ of } Z\text{-compatible codewords with any } V_r(X) \leq \frac{1}{2} q^{n(z_{w_o} + \delta_1)} \right) &\leq e^{-\frac{1}{8} q^{n(z_{w_o} + \delta_1)}} \binom{c}{z_r}_q \\ &\leq 4q^{nz_r-z_r^2} e^{-\frac{1}{8} q^{n(z_{w_o} + \delta_1)}}. \end{aligned}$$

We conclude that the probability of James having less than  $\frac{1}{2} q^{n(z_{w_o} + \delta_1)}$   $Z$ -compatible codewords is exponentially small in  $n$ .

Afterwards, we can reveal the oracle-given set  $\mathcal{M}_{og}$  to James and analyse the probability of error in the two following cases.

1) *Type-I Error:* In this case, we consider the confusing codeword  $\hat{X}$ , i.e. the codeword that may confuse Bob with the true codeword, is in  $\mathcal{C} \setminus \mathcal{M}_{og}$ . Recall that the set  $\mathcal{C} \setminus \mathcal{M}_{og}$  is considered independent from the  $\mathcal{M}_{og}$ .

We use the following lemma to argue that with high probability there are at most  $n^3$  confusing codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$ .

**Lemma 2.** *For any  $V_r(X)$  observed by a weak adversary through the network, let  $V(X_i) \in \mathcal{M}_{og}$  be a  $Z$ -compatible codeword and let  $V(S)$  be the adversary's jamming action. For  $V(Y_i) = V_{r_o}(X) \oplus V_u(X_i) \oplus V(S)$ , define the decoding region of  $V(Y_i)$  as  $\mathcal{D}(Y_i) \triangleq \{V(X) \mid \dim(V(X)) = c, d(V(X), V(Y_i)) \leq z_w\}$ . Then, based on the random generation of the codebook  $\mathcal{C}$ , we can write*

$$\Pr \left( \exists V_r(X), V(S), \text{ s.t. } \left| \bigcup_{V(X_i) \in \mathcal{M}_{og}} \mathcal{D}(Y_i) \cap (\mathcal{C} \setminus \mathcal{M}_{og}) \right| \geq n^3 \right) \leq e^{-\frac{\alpha}{3} n^3}.$$

In other words, for any  $V_r(X)$  observed by James and any  $V(S)$  that James inject into the network, the probability that more than  $n^3$  codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$  fall into the union of the decoding regions  $\mathcal{D}(Y_i)$  of codewords  $V(X_i) \in \mathcal{M}_{og}$  is bounded from above by  $e^{-\frac{\alpha}{3} n^3}$ .

*Proof.* We start by bounding the cardinality of the decoding region  $\mathcal{D}(Y)$  for a given received codeword  $V(Y)$ . Since our decoding strategy is to decode to a codeword within distance  $z_w$  from  $V(Y)$ , the cardinality  $|\mathcal{D}(Y)|$  is bounded as

$$\begin{aligned} |\mathcal{D}(Y)| &= \sum_{i=1}^{z_w} \binom{c}{i}_q \binom{n}{i}_q \\ &\leq z_w \binom{c}{z_w}_q \binom{n}{z_w}_q \\ &\leq 16z_w q^{Cz_w - z_w^2} q^{nz_w - z_w^2}. \end{aligned} \tag{6}$$

Given an observation  $V_r(X)$ , its corresponding  $\mathcal{M}_{og}$  and a jamming action  $V(S)$ , let  $\Lambda \triangleq \bigcup_{V(X_i) \in \mathcal{M}_{og}} \mathcal{D}(Y_i)$  be the union of the decoding regions corresponding to all codewords in  $\mathcal{M}_{og}$ . Then the cardinality of  $\Lambda$  is at most  $16q^{n\epsilon_1} z_w q^{Cz_w - z_w^2} q^{nz_w - z_w^2}$ . The probability that a codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$  falls in  $\Lambda$ , i.e., is confusing, is given by

$$\Pr(V(X) \in \Lambda \cap \mathcal{C} \setminus \mathcal{M}_{og}) = \frac{16q^{n\epsilon_1} z_w q^{Cz_w - z_w^2} q^{nz_w - z_w^2}}{q^{nC - C^2}} \quad (7)$$

