Optimal Information Security Against Limited-view Adversaries: Beyond MDS Codes

Qiaosheng Zhang, Swanand Kadhe, Mayank Bakshi, *Member, IEEE*

Sidharth Jaggi, *Senior Member, IEEE* and Alex Sprintson, *Senior Member, IEEE*

***Abstract*—Maximum distance separable (MDS) codes are often considered to have the optimal error correction capability against malicious adversaries because they achieve the Singleton bound in terms of the rate-distance tradeoff. However, by allowing a vanishing probability of decoding error and considering an adversary with limited knowledge, it is interesting to understand whether a rate higher than the Singleton bound is achievable, and if so, what the optimal rate is. To answer these questions, we instantiate the aforementioned problem as a communication problem where the transmission medium is a *wiretap multipath network* that consists of multiple parallel links. A malicious adversary is able to eavesdrop on a subset of links, and also jam on a potentially overlapping subset of links. The primary objective is to ensure the communication is robust to adversarial jamming; additionally, another goal is to guarantee that the communication is information-theoretically secure with respect to the adversary. We present a complete characterization of both *capacity* and *secrecy capacity* as functions of the number of links that can be eavesdropped and/or jammed. Our achievability schemes are computationally efficient, and rely on a non-trivial combination of MDS codes and a pairwise hashing scheme.**

***Index Terms*—Maximum distance separable (MDS) codes, Adversarial jamming, Information-theoretic security.**

I. Introduction

MAXIMUM distance separable (MDS) codes are a type of error-correcting code that have the highest possible pairwise distance between codewords for a given code length and message length, in the sense that they match the theoretical limit on the distance of any codes (known as the *Singleton bound* [2]). Assuming that the code length is L and there is a malicious adversary who can jam up to z locations of the codeword, to ensure reliable decoding without any error, the Singleton bound implies that the message length should be at most $L-2z$. This can be achieved by any MDS codes. However, when it is allowed to tolerate a vanishing probability of decoding error (with respect to the increase of field size), and when the adversary only has limited knowledge about the codeword (called the *limited-view adversary*, in contrast to the adversary who has full knowledge of the codeword), this paper shows that the Singleton bound is no longer valid, and that a rate higher than $L-2z$ is achievable. Interestingly, we figure out that the optimal rate depends not only on the number of locations that the adversary can jam, but also on the number of locations that the adversary can eavesdrop, as well as the intersection between the eavesdropped and jammed locations.

Apart from reliable decoding, another common objective is to avoid the leakage of information to the adversary who is also eavesdropping. In this work, we adopt the notion of *information-theoretic secrecy* [3] as a measure of the information leakage, and also characterize the optimal rate when it is required to achieve both reliable decoding and information-theoretic secrecy.

The coding problem discussed above, either with or without the secrecy consideration, has close connections to a variety of real-world applications. In Subsections A and B below, we introduce two representative applications — one arising from communication systems and another arising from distributed storage systems — through which we further emphasize the significance of our problem and also provide an overview of our main results. In Subsection C, we present a unified framework, called the *wiretap multipath network*, that formally describes the problem of interest in this paper. Following that, we provide a summary of contributions of this work.

A. Motivating Example 1: a communication setting

Suppose a transmitter Alice wishes to wirelessly transmit a message to a receiver Bob by communicating over L orthogonal/independent frequencies. Their communication is intercepted by a limited-view adversary James who has his receiver tuned to a subset $\mathcal{Z}_{\mathrm{E}}$ of the L frequencies, and can jam a potentially overlapping subset $\mathcal{Z}_{\mathrm{J}}$ of the L frequencies by adding artificial noise. Also assume that the artificial noise imposed by James is the only source of noise in the transmission. Based on the eavesdropped signals and the knowledge of the codebook, James is thus able to cleverly design his jamming strategy and to maximize the damage to the communication. For this communication setting, we wish to answer the following two questions:

- *Question 1: Without knowing which frequencies James are eavesdropping/jamming, what is the optimal rate*[1] *at which Bob can decode Alice's message correctly?*
- *Question 2: What is the optimal rate if we also wish to keep the message information-theoretically secret from James simultaneously?*

Q. Zhang is with Shanghai Artificial Intelligence Laboratory. S. Kadhe is with IBM's Almaden Research Center. M. Bakshi is with the School of Electrical, Computer and Energy Engineering, Arizona State University. S. Jaggi is with the School of Mathematics, University of Bristol. A. Sprintson is with the Department of ECE, Texas A&M University. This work was presented in part at the 2015 IEEE International Theory Workshop (ITW) [1].

[1]The notion of *optimal rate* (also called the *capacity*) is formally defined in Section II. Roughly speaking, the *rate* is defined as the logarithm of message size normalized by the blocklength, while the capacity is defined as the maximum rate that can ensure a vanishing decoding error probability (as the blocklength tends to infinity).

These questions are precisely answered in Theorem 1, which shows that when the channel corresponding to each frequency is of unit capacity, asymptotically the optimal rate in Question 1 is $L - |\mathcal{Z}_{\rm J}|$ if $|\mathcal{Z}_{\rm J}| + |\mathcal{Z}_{\rm E}| < L$, and is $\max\{L - |\mathcal{Z}_{\rm J}| - |\mathcal{Z}_{\rm J} \cap \mathcal{Z}_{\rm E}|, 0\}$ otherwise. For Question 2, the optimal rate is $L - |\mathcal{Z}_{\rm J}| - |\mathcal{Z}_{\rm E}|$ if $|\mathcal{Z}_{\rm J}| + |\mathcal{Z}_{\rm E}| < L$, and is zero otherwise.

B. Motivating example 2: a storage system setting

Suppose Alice wants to store data in L disks in a distributed manner. An adversary James has the permission to read a subset $\mathcal{Z}_{\rm E}$ of the disks, and has the permission to overwrite the data in a subset $\mathcal{Z}_{\rm J}$ of the disks. For this storage system setting, we arise similar questions:

- *Question 3: Without knowing which disks James has access to read/overwrite, what is the maximum amount of data that Alice can store reliably?*
- *Question 4: What is the maximum amount of data that Alice can store reliably and secretly?*

We show in Theorem 2 that if the form of adversary's attack is to *overwrite* data (rather than to add additive noise in the wireless setting), and when each disk is of unit (or equal) capacity, asymptotically the maximum rate in Question 3 is $L - |\mathcal{Z}_{\rm J}|$ if $|\mathcal{Z}_{\rm E} \setminus \mathcal{Z}_{\rm J}| + 2|\mathcal{Z}_{\rm J}| < L$, and is $\max\{L - 2|\mathcal{Z}_{\rm J}|, 0\}$ otherwise. For Question 4, the maximum rate is $L - |\mathcal{Z}_{\rm J}| - |\mathcal{Z}_{\rm E}|$ if $|\mathcal{Z}_{\rm E} \setminus \mathcal{Z}_{\rm J}| + 2|\mathcal{Z}_{\rm J}| < L$, and is zero otherwise.

C. A formal and unified model—the wiretap multipath network

We now introduce a formal and unified model, named the *wiretap multipath network*, that encompasses the two settings described in Subsections A and B as special cases. We point out that, although the wiretap multipath network described below is intrinsically a communication model, it can nevertheless be mapped to distributed storage systems since one can view a storage system as a special communication system that transmits information from the past to the future. Thus, from now on, the main focus of this work is on the wiretap multipath network.

Model descriptions: The wiretap multipath network is a communication network that consists of L parallel links, denoted by $\mathcal{E} \triangleq \{E_1, E_2, \ldots, E_L\}$. The limited-view adversary James can eavesdrop on a subset of links $\mathcal{Z}_{\rm E} \subseteq \mathcal{E}$ (the "eavesropped" links) and jam on another subset of links $\mathcal{Z}_{\rm J} \subseteq \mathcal{E}$ (the "jammed" links). The links in $\mathcal{Z}_{\rm E} \cup \mathcal{Z}_{\rm J}$ are partitioned into three subsets — (i) the "eavesdrop-jam" links $\mathcal{Z}_{\rm EJ} \triangleq \mathcal{Z}_{\rm E} \cap \mathcal{Z}_{\rm J}$ that James can both eavesdrop on and jam, (ii) the "eavesdrop-only" links $\mathcal{Z}_{\rm EO} \triangleq \mathcal{Z}_{\rm E} \setminus \mathcal{Z}_{\rm EJ}$ that James can only eavesdrop on (but not jam), and (iii) the "jam-only" links $\mathcal{Z}_{\rm JO} \triangleq \mathcal{Z}_{\rm J} \setminus \mathcal{Z}_{\rm EJ}$ that James can only jam (but not eavesdrop on). The cardinalities of $\mathcal{Z}_{\rm EJ}$, $\mathcal{Z}_{\rm EO}$, $\mathcal{Z}_{\rm JO}$ are bounded from above as $|\mathcal{Z}_{\rm EJ}| \leq z_{\rm EJ}$, $|\mathcal{Z}_{\rm EO}| \leq z_{\rm EO}$, and $|\mathcal{Z}_{\rm JO}| \leq z_{\rm JO}$. Thus, James' power can be measured by the *power vector* $\mathbf{z} = (z_{\rm EJ}, z_{\rm EO}, z_{\rm JO})$. The adversary considered here is quite strong — he is computationally unbounded, is able to choose *any* subsets $\mathcal{Z}_{\rm EJ}, \mathcal{Z}_{\rm EO}, \mathcal{Z}_{\rm JO} \subseteq \mathcal{E}$ that satisfy the constraints given by $\mathbf{z}$, and knows *a priori* the communication scheme (including the encoder, decoder, and codebook) used by Alice and Bob. As a consequence, James can cleverly design his jamming strategy on $\mathcal{Z}_{\rm J}$, based on his knowledge of the communication scheme and the transmissions on $\mathcal{Z}_{\rm E}$. On the other hand, Alice and Bob only know the values of $z_{\rm EJ}, z_{\rm EO}, z_{\rm JO}$, but do not know *a priori* the actual sets $\mathcal{Z}_{\rm EJ}$, $\mathcal{Z}_{\rm EO}$ and $\mathcal{Z}_{\rm JO}$ that are controlled by James, nor do they know his jamming strategy.