$$= 16z_w q^{-n(C - \epsilon_1 - z_w - \frac{Cz_w - 2z_w^2}{n})} \quad (8)$$

Then the expected number of codewords from  $\mathcal{C} \setminus \mathcal{M}_{og}$  that fall in  $\Lambda$  is

$$\begin{aligned} \mathbb{E}[|\Lambda \cap \mathcal{C} \setminus \mathcal{M}_{og}|] &= 16z_w q^{-n(C - \epsilon_1 - z_w - \frac{Cz_w - 2z_w^2}{n})} q^{n(C - z_w - \epsilon - \epsilon_1)} \\ &= 16q^{-n(\epsilon - 2\epsilon_1 - \frac{Cz_w - 2z_w^2 - \log_q(z_w)}{n})} \\ &= q^{-n\epsilon_2} \end{aligned}$$

We can adjust  $\epsilon$  and  $\epsilon_1$  such that  $\epsilon > 2\epsilon_1 + \frac{Cz_w - 2z_w^2 - \log_q(z_w)}{n}$  to make sure that  $\epsilon_2$  is a positive number. Therefore, the expected number of confusing codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$  is exponentially small. Then, we can apply the upper tail of Chernoff bound [33, Eqn. (1.10.4)] to argue that the probability of having more than  $n^3$  confusing codewords in  $\mathcal{C} \setminus \mathcal{M}_{og}$  is bounded from above by  $e^{-\frac{n^3}{3}}$ . With this super-exponentially small probability, we can take the union bound over the number of  $V_r(X)$  and  $V(S)$ , which are all of size exponential in  $n$ , to argue that:

$$\Pr(\exists V_r(X), V(S), \text{ s.t. } |(\mathcal{C} \setminus \mathcal{M}_{og}) \cap \Lambda| \geq n^3) \leq e^{-\frac{\alpha}{3}n^3}$$

for some  $\alpha > 0$  to be obtained after taking the union bound.  $\square$

Next, we need to show that each confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$  can confuse at most  $n^3$  codewords in  $\mathcal{M}_{og}$  with high probability. This means that for a confusing codeword  $V(\hat{X})$  in  $\mathcal{C} \setminus \mathcal{M}_{og}$ , the number of codewords  $V(X_i) \in \mathcal{M}_{og}$  such that  $V(\hat{X})$  falls in the decoding region of  $V(Y_i) = V_{ro}(X) \oplus V_u(X_i) \oplus V(S)$  is no more than  $n^3$ .

As an intermediate step, we show that James' best attack can reveal to him a  $(z_{ro} + z_{rw} + z_{wo})$ -dimensional subspace of the codeword  $V(Y)$  received by Bob.

**Lemma 3.** *James can either observe or control at most a  $(z_{ro} + z_{rw} + z_{wo})$ -dimensional subspace of  $V(Y)$  that Bob receives.*

*Proof.* The key idea here is to argue that the  $z_{rw}$  links can only reveal to James a subspace of dimension  $z_{rw}$  of the received  $V(Y)$ . In other words, if James decides to eavesdrop and overwrite one of the  $z_{rw}$  links, then the total dimension revealed to James about  $V(Y)$  using this link is one (either the subspace he reads, or the subspace he inserts). To see this, recall that James eavesdrops  $z_{ro}$  links and can blindly jam  $z_{wo}$  links. This reveals to James a subspace of dimension  $z_{ro} + z_{wo}$  about  $V(Y)$ . Assume that James observes and overwrites one link of the  $z_{rw}$  links and only eavesdrops on the others. If our argument does not hold, then this action reveals to James a subspace of dimension  $z_{rw} + 1$  about  $V(Y)$ , i.e., those  $z_{rw}$  links contribute to  $V(Y)$  with a subspace of dimension  $z_{rw} + 1$ . This is a contradiction of the network code for the following reason. For James to learn a  $z_{rw}$ -dimensional subspace about  $V(Y)$  from those links, he will observe a  $z_{rw} \times C$  transfer matrix multiplying a dimension  $C$  code. And this  $z_{rw} \times C$  transfer matrix is part of a full-rank  $C \times C$  transfer matrix. Therefore, those links can contribute in a subspace of dimension at most  $z_{rw}$  to  $V(Y)$ . Which means that every subspace added by James on those links wipes out the subspace he deleted from  $V(Y)$  and his total knowledge from those links about  $V(Y)$  is a  $z_{rw}$ -dimensional subspace. Thus, the dimension of subspace that James can make sure to appear at Bob's side is  $z_{ro} + z_{rw} + z_{wo}$ .  $\square$

According to Lemma 3, the received  $V(Y)$  can be expressed as  $V(Y) = V_{ro}(X) \oplus V_u(X) \oplus V_{rw}(S_{rw}) \oplus V_{wo}(S_{wo})$  where  $V_u(X)$  is distributed uniformly at random from James' perspective. Since each codeword is chosen uniformly at random, it is as if each  $V_u(X)$  is also chosen uniformly random. We will use the randomness in  $V_u(X)$  to argue that a confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$  can confuse at most  $n^3$  codewords in  $\mathcal{M}_{og}$  with high probability.

**Lemma 4.** *For any  $V_r(X)$  observed by a weak adversary through the network and for any  $V(S)$  that the adversary injects into the network, let  $V(\hat{X})$  be a confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$ . Define  $\mathcal{D}_1 \triangleq \{V(X_i) \in \mathcal{M}_{og} \mid d(V_{ro}(X) \oplus V_u(X_i) \oplus V(S), V(\hat{X})) \leq z_w\}$  as the set of codewords in  $\mathcal{M}_{og}$  confusable by  $V(\hat{X})$ . Based on the randomness in  $V_u(X)$ , we can write*

$$\Pr(\exists V_r(X), V(S), \text{ s.t. } |\mathcal{D}_1| \geq n^3) \leq e^{-\frac{\alpha_1}{3}n^3}.$$

*In other words, the probability that a confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$  confuses more than  $n^3$  codewords in  $\mathcal{M}_{og}$  is bounded from above by  $e^{-\frac{\alpha_1}{3}n^3}$ .*

*Proof.* The more powerful omniscient adversary that knows the codebook and the transmitted message operates by carefully inserting errors to push the received codeword to the closest codeword (different than the transmitted one) in the codebook. To

emulate such a powerful adversary, the best strategy for James (a weak adversary) is to fully leverage his knowledge and push  $V(Y) = V_{ro}(X) \oplus V_u(X) \oplus V(S)$  towards  $V(\hat{X})$  that satisfies  $V(\hat{X}) = V_{ro}(X) \oplus V_u(\hat{X}) \oplus V(S)$ . This means that James chooses a codeword compatible with his observation, deemed to be close to the transmitted codeword, and tries to push  $V(Y)$  towards that codeword. Otherwise, James will not be using his power efficiently. We do the analysis for a given  $V_r(X)$  and a given  $V(S)$ . We then take a union bound over all possible  $V_r(X)$  and  $V(S)$ .

A codeword  $V(\hat{X})$  confuses  $V(X_i) \in \mathcal{M}_{og}$  if the following holds

$$d(V_{ro}(\hat{X}) \oplus V_u(\hat{X}) \oplus V(S), V_{ro}(X_i) \oplus V_u(X_i) \oplus V(S)) \leq z_w.$$

Notice that James has full control over  $V(S)$  and that all codewords  $V(X_i) \in \mathcal{M}_{og}$  satisfy  $V_{ro}(X_i) = V_{ro}(X)$ . To maximize the number of confusable codewords, James must chose  $V_{ro}(\hat{X}) = V_{ro}(X)$ . The only uncertainty that remains from James' perspective is in  $V_u(X)$  which remains uniformly distributed. Therefore, all we have to count is the number of codewords in  $\mathcal{M}_{og}$  that satisfy  $d(V_u(\hat{X}), V_u(X_i)) \leq z_w$ . By definition of the injection distance given in Eqn. (3), this implies that  $\dim(V_u(\hat{X}) \cap V_u(X_i)) \geq c - z_w$ .