We consider two ways in which James could attack the links — *additive jamming* and *overwrite jamming*. Under additive jamming, James can only impose additive noise; this is a natural attack model in wireless networks (as in Subsection A). Under overwrite jamming, James is allowed to completely *replace* the original transmissions with his own transmission patterns; this appears more natural in computer networks and distributed storage systems (as in Subsection B).

Objectives: The primary objective is to ensure the communication to be *robust* to James' jamming; that is, Bob should be able to reliably decode Alice's message with high probability regardless of James' jamming strategy. On top of robustness, an additional objective is to ensure the communication is information-theoretically secure with respect to James, i.e., the normalized mutual information between the message and James' observations on $\mathcal{Z}_{\rm E}$ tends to zero.

Main contributions: Our main contributions are as follows:

1) Given a constraint $\mathbf{z} = (z_{\rm EJ}, z_{\rm EO}, z_{\rm JO})$ on James' power, we provide a complete characterization on both the *capacity* (for reliable communication only) and *secrecy capacity* (for reliable and secure communication), for both additive and overwrite jamming (see Theorems 1 and 2). Interestingly, in each of the settings we examine, the adversary James can always be classified into one of two regimes — either a *weak adversary regime*, or a *strong adversary regime* — based on $\mathbf{z} = (z_{\rm EJ}, z_{\rm EO}, z_{\rm JO})$. These two regimes are fundamentally different in the sense that Alice and Bob are able to detect the set $\mathcal{Z}_{\rm J}$ (jammed by James) in the weak adversary regime, while it is impossible to fully detect $\mathcal{Z}_{\rm J}$ in the strong adversary regime. This leads to fundamentally different capacities and secrecy capacities in the two regimes.[2]
2) En route to characterizing the capacity and secrecy capacity, we develop a unified achievability scheme that can be used for reliable communication, either with or without secrecy guarantees. This scheme relies on a non-trivial combination of MDS codes and a *pairwise-hashing scheme* [4] (which is used to detect the links jammed by James). To achieve information-theoretic secrecy, Alice generates uniformly distributed *private keys*, and the crux is to mix the message with private keys at the encoder.

Notations: Random variables and their realizations are respectively denoted by uppercase and lowercase letters, e.g., X and x. Sets are denoted by calligraphic letters, e.g., $\mathcal{X}$. Vectors are denoted by boldface letters, e.g., $\mathbf{X}$ and $\mathbf{x}$. For two vectors $\mathbf{x}_1$

[2]Roughly speaking, in the weak adversary regime, the transmissions on $\mathcal{Z}_{\rm J}$ can be treated as erasures, and the information transmitted on the remaining links can be fully utilized. In contrast, in the strong adversary regime, it is necessary to back off on the rate and rely on classical error-correcting codes to ensure reliable communication on some subset of the links.

and $\mathbf{x}_2$, we use $[\mathbf{x}_1, \mathbf{x}_2]$ to represent the stacking of the two vectors. Matrices are denoted by boldface underlined letters with dimensions on the bottom-right, e.g., $\underline{\mathbf{X}}_{m\times n}$, or simply $\underline{\mathbf{X}}$ when the dimensions are clear from the context. For any $x \in \mathbb{R}$, we define $[x]^+ \triangleq \max\{0, x\}$. For any integers $a \leq b$, we define $[a:b] \triangleq \{a, a+1, \ldots, b\}$.

Paper outline: The rest of this paper is organized as follows. Section II introduces several works that have close connections to this paper. The problem setting is formally stated in Section III, and our main results are presented in Section IV. We provide the detailed proofs of our main results in Section V, and conclude this work in Section VI.

II. Related works

The problem of reliable communication (with no secrecy constraints) against a malicious adversary has been well-studied in the past. The capacity has been characterized under various settings, including the classical error-correction setup [2], [5]–[7] and the network error-correction setting [1], [4], [8]–[18]. In many models, a key feature is that the adversary James can decrease the capacity by *twice* the number of links he jams (i.e., inflicting "double-damage"). As an example, if James knew *precisely* which codeword was being transmitted (a so-called *omniscient adversary*), he could "push" Alice's codeword towards another "nearest codeword" — hence all pairs of potential codewords have to differ in at least *twice* the number of links that James can control. This is the essential reason behind the Singleton bound [2]. This heuristic also suggests an intuitive scheme for Bob's decoder— try to detect as many jammed links in $\mathcal{Z}_{\mathrm{J}}$ as possible and treat those as erasures. If James' jamming could be regarded as erasures, the capacity would only be decreased by the number of links he jams (i.e., inflicting "single-damage"). Critically, James is able to cause "double-damage" if he has sufficient information on $\mathcal{Z}_{\mathrm{E}}$ before choosing his jamming strategy on $\mathcal{Z}_{\mathrm{J}}$, and is only able to cause "single-damage" otherwise. This work establishes the connection between the degree of damage James causes and the amount of information needed.

Connections to prior works on wiretap multipath networks: The problem of reliable and secure communication over the wiretap multipath network has also received considerable attention in the literature. Ref. [8] considered the setting in which the sets that are eavesdropped and jammed (i.e., $\mathcal{Z}_{\mathrm{E}}$ and $\mathcal{Z}_{\mathrm{J}}$) are disjoint — this corresponds to a special case of this work with $z_{\mathrm{EJ}} = 0$. Ref. [4], [14] considered another extreme setting in which the adversary eavesdrops and jams on the *same* subset of links — this corresponds to another special case of this work with $z_{\mathrm{EO}} = z_{\mathrm{JO}} = 0$. We refer the readers to [15] for a survey. Recently works [19]–[21] have considered the problem of transmitting messages reliably and *stealthily* over multipath networks, wherein the additional objective is to hide the *fact* that communication is taking place.

Connections to secure network coding: In addition to the wiretap multipath network, several works [8], [12], [17], [18] have studied reliable and secure communication over more general networks where the links intersect with each other, which is known as the *secure network coding problem*. Although their model encompasses our multipath network as a special case, it is worth noting that none of these works have taken into account the effect of the intersection between the eavesdropped links and jammed links when characterizing the capacity and secrecy capacity of communication. To obtain a clearer understanding of the differences, we discuss and compare the results of [8], [12], [17], [18] with our own results in Remark 4, Section IV.

Connections to prior works on adversarial wiretap (AWTP) channels: Another model that is related to our setup is that of an AWTP channel [22], wherein the adversary can eavesdrop up to a given fraction of symbols sent over a channel, and can jam another (possibly intersecting) fraction of symbols. There are two key differences from our work: (i) they only considered the additive jamming model, and (ii) the capacity characterization is parametrized with "coarser granularity" in the sense that the adversary's power is measured in terms of the *total* number of eavesdropped links (of size z_{E}) and jammed links (of size z_J), instead of $\mathbf{z} = (z_{\mathrm{EJ}}, z_{\mathrm{EO}}, z_{\mathrm{JO}})$ as considered in this work. We also note that the recent work [23] considered the problem of secure private matrix multiplication; while their problem of interest differs from ours, their main idea of designing codes that are beyond the Singleton bound is similar to our work.

Connections to the wiretap channel II with active adversaries: The paper [24] considered the problem of transmitting n bits over a channel in which a fraction of bits can be eavesdropped and jammed by a malicious adversary. A detailed comparison between [24] and this work is provided as follows.

- The number of eavesdopped/jammed bits in [24] grows linearly with the blocklength n. In contrast, in our work, the number of links, the number of eavesdropped links, and the number of jammed links are all constants that do not grow with the blocklength n.
- The adversary is only allowed to eavesdrop and jam on a *same* subset of bits, while this work allows the adversary to choose two different (and possibly overlapping) sets of links for eavesdropping and jamming.
- Perhaps more importantly, in our work, the transmission on each link can be viewed as *symbols over a field whose order grows with* n, and the symbols on links that are not chosen by the adversary are completely under the control of Alice and Bob. This is crucial for our pairwise hashing scheme to succeed. In contrast, the n transmitted bits in [24] are all binary; if we treat the transmitted bits as symbols over a field whose order grows with n, the adversary is able to eavesdrop/jam on *all* the symbols (i.e., choose at least one bit for each symbol), making reliable communication impossible.

Connections to secure message transmission: Our work is also related to the problem of secure message transmission (SMT) [25], [26]. Under SMT, a sender aims to communicate a message reliably and secretly to the receiver over multiple parallel links out of which a fraction of links are eavesdropped and another (possibly intersecting) fraction are jammed. There are a several differences from our model: (i) the SMT problem focuses on computing a lower bound on the number of links that are required for reliable and secure communication of

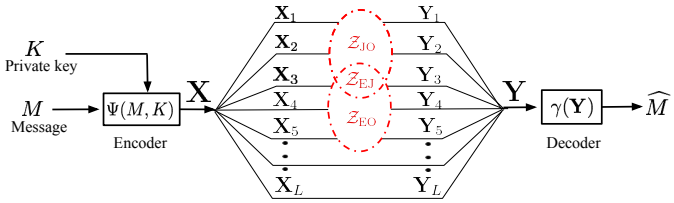

Fig. 1: System diagram for the wiretap multipath network consisting of L parallel links. The adversary can jam (but not eavesdrop) the set of links $\mathcal{Z}_{\rm JO} = \{E_1, E_2\}$, eavesdrop and jam the link $\mathcal{Z}_{\rm EJ} = \{E_3\}$, and eavesdrop (but not jam) the set of links $\mathcal{Z}_{\rm EO} = \{E_4, E_5\}$. As a result, $\mathbf{Y}_i$ is generally not equal to $\mathbf{X}_i$ for $i = 1, 2, 3$, and $\mathbf{Y}_i = \mathbf{X}_i$ for $i \in [4 : L]$.

one message symbol, and usually do not focus on providing information-theoretically tight capacity characterizations, (ii) most schemes are multi-round, 2-way protocols where the receiver can (actively) talk to the sender (though some protocols are indeed 1-way), (iii) the problem parametrization for eavesdropping and jamming is again in terms of $(z_{\rm E}, z_J)$.

III. Problem Statement

In the considered wiretap multipath network, it is assumed that each link E_i is of unit capacity (i.e., one bit per use) and the input and output are both binary. In the following, we formally describe the encoder, decoder, and possible adversarial actions for a code for *blocklength* n.[3] The system diagram of the wiretap multipath network model is illustrated in Fig. 1.