Recall that  $\dim(V_u(X_i)) = \dim(V_u(\hat{X})) = c - z_{ro} - z_w$ . Therefore, for a fixed  $V_u(\hat{X})$ , the number of  $V_u(X_i)$  that have an intersection of dimension at least  $c - 2z_w - z_{ro}$  with  $V_u(\hat{X})$  is bounded by

$$\begin{aligned} \sum_{i=1}^{z_w} \binom{c - z_{ro} - z_w}{c - z_{ro} - z_w - i}_q \binom{n}{i}_q &\leq z_w \binom{c - z_{ro} - z_w}{\frac{1}{2}(c - z_{ro} - z_w)}_q \binom{n}{z_w}_q \\ &\leq 4z_w q^{(c - z_{ro} - z_w)^2 \frac{1}{4}} q^{nz_w - z_w^2} \end{aligned}$$

Thus, the probability that  $V(\hat{X})$  confuses  $V_{ro}(X) \oplus V_u(X_i) \oplus V(S)$  is bounded as follows

$$\begin{aligned} \Pr(V(\hat{X}) \text{ confuses } V(X_i)) &\leq \frac{4z_w q^{(c - z_{ro} - z_w)^2 \frac{1}{4}} q^{nz_w - z_w^2}}{\binom{n}{c - z_{ro} - z_w}_q} \\ &\leq 4z_w q^{-n(c - z_{ro} - 2z_w - \frac{(c - z_{ro} - z_w)^2 \frac{1}{4} - z_w^2}{n} + (c - z_{ro} - z_w)^2)} \\ &\leq 4z_w q^{-n}. \end{aligned}$$

The last inequality holds since  $c > z_{ro} + 2z_w$  and all the numbers in the exponent of  $q$  are integers. Thus, the expected number of codewords in  $\mathcal{M}_{og}$  that a confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$  can confuse is  $4z_w q^{-n} q^{n\epsilon_1} = q^{-n\epsilon_3}$ . Then, by the upper tail of the Chernoff bound [33, Eqn. (1.10.4)] we can argue that the probability that  $V(\hat{X})$  can confuse more than  $n^3$  codewords in  $\mathcal{M}_{og}$  is no more than  $e^{-\frac{n^3}{3}}$ . Then we take union bound over  $V_r(X)$  and  $V(S)$ , which are both exponentially in  $n$ , to show that the lemma holds with some  $\alpha_1 > 0$ .  $\square$

Based on Lemma 2 and Lemma 4, we can argue that with high probability at most  $n^6$  codewords in  $\mathcal{M}_{og}$  can be confused by a confusing codeword in  $\mathcal{C} \setminus \mathcal{M}_{og}$ .

2) *Type-II Error*: In this case, we consider the confusing codeword  $V(\hat{X})$  to be in  $\mathcal{M}_{og}$ . Recall that the size of  $\mathcal{M}_{og}$  is  $q^{n\epsilon_1}$ . We pick each element of  $\mathcal{M}_{og}$  uniformly at random from the set of all compatible codewords. Recall that the number of possible compatible codewords is  $\binom{n}{c - z_r}_q$ .

Then we arrange the codewords in  $\mathcal{M}_{og}$  in the following way: *i)* Initialize a  $q^{\frac{n\epsilon_1}{2}} \times q^{\frac{n\epsilon_1}{2}}$  grid; *ii)* Arrange each codeword of  $\mathcal{M}_{og}$  randomly into the grid. We pick any row or column from the grid and refer to it as the mini-oracle-given set  $\mathcal{M}_{mi}$ . In this way, we divide the codewords in  $\mathcal{M}_{og}$  into two parts:  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  and  $\mathcal{M}_{mi}$ . Here the set  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  is considered independent from  $\mathcal{M}_{mi}$  in the unseen dimension  $c - z_r$  subspace. Now we consider a codeword  $V(\hat{X})$  in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  that may confuse a codeword in  $\mathcal{M}_{mi}$ .

**Lemma 5.** *For any  $V_r(X)$  observed by James, let  $S_{rw}$  and  $S_{wo}$  be his jamming action and recall the decoding region defined as  $\mathcal{D}(Y_i) = \{V(X) \mid \dim(V(X)) = c, d(V(X), V(Y_i)) \leq z_w\}$  where  $V(Y_i) = V_{ro}(X) \oplus V_u(X_i) \oplus V_{rw}(S_{rw}) \oplus V_{wo}(S_{wo})$ . Then, based on the randomness from the subspace  $V_u(X)$  of  $V(X)$  that is not observed by James, we can write*

$$\Pr \left( \exists V_r(X), V(S), \text{ s.t. } \left| \bigcup_{V(X_i) \in \mathcal{M}_{mi}} \mathcal{D}(Y_i) \cap (\mathcal{M}_{og} \setminus \mathcal{M}_{mi}) \right| \geq n^3 \right) \leq e^{-\frac{\alpha_2}{3} n^3}.$$

*In other words, for any  $V_r(X)$  observed by James and any  $V(S)$  that James inject into the network, the probability that more than  $n^3$  codewords in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  fall into the union of the decoding regions  $\mathcal{D}(Y_i)$  of codewords  $X_i \in \mathcal{M}_{mi}$  is bounded from above by  $e^{-\frac{\alpha_2}{3} n^3}$ .*

*Proof.* Recall from Eqn. (6) that the cardinality of the decoding region of  $V(Y)$  is no more than  $16z_w q^{cz_w - z_w^2} q^{nz_w - z_w^2}$ . Given an observation  $V_r(X)$ , the set  $\mathcal{M}_{mi}$  and a jamming action  $V(S)$ , let  $\Lambda_{mi} \triangleq \bigcup_{V(X_i) \in \mathcal{M}_{mi}} \mathcal{D}(Y_i)$  be the union of the decoding

regions corresponding to all codewords in  $\mathcal{M}_{mi}$ . Then, the cardinality of  $\Lambda_{mi}$  is at most  $16z_w q^{Cz_w - z_w^2} q^{nz_w - z_w^2} q^{n\frac{\epsilon_1}{2}}$ . The probability that a codeword in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  falls in  $\Lambda_{mi}$ , i.e., is confusing, is given by

$$\begin{aligned} \frac{16z_w q^{Cz_w - z_w^2} q^{nz_w - z_w^2} q^{n\frac{\epsilon_1}{2}}}{q^{n(C-z_r) - (C-z_r)^2}} &= 16z_w q^{-n(C-z_r-z_w-\frac{\epsilon_1}{2} + \frac{2z_w^2 - Cz_w}{n})} \\ &= q^{-n\epsilon_4} \end{aligned}$$

where the denominator is the size of the subspace that is not observed by James and  $\epsilon_4$  is some positive number. Hence, the expected number of confusing codewords is  $q^{-n\epsilon_4} q^{n\epsilon_1} = q^{-n\epsilon_5}$  for some positive  $\epsilon_5 = \epsilon_4 - \epsilon_1$ . By applying the upper tail of the Chernoff bound [33, Eqn. (1.10.4)], we conclude that the probability of having more than  $n^3$  confusing codewords in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  is bounded from above by  $e^{-\frac{n^3}{3}}$ .

Taking the union bound over the size of  $V_r(X)$  and  $V(S)$ , we can argue that with probability at most  $e^{-\frac{\alpha_2}{3}n^3}$  for some coefficient  $\alpha_2 > 0$ , there are more than  $n^3$  confusing codewords in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$ .  $\square$

Next we need to show that each confusing codeword in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  can confuse at most  $n^3$  codewords in  $\mathcal{M}_{mi}$ . The argument is similar to the one made in Lemma 4.

**Lemma 6.** *For any  $V_r(X)$  observed by a weak adversary through the network and for any  $V(S)$  that the adversary injects into the network, let  $V(\hat{X})$  be a confusing codeword in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$ . Define  $\mathcal{D}_2 \triangleq \{V(X_i) \in \mathcal{M}_{mi} \mid d(V_{ro}(X) \oplus V_u(X_i) \oplus V(S), V(\hat{X})) \leq z_w\}$  as the set of codewords in  $\mathcal{M}_{mi}$  confusable by  $V(\hat{X})$ . Based on the randomness in  $V_u(X)$  we can write*

$$\Pr(\exists V_r(X), V(S), \text{ s.t. } |\mathcal{D}_2| \geq n^3) \leq e^{-\frac{\alpha_3}{3}n^3}.$$