A. Encoder and Decoder

The transmitter Alice encodes a uniformly distributed message $M \in \mathcal{M}$ to a codeword $\mathbf{X} \in \{0,1\}^{Ln}$, possibly with the help of a private key $K \in \mathcal{K}$. The receiver Bob receives $\mathbf{Y} \in \{0,1\}^{Ln}$ and outputs a message reconstruction $\widehat{M}$ based on $\mathbf{Y}$. The encoding and decoding functions respectively take the form $\Psi : \mathcal{M} \times \mathcal{K} \to \{0,1\}^{L\times n}$ and $\gamma : \{0,1\}^{L\times n} \to \mathcal{M}$. Furthermore, we denote the sub-codeword transmitted and received on the i-th link E_i as $\mathbf{X}_i \in \{0,1\}^n$ and $\mathbf{Y}_i \in \{0,1\}^n$, respectively. The *rate* R is defined as $R \triangleq (\log \mathcal{M})/n$.

Remark 1. While the presentation here focuses on the simple case of a binary input alphabet, we point out that the input alphabet size can be generalized to any prime power in a straightforward manner, without affecting the main results.

B. The adversary and the induced channel

Out of the L links of the multipath network, James is able to eavesdrop (but not jam) a subset $\mathcal{Z}_{\rm EO}$, jam (but not eavesdrop) a subset $\mathcal{Z}_{\rm JO}$, and eavesdrop and jam a subset $\mathcal{Z}_{\rm EJ}$, where $|\mathcal{Z}_{\rm EO}| \le z_{\rm EO}$, $|\mathcal{Z}_{\rm JO}| \le z_{\rm JO}$, and $|\mathcal{Z}_{\rm EJ}| \le z_{\rm EJ}$. James' power is measured by the power vector $\mathbf{z} = (z_{\rm EJ}, z_{\rm EO}, z_{\rm JO})$. For notational convenience, we also define $z_{\rm E} \triangleq z_{\rm EO} + z_{\rm EJ}$ and $z_J \triangleq z_{\rm EJ} + z_{\rm JO}$. Alice and Bob know the value of $\mathbf{z}$; however, they do not know how James chooses $\mathcal{Z}_{\rm EO}$, $\mathcal{Z}_{\rm JO}$ $\mathcal{Z}_{\rm EJ}$, as well as his jamming strategy in advance. On the contrary, the scheme used by Alice and Bob is available to James.

Below, we discuss two types of jamming that are considered in this work, through which we also elucidate the connection between the input and output of the channel.

1) Under additive jamming, James is able to impose additive noise $\mathbf{N}_i \in \{0,1\}^n$ on each link E_i that belongs to $\mathcal{Z}_{\rm J} = \mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$. Bob's received vector $\mathbf{Y}_i = \mathbf{X}_i \oplus \mathbf{N}_i$ if $E_i \in \mathcal{Z}_{\rm J}$, and $\mathbf{Y}_i = \mathbf{X}_i$ otherwise, where '$\oplus$' is the bit-wise XOR.
2) Under overwrite jamming, James is able to replace the transmissions on $E_i \in \mathcal{Z}_{\rm J}$ completely. We denote James' jamming vector on each link $E_i \in \mathcal{Z}_{\rm J}$ by $\mathbf{N}_i \in \{0,1\}^n$. Bob's received vector $\mathbf{Y}_i = \mathbf{N}_i$ if $E_i \in \mathcal{Z}_{\rm J}$, and $\mathbf{Y}_i = \mathbf{X}_i$ otherwise.

C. Reliability and Secrecy

Reliability is measured via the *error probability* $P_{\rm err} \triangleq \Pr(M \neq \widehat{M})$, which is averaged over the message and maximized over James' jamming strategy. In parallel to reliability, as a subsidiary communication goal, we may *also* aim to achieve information-theoretic secrecy. We denote the sub-codewords on $\mathcal{Z}_{\rm E}$ (the set of links eavesdropped by James) by $\mathbf{X}_{\mathcal{Z}_{\rm E}}$. We say the communication achieves information-theoretic secrecy if regardless of which $\mathcal{Z}_{\rm E}$ is chosen, the normalized mutual information between the message and James' observation $\mathbf{X}_{\mathcal{Z}_{\rm E}}$ tends to zero, i.e. $\lim_{n\to\infty} I\left(M; \mathbf{X}_{\mathcal{Z}_{\rm E}}\right)/n = 0$ for every $\mathcal{Z}_{\rm E} \subseteq \mathcal{E}$ such that $|\mathcal{Z}_{\rm E}| \le z_{\rm EO} + z_{\rm EJ} = z_{\rm E}$.

Definition 1 (Capacity)**.** *A rate R is said to be* achievable *if there exists a sequence of codes with increasing blocklength n such that $\lim_{n\to\infty} \log|\mathcal{M}|/n \ge R$ and $\lim_{n\to\infty} P_{\rm err} = 0$. The* capacity *is defined as the supremum of all achievable rates.*

Definition 2 (Secrecy capacity)**.** *A rate R is said to be* securely achievable *if there exists a sequence of codes with increasing blocklength n such that $\lim_{n\to\infty} \log|\mathcal{M}|/n \ge R$, $\lim_{n\to\infty} P_{\rm err} = 0$, and $\lim_{n\to\infty} I\left(M; \mathbf{X}_{\mathcal{Z}_{\rm E}}\right)/n = 0$ for all $\mathcal{Z}_{\rm E} \subseteq \mathcal{E}$ such that $|\mathcal{Z}_{\rm E}| \le z_{\rm EO} + z_{\rm EJ}$. The* secrecy capacity *is defined as the supremum of all securely achievable rates.*

Remark 2. The secrecy criterion adopted here is commonly known as *weak secrecy*. In the literature, people also use other secrecy criterions such as *perfect secrecy* (if $I\left(M; \mathbf{X}_{\mathcal{Z}_{\rm E}}\right) = 0$ is satisfied) and *strong secrecy* (if $\lim_{n\to\infty} I\left(M; \mathbf{X}_{\mathcal{Z}_{\rm E}}\right) = 0$ is satisfied). While this work focuses on weak secrecy, we remark that once weak secrecy is achieved, strong secrecy can also be achieved via the *information reconciliation* and *privacy amplification* techniques developed in [27].

IV. Main Results

In this section, we present the capacity and secrecy capacity under both additive jamming and overwrite jamming. The adversary can be classified into either a weak adversary or a strong adversary, depending on the power vector $\mathbf{z} = (z_{\rm EJ}, z_{\rm EO}, z_{\rm JO})$. For additive jamming, the weak and strong adversary regimes are respectively given as

$$\mathcal{Z}_{\rm w}^{\rm add} = \{\mathbf{z} : z_{\rm EO} + z_{\rm JO} + 2z_{\rm EJ} < L\}, \tag{1}$$

[3] Here, we refer to the length of transmitted bits n on each link as the blocklength (which is assumed to grow without bound), while we assume the number of links L to be a constant. When the blocklength is large, one can view the n bits transmitted on each link as symbols over a large finite field — this is critical in this work since some of our schemes (e.g., pairwise-hashing) are designed to operate in the large alphabet regime.

$$\mathcal{Z}_{\rm s}^{\rm add} = \{\mathbf{z} : z_{\rm EO} + z_{\rm JO} + 2z_{\rm EJ} \geq L\}, \tag{2}$$

where $\mathcal{Z}_{\rm s}^{\rm add}$ is the complement of $\mathcal{Z}_{\rm w}^{\rm add}$. The two regimes are illustrated in Fig. 2.

Theorem 1 (Additive jamming)**.** *For any $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}$, the capacity $C^{\rm add}(\mathbf{z}) = L-(z_{\rm EJ}+z_{\rm JO}) = L-z_J$ and the secrecy capacity $C_s^{\rm add}(\mathbf{z}) = L-(z_{\rm JO}+z_{\rm EO}+2z_{\rm EJ}) = L-z_{\rm E}-z_J$. For any $\mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm add}$, the capacity $C^{\rm add}(\mathbf{z}) = [L-(2z_{\rm EJ}+z_{\rm JO})]^+$ and the secrecy capacity $C_s^{\rm add}(\mathbf{z}) = 0$.*

For overwrite jamming, the weak and strong adversary regimes are respectively given by

$$\mathcal{Z}_{\rm w}^{\rm ow} = \{\mathbf{z} : z_{\rm EO} + 2z_{\rm JO} + 2z_{\rm EJ} < L\}, \tag{3}$$

$$\mathcal{Z}_{\rm s}^{\rm ow} = \{\mathbf{z} : z_{\rm EO} + 2z_{\rm JO} + 2z_{\rm EJ} \geq L\}. \tag{4}$$

Theorem 2 (Overwrite jamming)**.** *For any $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm ow}$, the capacity $C^{\rm ow}(\mathbf{z}) = L-(z_{\rm EJ}+z_{\rm JO}) = L-z_J$ and the secrecy capacity $C_s^{\rm ow}(\mathbf{z}) = L-(z_{\rm JO}+z_{\rm EO}+2z_{\rm EJ}) = L-z_{\rm E}-z_J$. For any $\mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm ow}$, the capacity $C^{\rm ow}(\mathbf{z}) = [L-(2z_{\rm EJ}+2z_{\rm JO})]^+ = [L-2z_J]^+$ and the secrecy capacity $C_s^{\rm ow}(\mathbf{z}) = 0$.*

Remark 3. (i) First, observe that if James can jam z_J links, one cannot hope to get a rate higher than $L-z_J$. In fact, this rate is indeed achievable in the the weak adversary regime (for both additive and overwrite jamming). To achieve this rate, Bob needs to first detect the links being jammed (i.e., $\mathcal{Z}_{\rm J} = \mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$) and treat these links as erasures, and then recover the message from the uncorrupted links (i.e., $\mathcal{E} \setminus \mathcal{Z}_{\rm J}$). Our achievability scheme relies on a pairwise-hashing scheme together with an erasure code. The pairwise-hashing scheme is used to detect the corrupted links, while the erasure code is used to decode the message from the uncorrupted links. See Section V-A for details.

(ii) Second, in the strong adversary regime, the pairwise-hashing scheme is no longer helpful to detect all the links in $\mathcal{Z}_{\rm J}$. Under additive jamming, links in $\mathcal{Z}_{\rm EJ}$ cannot be detected by Bob (but links in $\mathcal{Z}_{\rm JO}$ can still be detected); under overwrite jamming, neither $\mathcal{Z}_{\rm JO}$ nor $\mathcal{Z}_{\rm EJ}$ can be detected. Thus, we use an error-correcting code (RS code) with sufficient redundancy to correct the errors in $\mathcal{Z}_{\rm J}$ that cannot be detected. See Section V-C for details.

(iii) Regarding the secrecy capacity under either additive or overwrite jamming: in the weak adversary regime, the achievability scheme is similar to that for Theorems 1 and 2 except that Alice needs to mix her message with $z_{\rm E}$ private keys. The converse follows from standard information-theoretic inequalities and the fact that any subset of links of size $z_{\rm E}$ cannot carry any meaningful information (due to the secrecy requirement).

(iv) In the weak adversary regime, the computational complexity of our scheme (for either type of jamming) is $\mathcal{O}(L^2n^2)$. In the strong adversary regime, the computational complexity of our scheme (for either type of jamming) is $\mathcal{O}(nL^2\log^2(nL))$.

Remark 4. Below, we discuss the connections between our work and several prior works on the secure network coding problem, and also provide a comparison of the results obtained in these works. The work [12] characterized the capacity and secrecy capacity for the secure network coding problem over a general network (where the links may intersect with each other) with additive adversaries. Specializing the general network in [12] to our multipath network, we note that [12, Theorems 2 and 3] are *identical* to our Theorem 1 when $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}$, but [12, Theorems 2 and 3] do not cover the regime $\mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm add}$. In the current paper, our Theorem 1 not only gives the result for the parameter regime $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}$, but also provides the characterizations of capacity and secrecy capacity for the other regime $\mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm add}$. The work [8] also considered secure network coding over a general network with additive adversaries; however, it is assumed that the eavesdropped set $\mathcal{Z}_{\rm E}$ and the jammed set $\mathcal{Z}_{\rm J}$ are *disjoint*. Specializing their general network model to our multipath network, [8] shows that the secrecy capacity is $L-z_{\rm E}-z_J$ when $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}$ (which is also identical to our Theorem 1), but they do not consider the parameter regime $\mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm add}$.

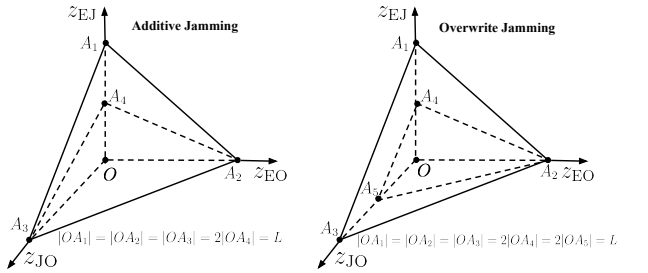

Fig. 2: For additive (resp. overwrite) jamming, the tetrahedron $A_4OA_2A_3$ (resp. $A_4OA_2A_5$) represents the weak adversary regime, while the tetrahedron $A_1A_2A_3A_4$ (resp. $A_1A_3A_5A_4A_2$) represents the strong adversary regime.

The prior work [17] studied the secure network coding problem with active adversaries, where both reliability and secrecy are required simultaneously. They proposed a coding scheme based on the nested coset coding scheme with maximum-rank-distance (MRD) codes, and analyzed the maximum achievable rate under the zero-error criterion. The work [18] proposed a secure network coding scheme that follows a similar principle as in [17], and further provided an explicit construction of the codes. We point out that the code constructions in [17] and [18] are different from ours; and the problem parametrization for eavesdropping and jamming is in terms of $(z_{\rm E}, z_J)$, without considering the intersection between the eavesdropped set and jammed. Also, when specializing their general network model to our multipath network, we note that the rate achieved by their schemes is $L-2z_J-z_{\rm E}$, which is in general smaller than the rate achieved by our scheme.[4]

Generalization to unequal link-capacity networks

The aforementioned capacity characterizations can also be extended to more general networks wherein different links are allowed to have different capacities. We assume each link E_i has capacity W_i (for $i \in [1:L]$), and the total capacity

[4]We point out a subtle point in the comparison: the work [17] and [18] considered the more stringent zero-error criterion, while our work focuses on the vanishing-error criterion.

(without adversary) of the network is $\widehat{L} \triangleq \sum_{i=1}^{L} W_i$ bits per use. In this model, James can jam links with highest sum-capacity to incur maximum damage. To take this into account, we define the sum-capacity of any set of links $\mathcal{S}$ as $W_{\mathcal{S}}$. For any integer $t \leq L$, we define the highest sum-capacity of t links as $W_t \triangleq \max_{\mathcal{S}:|\mathcal{S}|=t} W_{\mathcal{S}}$. Theorem 3 provides capacity characterizations for this general setting.

Theorem 3 (Unequal link-capacity network)**.** *The capacities $C^{\rm add}(\mathbf{z})$ and $C^{\rm ow}(\mathbf{z})$, for additive and overwrite jamming respectively, are given by*

$$C^{\rm add}(\mathbf{z}) = \begin{cases} \widehat{L} - W_{z_{\rm EJ}+z_{\rm JO}}, & \text{if } \mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}; \\ [\widehat{L} - W_{2z_{\rm EJ}+z_{\rm JO}}]^+, & \text{if } \mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm add}, \end{cases}; \quad (5)$$

$$C^{\rm ow}(\mathbf{z}) = \begin{cases} \widehat{L} - W_{z_{\rm EJ}+z_{\rm JO}}, & \text{if } \mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm ow}; \\ [\widehat{L} - W_{2z_{\rm EJ}+2z_{\rm JO}}]^+, & \text{if } \mathbf{z} \in \mathcal{Z}_{\rm s}^{\rm ow}. \end{cases} \quad (6)$$

The main idea behind Theorem 3 is similar to those for Theorems 1 and 2; that is, to detect as many corrupted links as possible[5]. The only difference is that James is able to corrupt the links with largest sum-capacities. Thus, for brevity we only provide detailed proofs of Theorems 1 and 2, while Theorem 3 can be proved in a completely analogous fashion.

V. Proofs for Theorems 1 and 2

A. Achievability for the weak adversary regime

In this subsection, we describe a unified achievability scheme for both (i) reliable communication and (ii) reliable and secure communication. The difference is that in case (ii), we reduce the message rate and instead add extra private keys to ensure secrecy.

1) Additive jamming: Recall that in the weak adversary regime $\mathbf{z} \in \mathcal{Z}_{\rm w}^{\rm add}$, the capacity $C^{\rm add} = L - z_J$ and the secrecy capacity $C_s^{\rm add} = L - z_J - z_{\rm E}$. Note that $C_s^{\rm add} + z_{\rm E} = C^{\rm add}$. Let d be an integer satisfying $d^2 + 2Ld = n/(\log(nL))$. When secrecy is not required, we set the length of the message to be $C^{\rm add} d^2 \log(nL)$ bits, thus $\lim_{n\to\infty} \log|\mathcal{M}|/n = C^{\rm add}$. When secrecy is required, we set the length of the message to be $C_s^{\rm add} d^2 \log(nL)$ bits, thus $\lim_{n\to\infty} \log|\mathcal{M}|/n = C_s^{\rm add}$.

(a) Encoder: From now on, we view the message bits in terms of symbols over finite fields either $\mathbb{F}_q$ or $\mathbb{F}_Q$, where $q \triangleq 2^{\log(nL)}$ and $Q \triangleq q^{d^2}$. Specifically, encoding is operated over $\mathbb{F}_Q$ and the pairwise-hashing scheme is operated over $\mathbb{F}_q$.

- When secrecy is not required, one can view the message M either as $C^{\rm add} d^2$ symbols over $\mathbb{F}_q$, or as $C^{\rm add}$ symbols $[\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{C^{\rm add}}]$ over $\mathbb{F}_Q$.
- When secrecy is required, one can view the message M either as $C_s^{\rm add} d^2$ symbols over $\mathbb{F}_q$, or as $C_s^{\rm add}$ symbols $[\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{C_s^{\rm add}}]$ over $\mathbb{F}_Q$. Alice also generates $z_{\rm E}$ symbols $[\mathbf{k}_1, \ldots, \mathbf{k}_{z_{\rm E}}]$ of uniformly distributed private key K (over $\mathbb{F}_Q$). We refer to the concatenation of M and K as the *super-message* $\widetilde{M}$, which has the form $[\mathbf{m}_1, \ldots, \mathbf{m}_{C_s^{\rm add}}, \mathbf{k}_1, \ldots, \mathbf{k}_{z_{\rm E}}]$.

[5]As discussed in Remark 3, all the links in $\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$ can be detected in the weak adversary regimes, only the links in $\mathcal{Z}_{\rm JO}$ can be detected in the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm add}$ under additive jamming, while none of the links in $\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$ can be detected in the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm ow}$ under overwrite jamming.

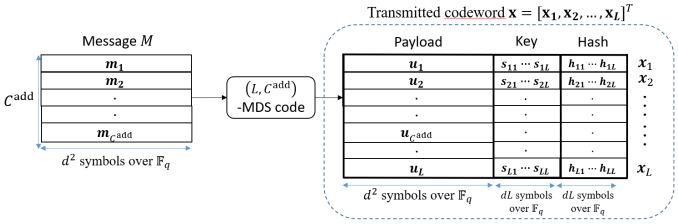

Fig. 3: Encoder (weak adversary regime, additive jamming, without secrecy requirements): Alice first uses an $(L, C^{\rm add})$-MDS code to encode the message to $[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_L]$ over $\mathbb{F}_Q$ (which are referred to as payloads), and then appends keys and hashes (generated/calculated based on the pairwise-hashing scheme) to the payloads.

In both cases, Alice uses an $L \times C^{\rm add}$ full-rank Cauchy generator matrix G (over $\mathbb{F}_Q$) to encode either the message $[\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{C^{\rm add}}]$ or the super-message $[\mathbf{m}_1, \ldots, \mathbf{m}_{C_s^{\rm add}}, \mathbf{k}_1, \ldots, \mathbf{k}_{z_{\rm E}}]$. The output is denoted by $[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_L]$. The encoder for the scenario when secrecy is not required is illustrated in Fig. 3. Since G is a full-rank Cauchy matrix, it has the property that any square sub-matrix of G is non-singular. This implies that the code (denoted by $\mathcal{C}_G$) associated with the generator matrix G is a MDS code (i.e., the distance of $\mathcal{C}_G$ is $L - C^{\rm add} + 1$), thus it is capable to tolerate $L - C^{\rm add} = z_J$ erasures.