*In other words, the probability that a confusing codeword in  $\mathcal{M}_{og} \setminus \mathcal{M}_{mi}$  confuses more than  $n^3$  codewords in  $\mathcal{M}_{mi}$  is bounded from above by  $e^{-\frac{\alpha_3}{3}n^3}$ .*

*Proof.* The proof is similar to the proof of Lemma 4. First by Lemma 3, despite that James manages to eavesdrop on  $z_r$  links and overwrite  $z_w$  links, he can control a subspace of dimension at most  $z_{ro} + z_{rw} + z_{wo}$  in  $V(Y)$ . Thus, the same analysis made in Lemma 4 holds and  $V(\hat{X})$  can confuse  $V_{ro}(X) \oplus V_u(X_i) \oplus V(S)$  with probability at most  $4z_w q^{-n}$ . Then, the expected number of confusable codewords in  $\mathcal{M}_{mi}$  is  $4z_w q^{-n} q^{\frac{n\epsilon_1}{2}} = q^{-n\epsilon_6}$ . By the Chernoff bound [33, Eqn. (1.10.4)] we can argue that with probability at most  $e^{-\frac{n^3}{3}}$ , there are more than  $n^3$  codewords in  $\mathcal{M}_{mi}$  that are confusable with this  $V(\hat{X})$ .

Taking the union bound over the size of  $V_r(X)$  and  $V(S)$ , which are both exponentially in  $n$ , we argue that the lemma holds for some  $\alpha_3 > 0$ .  $\square$

Based on the Lemma 5 and Lemma 6, we can argue that for one row or one column to be the  $\mathcal{M}_{mi}$ , and for any  $V_r(X)$  and  $V(S)$ , the probability having more than  $n^6$  confusable codewords in the  $\mathcal{M}_{mi}$  is bounded from above by  $e^{-\frac{\alpha_2 + \alpha_3}{3}n^3}$ . Also, note that the confusable codewords will be either in a row or in a column of  $\mathcal{M}_{og}$ . Henceforth, the total number of confusable codewords that can be confused by a confusing codeword from  $\mathcal{M}_{og}$  in the whole  $\mathcal{M}_{og}$  is no more than  $2n^6 q^{\frac{n\epsilon_1}{2}}$  with high probability.

Overall, based on the analysis for type-I error and type-II error, we proved that with high probability, there are at most  $n^6 + 2n^6 q^{\frac{n\epsilon_1}{2}}$  confusable codewords in  $\mathcal{M}_{og}$ . We can conclude that the probability of James' attack succeeding in confusing the actually transmitted codeword is at most  $\frac{n^6 + 2n^6 q^{\frac{n\epsilon_1}{2}}}{q^{n\epsilon_1}} \approx \frac{2n^6}{q^{n\epsilon_1/2}}$ , which is still exponentially small in  $n$ .

### C. Converse

We now argue that the rate achieved by our scheme is optimal by providing jamming strategies for James that ensure that any rate higher than those attained by our schemes must result in a non-vanishing probability of error.

The rate converse of  $C - z_w$  follows by standard cutset arguments; since there are at most  $Cn$  symbols on the min-cut, if James corrupts  $z_w n$  of these symbols with random noise, the residual throughput is at most  $(C - z_w)n$ . The tighter rate converse of  $(C - 2z_w)^+$  corresponding to the strong adversary regime of  $z_{ro} + 2(z_{rw} + z_{wo}) \geq C$  follows from the techniques in [18]. In [18], even for the special case of a "parallel-edge network" comprising simply of  $C$  edges linking the source to the sink, the jammer proceeds as follows. Roughly speaking, James first observes the transmissions on the  $z_{ro}$  read-only links, picks a codeword  $X'$  uniformly at random from all possible codewords compatible with these observations, and then on the  $z_{wo} + z_{rw}$  links he can write on, he replaces the transmissions with the transmissions corresponding to  $X'$ . It can then be seen that the decoder Bob is unable to determine whether Alice's actual transmission is  $X$  or  $X'$ . In [18] this proof is formalized by combining with a Fano's inequality-based argument to show that the probability of error is bounded away from zero for any code (including scenarios wherein stochastic encoding is employed). When specialized to the specific subspace codes used in this work, James' attack proceeds as follows. If the rate exceeds  $C - 2z_w$ , then by the strong-adversary condition he can pick a codeword  $V(X')$  compatible with his observations on his read-only links, and then replace the transmissions on the  $z_w$  he can corrupt to be compatible with this  $V(X')$ .

#### D. Secrecy capacity

We explain how to use the coset code of [20] to securely achieve the rate  $R_{sec}^* = C - z_r - z_w - \epsilon$  for the weak adversary regime, i.e.,  $C > z_{ro} + 2z_w$ . Recall that the capacity for the strong adversary regime is equal to zero.

The coding strategy consists of using an MDS code  $\mathcal{C}_{MDS} \in \mathbb{F}_q^{\mathbb{R}}$  with length equal to  $\mathbb{R}$  and dimension equal to  $z_r$ . Alice partitions the space  $\mathbb{F}_q^{\mathbb{R}}$  into  $q^{n(\mathbb{R}-z_r)}$  cosets of  $\mathcal{C}_{MDS}$ , each of size  $q^{nz_r}$ . Let  $H$  be the  $(\mathbb{R} - z_r) \times \mathbb{R}$  parity check of  $\mathcal{C}_{MDS}$ . To send a message  $m$  that consists of  $n(\mathbb{R} - z_r)$  symbols, Alice chooses a vector  $s$  uniformly at random from the coset  $\mathcal{C}_1 \subset \mathbb{F}_q^{\mathbb{R}}$  of  $\mathcal{C}_{MDS}$  that satisfies  $m = Hs$  for all  $s \in \mathcal{C}_1$ . Due to the properties of MDS codes, observing any  $nz_r$  or less symbols of  $s$  does not reveal any information about  $m = Hs$ . To send  $s$  over the network, Alice represents  $s$  as a vector in  $\mathbb{F}_q^{mz_r}$  and encodes it using the random subspace code introduced in this paper. Perfect secrecy is maintained because James observes at most  $z_r$  links which reveal at most  $nz_r$  symbols of  $s$ . Reliability against James' jamming attack is ensured with high probability by the subspace codes. After receiving and decoding  $s$  with high probability, Bob simply computes  $m = Hs$  to recover the message.

Note that the network performs linear operations on the transferred packets which may give more information than intended to the adversary and break the perfect secrecy. The authors of [20] show that perfect secrecy is guaranteed under any random linear network code as long as all transfer matrices  $T_{z_r}$  of any collection of  $z_r$  links do not belong to the space spanned by the rows of  $H$ . This can be maintained by choosing a large enough field size  $q$ .

Reliable communication is guaranteed as long as  $\mathbb{R} = C - z_w - \epsilon$  for sufficiently small values of  $\epsilon$ . This ensures a secure and reliable transmission of a message  $m$  of length  $n(\mathbb{R} - z_r)$  and therefore achieves  $R_{sec} = C - z_r - z_w - \epsilon$ .

The fact that, for all parameter regimes in  $C, z_r, z_w$ , communication is simultaneously reliable and secure (even if one only requires weak secrecy) follows from the corresponding converse argument for parallel-edge networks with overwrite adversaries in [18].

#### IV. ACKNOWLEDGEMENT

RB's work was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 801434) and from the Technical University of Munich - Institute for Advanced Studies, funded by the German Excellence Initiative and European Union Seventh Framework Programme under Grant Agreement No. 291763. SJ's work was supported by funding from the Hong Kong UGC GRF grants 14304418, 14300617 and 14313116. YZ has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 682203-ERC-[Inf-Speed-Tradeoff].