Each symbol $\mathbf{u}_i \in \mathbb{F}_Q$ can also be viewed as an $d \times d$ matrix $\underline{\mathbf{U}}_i$ over $\mathbb{F}_q$ (i.e., $\underline{\mathbf{U}}_i \in \mathbb{F}_q^{d\times d}$). We refer to $\underline{\mathbf{U}}_i$ as the *payload* on link E_i. Alice then adopts the pairwise-hashing scheme. On each link E_i, Alice generates L uniformly distributed keys $[\mathbf{s}_{i1}, \mathbf{s}_{i2}, \ldots, \mathbf{s}_{iL}]$ over $\mathbb{F}_q^d$. For each $j \in [1:L]$, she calculates a hash $\mathbf{h}_{ij}$ using the *matrix-hashing function* defined below.

Definition 3 (Matrix-hashing function)**.** *Given $\underline{\mathbf{U}} \in \mathbb{F}_q^{d\times d}$ and $\mathbf{s} \in \mathbb{F}_q^d$, the matrix-hashing function $f : \mathbb{F}_q^{d\times d} \times \mathbb{F}_q^d \to \mathbb{F}_q^d$ is defined as $f(\underline{\mathbf{U}}, \mathbf{s}) \triangleq \underline{\mathbf{U}}\mathbf{s}$.*

Thus, the hash $\mathbf{h}_{ij}$ is equal to $f(\underline{\mathbf{U}}_j, \mathbf{s}_{ij})$, and the transmissions on link E_i take the form

$$\mathbf{x}_i = [\underline{\mathbf{U}}_i, \mathbf{s}_{i1}, \ldots, \mathbf{s}_{iL}, \mathbf{h}_{i1}, \ldots, \mathbf{h}_{iL}].$$

(b) Decoder: The received vector on link E_i is denoted by $\mathbf{y}_i = [\underline{\mathbf{U}}'_i, \mathbf{s}'_{i1}, \ldots, \mathbf{s}'_{iL}, \mathbf{h}'_{i1}, \ldots, \mathbf{h}'_{iL}]$. Note that $\mathbf{y}_i = \mathbf{x}_i$ if $E_i \notin \mathcal{Z}_{\rm J}$. Each link E_i is said to be *self-consistent* if $\mathbf{h}'_{ii} = f(\underline{\mathbf{U}}'_i, \mathbf{s}'_{ii})$. Each pair of links (E_i, E_j) is said to be *pairwise-consistent* if both $\mathbf{h}'_{ij} = f(\underline{\mathbf{U}}'_j, \mathbf{s}'_{ij})$ and $\mathbf{h}'_{ji} = f(\underline{\mathbf{U}}'_i, \mathbf{s}_{ji})$ are satisfied. Let $\mathcal{Z}_{\rm G} \triangleq \mathcal{E} \setminus (\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm JO})$ be the subset of "good" links that can neither be eavesdropped nor jammed, where $z_{\rm G} \triangleq |\mathcal{Z}_{\rm G}| = L - z_{\rm EJ} - z_{\rm EO} - z_{\rm JO}$. The decoding procedure is described below and illustrated in Fig. 4.

- Step 1: Check the self-consistency of each link, and output an estimate of the set $\mathcal{Z}_{\rm JO}$ as $\widehat{\mathcal{Z}}_{\rm JO} = \{E_i \in \mathcal{E} : E_i \text{ is not self-consistent}\}$.
- Step 2: Construct an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where the vertex set $\mathcal{V} = \mathcal{E} \setminus \widehat{\mathcal{Z}}_{\rm JO}$ contains all the self-consistent links. Two links E_i and E_j are connected (i.e., $(E_i, E_j) \in \mathcal{E}$) if and only if they are pairwise-consistent. Bob then looks for the largest *clique*[6] (i.e., the largest complete

[6]The idea of using maximal cliques for error detection has also been used in a recent work [28] in distributed learning.

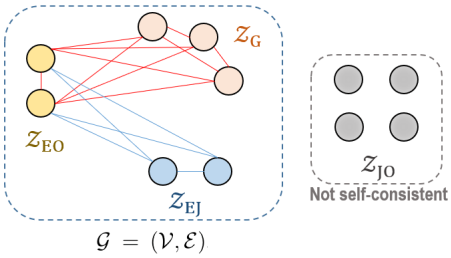

Fig. 4: Decoder (weak adversary regime, additive jamming): Bob first checks the self-consistency of each link, and constructs a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ on the set of self-consistent links. Lemma 2 shows that w.h.p., none of the links in $\mathcal{Z}_{\rm JO}$ are self-consistent (thus $\widehat{\mathcal{Z}}_{\rm wo} = \mathcal{Z}_{\rm JO}$ in Step 1). Lemma 3 shows that w.h.p., links in $\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm G}$ forms a clique (induced by Alice's pairwise-hashing scheme), and links in $\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm EJ}$ may form another clique (induced by James' jamming). Since $|\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm G}| > |\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm EJ}|$ in the weak adversary regime, the largest clique is the one formed by $\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm G}$, thus Bob's estimate of $\mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm G}$ in Step 2 is correct. In Step 3, Bob reconstruct the message/super-message based on the payloads on $\mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$.

sub-graph) $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ in $\mathcal{G}$. The vertex set $\mathcal{V}'$ is an estimate of the set of uncorrupted links $\mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$.

- Step 3: Treat the transmissions on $\mathcal{E} \setminus \mathcal{V}'$ as erasures, and reconstruct the message or the super-message based on payloads $\{\underline{\mathbf{U}}'_i\}_{i \in \mathcal{V}'}$ (where $|\mathcal{V}'| = z_{\rm G} + z_{\rm EO} = L - z_{\rm EJ} - z_{\rm JO}$ conditioned on the success of preceding steps[7]). Let $G_{\mathcal{V}'}$ be the (non-singular) square sub-matrix of G corresponding to the set $\mathcal{V}'$. The message/super-message can then be reconstructed by multiplying $G_{\mathcal{V}'}^{-1}$ with the vector $\{\underline{\mathbf{U}}'_i\}_{i \in \mathcal{V}'} \in \mathbb{F}_Q^{L - z_{\rm EJ} - z_{\rm JO}}$.

(c) Computational complexity: The encoder of the MDS code takes at most $LC^{\rm add}$ multiplications and $LC^{\rm add}$ additions over $\mathbb{F}_Q$, thus the computational complexity is at most $LC^{\rm add}((\log Q)^2 + \log Q) \le L^2(n^2+n)$. Calculating one hash (based on the matrix-hashing function) takes at most d^2 multiplications and d^2 additions over $\mathbb{F}_q$, thus the computational complexity of calculating L^2 hashes is bounded from above by $L^2(d^2(\log q)^2 + d^2 \log q) \le L^2 n[\log^2(nL) + \log(nL)]$. Therefore, the overall encoding complexity is $\mathcal{O}(L^2 n^2)$.

To check self-consistency and pairwise-consistency, Bob needs to calculate L^2 hashes, and the computational complexity is at most $L^2 n[\log^2(nL) + \log(nL)]$. Finding the largest clique is in general NP-hard [29]; however, in our work, we are given a very strong promise — only nodes in the largest clique have "high" degree (at least $z_{\rm EO} + z_{\rm G} - 1$), whereas all other nodes have "low" degree with high probability over our hashing scheme. This promise makes it computationally tractable to find the largest clique. The decoder of the MDS code takes at most $(C^{\rm add})^2$ multiplications and $(C^{\rm add})^2$ additions over $\mathbb{F}_Q$, thus the complexity is at most $L^2(n^2+n)$ (by noting that $C^{\rm add} \le L$). Therefore, the overall decoding complexity is also $\mathcal{O}(L^2 n^2)$.

(d) Proof of reliability: Before proceeding with the detailed proof, we first introduce a lemma that describes a key property of the matrix-hashing function.

[7]If $|\mathcal{V}'| > L - z_{\rm EJ} - z_{\rm JO}$, one can remove any $|\mathcal{V}'| - (L - z_{\rm EJ} - z_{\rm JO})$ links from $\mathcal{V}'$ to ensure that the cardinality of $\mathcal{V}'$ is still $L - z_{\rm EJ} - z_{\rm JO}$.

Lemma 1. *Suppose* $\mathbf{S}$ *is uniformly distributed over* $\mathbb{F}_q^d$. *For any fixed* $\underline{\mathbf{U}} \in \mathbb{F}_q^{d \times d} \setminus \{\mathbf{0}\}$ *and hash* $\mathbf{h} \in \mathbb{F}_q^d$, *we have* $\mathbb{P}_{\mathbf{S}}(\mathbf{h} = f(\underline{\mathbf{U}}, \mathbf{S})) \le 1/q$.

Proof of Lemma 1. Since $\underline{\mathbf{U}} \neq 0$, there must exist an $i \in [1:d]$ such that $\underline{\mathbf{U}}_i$, the i-th row of $\underline{\mathbf{U}}$, is a non-zero vector. Hence, $\mathbb{P}_{\mathbf{S}}(\mathbf{h} = f(\underline{\mathbf{U}}, \mathbf{S})) \le \mathbb{P}_{\mathbf{S}}(h_i = \underline{\mathbf{U}}_i \mathbf{S}) \le 1/q$, where the last inequality follows from the Schwartz-Zippel Lemma. □

The proof of reliability relies on Lemmas 2 and 3 presented below. Specifically, Lemma 2 states that Bob is able to correctly estimate $\mathcal{Z}_{\rm JO}$ (i.e., $\widehat{\mathcal{Z}}_{\rm JO} = \mathcal{Z}_{\rm JO}$) in Step 1 with high probability, and Lemma 3 states that Bob is able to correctly identify the set of uncorrupted links (i.e., $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$) in Step 2 with high probability. Conditioned on the success of Steps 1 and 2, Bob then treats the links $\mathcal{E} \setminus \mathcal{V}' = \mathcal{Z}_{\rm JO} \cup \mathcal{Z}_{\rm EJ}$ (where $|\mathcal{Z}_{\rm JO} \cup \mathcal{Z}_{\rm EJ}| \le L - C^{\rm add}$) as erasures, and decodes from the payloads $\{\underline{\mathbf{U}}_i\}_{i \in \mathcal{V}'}$ on the uncorrupted links $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$. Step 3 will succeed since the code $\mathcal{C}_G$ is capable to tolerate $L - C^{\rm add}$ erasures.

In Lemmas 2 and 3 below, we assume when James is able to jam E_i (i.e., $E_i \in \mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$), he always chooses to modify the payload so that $\underline{\mathbf{U}}'_i \neq \underline{\mathbf{U}}_i$. This assumption is merely for ease of presentation and does not affect the correctness of the proof. This is because if James chooses to keep $\underline{\mathbf{U}}'_i = \underline{\mathbf{U}}_i$ on link $E_i \in \mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$, Bob's decoder will still succeed even if E_i cannot be identified as an erasure.

Lemma 2. *For each link* $E_i \in \mathcal{Z}_{\rm JO}$, *it is not self-consistent with probability at least* $1 - (1/nL)$. *Furthermore, the probability that Bob's estimate* $\widehat{\mathcal{Z}}_{\rm JO} = \mathcal{Z}_{\rm JO}$ *is at least* $1 - (z_{\rm JO}/nL)$.

Proof. Consider a link $E_i \in \mathcal{Z}_{\rm JO}$. Since the transmissions on E_i cannot be eavesdropped, James does not have any information about the key $\mathbf{s}_{ii}$ on E_i. That is, from James' perspective, the key is uniformly distributed over $\mathbb{F}_q^d$, and is thus denoted by the uppercase boldface letter $\mathbf{S}_{ii}$. Let $\mathbf{e}_{ii}^s$ be the additive noise (over $\mathbb{F}_q$) on the locations of $\mathbf{S}_{ii}$. Thus, conditioned on $\mathbf{h}_{ii} = f(\underline{\mathbf{U}}_i, \mathbf{S}_{ii})$, the probability that E_i is self-consistent (regardless of the values of $\mathbf{h}'_{ii}$ and $\underline{\mathbf{U}}'_i$) is

$$\begin{aligned}&\mathbb{P}_{\mathbf{S}_{ii}}\left(\mathbf{h}'_{ii} = f(\underline{\mathbf{U}}'_i, \mathbf{S}_{ii} + \mathbf{e}_{ii}^s) | \mathbf{h}_{ii} = f(\underline{\mathbf{U}}_i, \mathbf{S}_{ii})\right)\\ &= \mathbb{P}_{\mathbf{S}_{ii}}\left(\mathbf{h}'_{ii} - \mathbf{h}_{ii} - f(\underline{\mathbf{U}}'_i, \mathbf{e}_{ii}^s) = f(\underline{\mathbf{U}}'_i - \underline{\mathbf{U}}_i, \mathbf{S}_{ii})\right) \le \frac{1}{q},\end{aligned}$$

which is due to the linearity of the matrix-hashing function, as well as Lemma 1 (by noting that $\underline{\mathbf{U}}'_i - \underline{\mathbf{U}}_i \neq \mathbf{0}$). This probability converges to zero since we set $q = 2^{\log(nL)}$.

Taking a union bound over all the links in $\mathcal{Z}_{\rm JO}$, we have $\mathbb{P}\big(\widehat{\mathcal{Z}}_{\rm JO} = \mathcal{Z}_{\rm JO}\big) \ge 1 - \frac{z_{\rm JO}}{q} = 1 - \frac{z_{\rm JO}}{nL}$, which means Bob is able to correctly detect the set $\mathcal{Z}_{\rm JO}$ with high probability. □

Lemma 3. *With probability at least* $1 - (z_{\rm EJ} + z_{\rm G})/q$, *Bob can estimate of the set of uncorrupted links successfully, i.e.,* $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$.

Proof. First note that any two links E_i and E_j in the set $\mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$ are pairwise-consistent, since James cannot jam on these links. Thus, all the links in $\mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$ form an *correct clique* $\mathcal{G}'_{\checkmark}$. In addition, the following argument shows that the correct clique $\mathcal{G}'_{\checkmark}$ cannot be further enlarged with high probability. Consider a link $E_i \in \mathcal{Z}_{\rm G}$ which belongs to $\mathcal{G}'_{\checkmark}$, and note that

each of the keys $\{\mathbf{S}_{ij}\}_{j\in[1:L]}$ on E_i is uniformly distributed over $\mathbb{F}_q^d$ from James' perspective. For any other link $E_j \in \mathcal{Z}_{\rm EJ}$, conditioned on the fact that $\mathbf{h}_{ij} = f(\underline{\mathbf{U}}_j, \mathbf{S}_{ij})$, we have

$$\begin{aligned}&\mathbb{P}\left((E_i, E_j) \text{ are pairwise-consistent}\right)\\ &\le \mathbb{P}_{\mathbf{S}_{ij}}\left(\mathbf{h}_{ij} = f(\underline{\mathbf{U}}'_j, \mathbf{S}_{ij}) | \mathbf{h}_{ij} = f(\underline{\mathbf{U}}_j, \mathbf{S}_{ij})\right)\\ &= \mathbb{P}_{\mathbf{S}_{ij}}\left(f(\underline{\mathbf{U}}'_j - \underline{\mathbf{U}}_j, \mathbf{S}_{ij}) = \mathbf{0}\right) \le \frac{1}{q} = \frac{1}{nL}, \end{aligned} \tag{7}$$

where the last inequality follows from Lemma 1 and the fact that $\underline{\mathbf{U}}'_j - \underline{\mathbf{U}}_j \neq \mathbf{0}$. A union bound over all the links $E_j \in \mathcal{Z}_{\rm EJ}$ yields that, with probability at least $1 - (z_{\rm EJ}/nL)$, E_i is not pairwise-consistent with *any* links in $\mathcal{Z}_{\rm EJ}$. This implies the correct clique $\mathcal{G}'_{\checkmark}$ would not contain any other links in $\mathcal{Z}_{\rm EJ}$.

On the other hand, if James wishes, he is able to carefully jam $\mathcal{Z}_{\rm EJ}$ (based on his observations on $\mathcal{Z}_{\rm EJ}$ and $\mathcal{Z}_{\rm EO}$) in such a way that: (i) Any two links $(E_i, E_j) \in (\mathcal{Z}_{\rm EJ} \times \mathcal{Z}_{\rm EJ})$ are pairwise-consistent, since he has full control of the transmissions on E_i and E_j; and (ii) Any two links $(E_i, E_j) \in (\mathcal{Z}_{\rm EO} \times \mathcal{Z}_{\rm EJ})$ are pairwise-consistent[8]. Therefore, James is able to construct a *fake clique* $\mathcal{G}'_{\times}$ that contains all the links in $\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm EO}$. Also, $\mathcal{G}'_{\times}$ cannot be further enlarged with high probability. Consider a link $E_j \in \mathcal{Z}_{\rm EJ}$ which belongs to $\mathcal{G}'_{\times}$. For any other link $E_i \in \mathcal{Z}_{\rm G}$, the probability that (E_i, E_j) is pairwise-consistent is at most $1/(nL)$ by (7). Taking a union bound over all $E_i \in \mathcal{Z}_{\rm G}$ yields that with probability at least $1 - (z_{\rm G}/nL)$, E_j is not pairwise-consistent with *any* links in $\mathcal{Z}_{\rm G}$. This implies the fake clique $\mathcal{G}'_{\times}$ would not contain any other links in $\mathcal{Z}_{\rm G}$.

Finally, note that the size of the correct clique $\mathcal{G}'_{\checkmark}$ is larger than the size of the fake clique $\mathcal{G}'_{\times}$, since $z_{\rm G} + z_{\rm EO} > z_{\rm EJ} + z_{\rm EO}$ in the weak adversary regime $\mathcal{Z}_{\rm w}^{\rm add}$. Therefore, the largest clique $\mathcal{G}' = \mathcal{G}'_{\checkmark}$, and the estimate of the set of uncorrupted links $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$. □

(e) Proof of secrecy: For secrecy, we show that James cannot infer any information from the links he eavesdrops. Let $\mathbf{X}_{\mathcal{Z}_{\rm E}}$ and $\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}}$ respectively be the transmitted vector and payloads on the links that are eavesdropped by James. Consider the following set of inequalities.

$$\begin{aligned} I(M; \mathbf{X}_{\mathcal{Z}_{\rm E}}) &= H(\mathbf{X}_{\mathcal{Z}_{\rm E}}) - H(\mathbf{X}_{\mathcal{Z}_{\rm E}}|M) && (8)\\ &\le nz_{\rm E} - I(\mathbf{X}_{\mathcal{Z}_{\rm E}}; K|M) && (9)\\ &= nz_{\rm E} - H(K) + H(K|\mathbf{X}_{\mathcal{Z}_{\rm E}}, M) && (10)\\ &\le H(K|\mathbf{X}_{\mathcal{Z}_{\rm E}}, M) + z_{\rm E}\cdot dL\log(nL) && (11)\\ &\le H(K|\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}}, M) + z_{\rm E}\cdot dL\log(nL) && (12)\end{aligned}$$

where (10) holds since K is independent of the message. Inequality (11) follows from the fact that the entropy of the uniformly distributed keys is at least $z_{\rm E}(n - dL\log(nL))$, where the term $z_{\rm E}\cdot dL\log(nL)$ corresponds to the loss of entropy due to the hashes. Finally, (12) is obtained by noting that $\mathbf{X}_{\mathcal{Z}_{\rm E}}$ comprises $\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}}$. Let $G_{\mathcal{Z}_{\rm E}}$ denote the rows of the Cauchy generator matrix G corresponding to the symbols $\mathbf{X}_{\mathcal{Z}_{\rm E}}$, thus $\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}} = G_{\mathcal{Z}_{\rm E}}\cdot[\mathbf{m}_1, \ldots, \mathbf{m}_{C_s^{\rm add}}, \mathbf{k}_1, \ldots, \mathbf{k}_{z_{\rm E}}]^T$. We now prove $H(K|\mathbf{U}_{\mathcal{Z}_{\rm E}}, M) = 0$ by showing that the following system of equations is solvable:

$$\begin{aligned}&[\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}}, \mathbf{m}_1, \ldots, \mathbf{m}_{L-z_J-z_{\rm E}}]^T \\ &= G'\cdot[\mathbf{m}_1, \ldots, \mathbf{m}_{C_s^{\rm add}}, \mathbf{k}_1, \ldots, \mathbf{k}_{z_{\rm E}}]^T, \text{ where } G' = \begin{bmatrix} G_{\mathcal{Z}_{\rm E}} \\ I \mid O \end{bmatrix},\end{aligned} \tag{13}$$

I denotes an identity matrix of size $(L - z_J - z_{\rm E}) \times (L - z_J - z_{\rm E})$, and O denotes a zero matrix of size $(L - z_J - z_{\rm E}) \times z_{\rm E}$. Using the fact that any square sub-matrix of a Cauchy matrix is non-singular, it can be shown that the matrix G' is non-singular. Thus, the linear system (13) can be inverted, and we have $H(K|\underline{\mathbf{U}}_{\mathcal{Z}_{\rm E}}, M) = 0$. Therefore, our scheme achieves weak secrecy since $\lim_{n\to\infty} z_{\rm E}\cdot dL\log(nL)/n = 0$.