#### REFERENCES

- [1] S. Li, "A short video describing the paper "Network Coding with Myopic Adversaries" by Sijie Li, Rawad Bitar, Sidharth Jaggi and Yihan Zhang," *Zoom*, 2021. [https://uhk.zoom.us/rec/share/xPwmmO5jVTZxbEIDCUoIACY\\_rcuRqkuq09D5fy4j8xBbtqdtTQaV1o-KohbvJOLS.SjKd6sBzYmKvyiHt?startTime=1612281070000](https://uhk.zoom.us/rec/share/xPwmmO5jVTZxbEIDCUoIACY_rcuRqkuq09D5fy4j8xBbtqdtTQaV1o-KohbvJOLS.SjKd6sBzYmKvyiHt?startTime=1612281070000).
- [2] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on information theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [3] 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.
- [4] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM transactions on networking*, vol. 11, no. 5, pp. 782–795, 2003.
- [5] 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.
- [6] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *Proceedings of the 12th annual international conference on Mobile computing and networking*, pp. 358–365, 2006.
- [7] 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.
- [8] "Inter-datacenter bulk transfers with codedbulk," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, USENIX Association, Apr. 2021.
- [9] R. W. Yeung, N. Cai, *et al.*, "Network error correction, i: Basic concepts and upper bounds," *Communications in Information & Systems*, vol. 6, no. 1, pp. 19–35, 2006.
- [10] N. Cai, R. W. Yeung, *et al.*, "Network error correction, ii: Lower bounds," *Communications in Information & Systems*, vol. 6, no. 1, pp. 37–54, 2006.
- [11] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros, "Resilient network coding in the presence of byzantine adversaries," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2596–2603, 2008.
- [12] 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.
- [13] D. Silva and F. R. Kschischang, "Universal secure error-correcting schemes for network coding," in *2010 IEEE International Symposium on Information Theory*, pp. 2428–2432, IEEE, 2010.
- [14] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.
- [15] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.
- [16] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network codes resilient to jamming and eavesdropping," *IEEE/ACM Transactions on Networking*, vol. 22, no. 6, pp. 1978–1987, 2014.
- [17] M. Hayashi, M. Owari, G. Kato, and N. Cai, "Secrecy and robustness for active attack in secure network coding," in *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 1172–1176, IEEE, 2017.
- [18] Q. Zhang, S. Kadhe, M. Bakshi, S. Jaggi, and A. Sprintson, "Talking reliably, secretly, and efficiently: A "complete" characterization," *2015 IEEE Information Theory Workshop*, pp. 1–5, 2015.
- [19] B. K. Dey, S. Jaggi, and M. Langberg, "Sufficiently myopic adversaries are blind," *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5718–5736, 2019.

- [20] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1361–1371, 2012.
- [21] S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing dynamic distributed storage systems against eavesdropping and adversarial attacks," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6734–6753, 2011.
- [22] N. B. Shah, K. Rashmi, and K. Ramchandran, "Secure network coding for distributed secret sharing with low communication cost," in *2013 IEEE International Symposium on Information Theory*, pp. 2404–2408, IEEE, 2013.
- [23] Q. Wang, H. Sun, and M. Skoglund, "The  $\epsilon$ -error capacity of symmetric pir with byzantine adversaries," in *2018 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2018.
- [24] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. A. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security, and privacy," in *The 22nd International Conference on Artificial Intelligence and Statistics*, pp. 1215–1225, PMLR, 2019.
- [25] Y. Yang, T. Ho, and W. Huang, "Network error correction with limited feedback capacity," *arXiv preprint arXiv:1312.3823*, 2013.
- [26] 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.
- [27] P. Tian, S. Jaggi, M. Bakshi, and O. Kosut, "Arbitrarily varying networks: Capacity-achieving computationally efficient codes," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 2139–2143, IEEE, 2016.
- [28] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in *2006 40th Annual Conference on Information Sciences and Systems*, pp. 857–863, IEEE, 2006.
- [29] F. Zhao, T. Kalker, M. Médard, and K. J. Han, "Signatures for content distribution with network coding," in *2007 IEEE International Symposium on Information Theory*, pp. 556–560, IEEE, 2007.
- [30] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings IEEE International Symposium on Information Theory*, p. 323, IEEE, 2002.
- [31] H. Yao, S. Jaggi, and M. Chen, "Passive network tomography for erroneous networks: A network coding approach," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5922–5940, 2012.
- [32] N. Alon and J. H. Spencer, *The probabilistic method*. John Wiley & Sons, 2004.
- [33] B. Doerr, "Probabilistic tools for the analysis of randomized optimization heuristics," *CoRR*, vol. abs/1801.06733, 2018.