2) Overwrite jamming: The achievability scheme for overwrite jamming is similar to that for additive jamming, hence we only highlight the differences between the two settings. First recall that the weak adversary regime $\mathcal{Z}_{\rm w}^{\rm ow} = \{\mathbf{z} : z_{\rm EO} + 2z_{\rm JO} + 2z_{\rm EJ} < L\}$ under overwrite jamming is smaller than that for additive jamming. This makes sense because an overwrite jammer is more powerful than an additive jammer. Under $\mathcal{Z}_{\rm w}^{\rm ow}$, the capacity $C^{\rm ow} = L - z_{\rm EJ} - z_{\rm JO} = L - z_J$ is the same as $C^{\rm add}$, and the secrecy capacity $C_s^{\rm ow} = L - z_{\rm EJ} - z_{\rm EO} - 2z_{\rm JO} = L - z_J - z_{\rm E}$ is the same as $C_s^{\rm add}$ as well.

The encoder and decoder are exactly the same as those for additive jamming. However, the analysis of reliability is different since an overwrite jammer is able to *completely control* the outputs on $E_i \in \mathcal{Z}_{\rm JO}$, while an additive jammer does not know the outputs on $\mathcal{Z}_{\rm JO}$ after jamming (since the inputs are unknown). We now sketch the proof of reliability.

- (Step 1) Under overwrite jamming, James is able to ensure all the links in $\mathcal{Z}_{\rm JO}$ to be self-consistent by carefully designing his jamming strategy, thus Bob's decoder outputs $\widehat{\mathcal{Z}}_{\rm JO} = \emptyset$ in Step 1. As a consequence, Lemma 2, which shows that Bob's estimate $\widehat{\mathcal{Z}}_{\rm JO} = \mathcal{Z}_{\rm JO}$ with high probability (in Step 1), is no longer valid.
- (Step 2) Since $\mathcal{Z}_{\rm JO}$ cannot be detected in Step 1 (i.e., $\widehat{\mathcal{Z}}_{\rm JO} = \emptyset$), the vertex set of the constructed graph is $\mathcal{E} \setminus \widehat{\mathcal{Z}}_{\rm JO} = \mathcal{E}$. We now argue that by using the strategy of finding the largest clique, Bob can still estimate of the set of uncorrupted links correctly (i.e., $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$) with high probability. Recall that under additive jamming, James is able to ensure any two links (E_i, E_j) in $\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm EO}$ to be pairwise-consistent. Under overwrite jamming, one can show that James is able to ensure any two links $(E_i, E_j) \in \mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm EO} \cup \mathcal{Z}_{\rm JO}$ to be pairwise-consistent by carefully controlling the outputs on $\mathcal{Z}_{\rm JO}$. As a consequence, he can construct a fake clique $\mathcal{G}'_{\times}$ of size $z_{\rm EJ} + z_{\rm EO} + z_{\rm JO}$, while the correct clique $\mathcal{G}'_{\checkmark}$ is still of size $z_{\rm G} + z_{\rm EO} = L - z_{\rm EJ} - z_{\rm JO}$. By noting that $z_{\rm EO} + 2z_{\rm JO} + 2z_{\rm EJ} < L$ in the weak adversary regime $\mathcal{Z}_{\rm w}^{\rm ow}$, the largest clique $\mathcal{G}'$ is again $\mathcal{G}'_{\checkmark}$, thus $\mathcal{V}' = \mathcal{Z}_{\rm G} \cup \mathcal{Z}_{\rm EO}$.
- (Step 3) Treating the links $\mathcal{E}\setminus\mathcal{V}' = \mathcal{Z}_{\rm JO} \cup \mathcal{Z}_{\rm EJ}$ as erasures and decoding based on $\{\underline{\mathbf{U}}_i\}_{i\in\mathcal{V}'}$. Step 3 will succeed since the MDS code is capable to tolerate $z_{\rm EJ} + z_{\rm JO}$ erasures.

[8]This is because James' knowledge of $\underline{\mathbf{U}}_i, \mathbf{s}_{ij}, \mathbf{h}_{ij}$ on E_i makes it possible to ensure $\mathbf{h}_{ij} = f(\underline{\mathbf{U}}'_j, \mathbf{s}_{ij})$ and $\mathbf{h}'_{ji} = f(\underline{\mathbf{U}}_i, \mathbf{s}'_{ji})$ by carefully designing $\underline{\mathbf{U}}'_j, \mathbf{s}'_{ji}, \mathbf{h}'_{ji}$.

Finally, we note that the proofs of secrecy for additive jamming and overwrite jamming are exactly the same, hence we omit it here for brevity.

B. Converse for the weak adversary regime

The proof of converse described here is valid for both additive and overwrite jamming.

First, for reliable communication (without secrecy constraints), it is impossible to achieve a rate higher than $L-z_J$, since James can corrupt all the links in $\mathcal{Z}_{\rm JO}\cup\mathcal{Z}_{\rm EJ}$ by adding random noise that is independent of Alice's transmissions.

Second, for reliable and secure communication, we use standard information-theoretic inequalities to show that the securely achievable rate cannot be higher than $L-z_J-z_{\rm E}$. Suppose James uses the following simple strategy — adding random noise on the links in $\mathcal{Z}_{\rm J}$, and eavesdropping on all links in $\mathcal{Z}_{\rm E}$. For any code of length n that achieve an error probability ϵ_n (where $\epsilon_n\to 0$ as $n\to\infty$) and information-theoretic secrecy, we have

$$\begin{aligned}
\log|\mathcal{M}| &= H(M|\mathbf{Y})+I(M;\mathbf{Y})\\
&\le n\epsilon_n + I(M;\mathbf{Y}) \qquad (14)\\
&= n\epsilon_n + I(M;\mathbf{Y}_1^{z_J}) + I(M;\mathbf{Y}_{z_J+1}^{L}|\mathbf{Y}_1^{z_J})\\
&\le n\epsilon_n + I(M;\mathbf{X}_{z_J+1}^{L}) \qquad (15)\\
&\le n\epsilon_n + I(M;\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}}) + I(M;\mathbf{X}_{z_J+z_{\rm E}+1}^{L}|\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}})\\
&\le n\epsilon_n + n\epsilon_n' + H(\mathbf{X}_{z_J+z_{\rm E}+1}^{L}|\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}}) \qquad (16)\\
&\le n\epsilon_n + n\epsilon_n' + n(L-z_J-z_{\rm E}). \qquad (17)
\end{aligned}$$

Here, (14) follows from Fano's inequality. To obtain (15), we assume without loss of generality that James jams the first z_J links, and we further have $I(M;\mathbf{Y}_1^{z_J})=0$ since James adds uniform random noise independent of Alice's transmissions. Also, we have $I(M;\mathbf{Y}_{z_J+1}^{L}|\mathbf{Y}_1^{z_J}) = I(M;\mathbf{Y}_{z_J+1}^{L})$ due to independence of the random noise, and $I(M;\mathbf{Y}_{z_J+1}^{L}) = I(M;\mathbf{X}_{z_J+1}^{L})$ since $\mathbf{Y}_{z_J+1}^{L}=\mathbf{X}_{z_J+1}^{L}$ holds for the set of uncorrupted links. To get (16), we use the fact that for any subset $\mathcal{Z}_{\rm E}$ of links of size $z_{\rm E}$, the secrecy requirement imposes that $I(M;\mathbf{X}_{\mathcal{Z}_{\rm E}})\le n\epsilon_n'$ for some $\epsilon_n'\to 0$, thus we have $I(M;\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}})\le n\epsilon_n'$. In addition, we have $I(M;\mathbf{X}_{z_J+z_{\rm E}+1}^{L}|\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}})\le H(\mathbf{X}_{z_J+z_{\rm E}+1}^{L}|\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}})$. Lastly, (17) follows from the fact $H(\mathbf{X}_{z_J+z_{\rm E}+1}^{L}|\mathbf{X}_{z_J+1}^{z_J+z_{\rm E}})\le H(\mathbf{X}_{z_J+z_{\rm E}+1}^{L})\le n(L-z_J-z_{\rm E})$. Therefore, we have $\lim_{n\to\infty}\frac{\log|\mathcal{M}|}{n}\le L-z_J-z_{\rm E}$.

C. Achievability for the strong adversary regime

1) Additive jamming: Recall that in the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm add}$, the capacity is $C^{\rm add}=[L-(2z_{\rm EJ}+z_{\rm JO})]^+$ and the secrecy capacity is $C_s^{\rm add}=0$. Thus, we only need to show that Alice and Bob can reliably communicate at a rate $L-(2z_{\rm EJ}+z_{\rm JO})$ when $L-(2z_{\rm EJ}+z_{\rm JO})>0$.

The encoder is similar to that in Subsection V-A, except that (i) the message M here contains $(L-2z_{\rm EJ}-z_{\rm JO})(n-c_0(L,n))$ bits (or equivalently, $L-2z_{\rm EJ}-z_{\rm JO}$ symbols over $\mathbb{F}_Q$), and (ii) we use a different type of MDS code — RS codes. Alice first uses an $(L,L-2z_{\rm EJ}-z_{\rm JO})$-RS code to encode the message to $[\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_L]$ over $\mathbb{F}_Q$, and then adopts the pairwise-hashing scheme (by rearranging each $\mathbf{u}_i\in\mathbb{F}_Q$ as an $d\times d$ matrix $\underline{\mathbf{U}}_i$ over $\mathbb{F}_q$). The input and output on link E_i respectively take the form $\mathbf{x}_i=[\underline{\mathbf{U}}_i,\mathbf{s}_{i1},\ldots,\mathbf{s}_{iL},\mathbf{h}_{i1},\ldots,\mathbf{h}_{iL}]$ and $\mathbf{y}_i=[\underline{\mathbf{U}}_i',\mathbf{s}_{i1}',\ldots,\mathbf{s}_{iL}',\mathbf{h}_{i1}',\ldots,\mathbf{h}_{iL}']$. Bob's decoding rule is as follows: (i) Check the self-consistency of each link, and output an estimate of the set $\mathcal{Z}_{\rm JO}$ as $\widehat{\mathcal{Z}}_{\rm JO}=\{E_i\in\mathcal{E}: E_i \text{ is not self-consistent}\}$; (ii) Treat $\{\underline{\mathbf{U}}_i'\}_{i\in\widehat{\mathcal{Z}}_{\rm JO}}$ as erasures, and apply the RS-decoder to $[\underline{\mathbf{U}}_1',\underline{\mathbf{U}}_2',\ldots,\underline{\mathbf{U}}_L']$ to reconstruct the message M. As proved in Lemma 2, Bob is able to ensure $\widehat{\mathcal{Z}}_{\rm JO}=\mathcal{Z}_{\rm JO}$ with high probability. Conditioned on the success of the Step 1, the message can be reconstructed correctly. This is because the RS code (of distance $2z_{\rm EJ}+z_{\rm JO}+1$) is capable to tolerate a combination of $z_{\rm JO}$ erasures and $z_{\rm EJ}$ errors.

2) Overwrite jamming: In the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm ow}$, the capacity is $C^{\rm ow}=[L-2z_J]^+$ and the secrecy capacity is $C_s^{\rm ow}=0$. Alice and Bob simply use an $(L,L-2z_J)$-RS code to achieve reliable communication. Note that the RS code has minimum distance $2z_J+1$, and is capable to correct $2z_J$ errors. Therefore, the rate $L-2z_J$ is achievable since the number of jammed links is at most $z_{\rm EJ}+z_{\rm JO}$.

3) Computational complexity: A clever implementation of the RS encoder (by performing *fast Fourier transform* [30]) ensures the computational complexity to be $\mathcal{O}(nL\log(L))$, while the complexity of the best known RS decoder [31] is $\mathcal{O}(nL^2\log(L))$. Thus, the overall encoding and decoding complexities (for both additive and overwrite jamming) are dominated by the pairwise-hashing scheme (described in Subsection V-A), which are at most $\mathcal{O}(nL^2\log^2(nL))$.

D. Converse for the strong adversary regime

1) Additive jamming: We first show that without the secrecy constraints, the error probability $\mathbb{P}(M\neq\widehat{M})$ is bounded away from zero if the rate exceeds the capacity $C^{\rm add}=L-(2z_{\rm EJ}+z_{\rm JO})$. Suppose $\log|\mathcal{M}|=n(L-2z_{\rm EJ}-z_{\rm JO}+\epsilon)$ for any $\epsilon>0$, and Alice's encoder follows from the distribution $P_{\mathbf{X}|M}$. Let $P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}|M}$ be the marginal distribution of $P_{\mathbf{X}|M}$ on the set $\mathcal{Z}_{\rm EO}$, and

$$P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathcal{Z}_{\rm EO})\triangleq\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}|M}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}|m),\quad\text{and}$$

$$P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}\triangleq\frac{P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}|M}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}|m)}{|\mathcal{M}|P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}})}.$$

James uses the following *observe-and-attack* strategy:

1) Choose $\mathcal{Z}_{\rm EO}=\{E_1,\ldots,E_{L-2z_{\rm EJ}-z_{\rm JO}}\}$ to eavesdrop. This is possible since $z_{\rm EO}\ge L-2z_{\rm EJ}-z_{\rm JO}$ in the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm add}$.
2) Choose $\mathcal{Z}_{\rm JO}=\{E_{L-2z_{\rm EJ}-z_{\rm JO}+1},\ldots,E_{L-2z_{\rm EJ}}\}$ and add random noise $\mathbf{E}_{\mathcal{Z}_{\rm JO}}$ (independent of transmissions) on $\mathcal{Z}_{\rm JO}$.
3) For the remaining $2z_{\rm EJ}$ links, let $\mathcal{Z}_a\triangleq\{E_{L-2z_{\rm EJ}+1},\ldots,E_{L-z_{\rm EJ}}\}$ and $\mathcal{Z}_b\triangleq\{E_{L-z_{\rm EJ}+1},\ldots,E_L\}$. James chooses $\mathcal{Z}_{\rm EJ}$ to be either $\mathcal{Z}_a$ or $\mathcal{Z}_b$ with equal probability.
4) The attack strategy is to first generate a fake message $M'\sim P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}$ based on his observations $\mathbf{x}_{\mathcal{Z}_{\rm EO}}$. James then uses Alice's public encoder $P_{\mathbf{X}|M}$, which can be

decomposed into $P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}|M} \cdot P_{\mathbf{X}_{\mathcal{E}\setminus\mathcal{Z}_{\rm EO}}|\mathbf{X}_{\mathcal{Z}_{\rm EO}},M}$, to generate a fake codeword $\mathbf{X}'$ such that $\mathbf{X}'_{\mathcal{Z}_{\rm EO}} = \mathbf{x}_{\mathcal{Z}_{\rm EO}}$ and $\mathbf{X}'_{\mathcal{E}\setminus\mathcal{Z}_{\rm EO}} \sim P_{\mathbf{X}_{\mathcal{E}\setminus\mathcal{Z}_{\rm EO}}|\mathbf{X}_{\mathcal{Z}_{\rm EO}},M}$. He then replaces the original sub-codeword $\mathbf{X}_{\mathcal{Z}_{\rm EJ}}$ on the subset $\mathcal{Z}_{\rm EJ}$ with the new sub-codeword $\mathbf{X}'_{\mathcal{Z}_{\rm EJ}}$.

By noting that $n(L-2z_{\rm EJ}-z_{\rm JO}+\epsilon) = H(M) = H(M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}) + H(\mathbf{X}_{\mathcal{Z}_{\rm EO}}) \le H(M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}) + n(L-2z_{\rm EJ}-z_{\rm JO})$, we have $n\epsilon \le H(M|\mathbf{X}_{\mathcal{Z}_{\rm EO}})$, which states that the conditional entropy of M after observing $\mathbf{X}_{\mathcal{Z}_{\rm EO}}$ is bounded away from zero. Further, we partition $\mathbf{x}_{\mathcal{Z}_{\rm EO}}$ into two sets: $\mathcal{A}_1 \triangleq \{\mathbf{x}_{\mathcal{Z}_{\rm EO}} : H(M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \ge n\epsilon/2\}$ and $\mathcal{A}_2 = \{\mathbf{x}_{\mathcal{Z}_{\rm EO}} : H(M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) < n\epsilon/2\}$. Thus,

$$\begin{aligned}
n\epsilon &\le H(M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}) \\
&= \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) H(M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&\qquad + \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_2} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) H(M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&\le nL \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) + \frac{n\epsilon}{2} \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_2} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&= \frac{n\epsilon}{2} + \Big(nL - \frac{n\epsilon}{2}\Big) \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}),
\end{aligned}$$

and we obtain that $\sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \ge \frac{\epsilon}{2J}$. Let $\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}$ be the event corresponding to $\{M=m, M'=m', \mathbf{X}_{\mathcal{Z}_{\rm EO}} = \mathbf{x}_{\mathcal{Z}_{\rm EO}}\}$. The error probability $\mathbb{P}(M \ne \widehat{M})$ is

$$\begin{aligned}
&\frac{1}{|\mathcal{M}|} \sum_m \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}|M}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}|m) \\
&\qquad \cdot \sum_{m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m'|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \cdot \mathbb{P}(\widehat{M} \ne m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}) \\
&= \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \sum_m P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&\qquad \cdot \sum_{m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m'|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \cdot \mathbb{P}(\widehat{M} \ne m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}) \\
&\ge \sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \sum_{m\ne m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&\qquad \cdot P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m'|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \cdot \mathbb{P}(\widehat{M} \ne m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}). \quad (18)
\end{aligned}$$

Note that conditioned on $\mathbf{x}_{\mathcal{Z}_{\rm EO}}$, Alice chooses her message M according to $P_{M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}}$, and James chooses his fake message M' independently according to the distribution $P_{M|\mathbf{x}_{\mathcal{Z}_{\rm EO}}}$. Lemma 4 below shows that if $\mathbf{x}_{\mathcal{Z}_{\rm EO}} \in \mathcal{A}_1$, the probability that $M \ne M'$ is bounded away from zero.

Lemma 4. *For any $\mathbf{x}_{\mathcal{Z}_{\rm EO}} \in \mathcal{A}_1$, we have $\sum_{m\ne m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m'|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \ge \frac{\epsilon}{3L}$.*

The proof of Lemma 4 can be found in Appendix. Without loss of generality, suppose $\mathcal{M} = [1:|\mathcal{M}|]$. Thus, (18) can be rewritten as

$$\begin{aligned}
&\sum_{\mathbf{x}_{\mathcal{Z}_{\rm EO}}\in\mathcal{A}_1} P_{\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \sum_{m<m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}(m'|\mathbf{x}_{\mathcal{Z}_{\rm EO}}) \\
&\qquad \times \Big(\mathbb{P}(\widehat{M} \ne m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}) + \mathbb{P}(\widehat{M} \ne m'|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\rm EO}}})\Big).
\end{aligned}$$

Lemma 5. *For any $\mathbf{x}_{\mathcal{Z}_{\rm EO}}$ and $m \le m'$, regardless of the decoder γ Bob uses, we have $\mathbb{P}(\widehat{M} \ne m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\rm EO}}}) + \mathbb{P}(\widehat{M} \ne m'|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\rm EO}}}) \ge 1$.*

The proof of Lemma 5 is provided in the Appendix. Combining (18), Lemmas 4 and 5, we conclude that if the rate equals $L - 2z_{\rm EJ} - z_{\rm JO} + \epsilon$ for any $\epsilon > 0$, the error probability $\mathbb{P}(M \ne \widehat{M}) \ge \frac{\epsilon^2}{12L^2}$. This completes the converse proof when secrecy is not required.

Finally, we prove by contradiction that no positive rate is achievable with secrecy constraints. Suppose there exists a scheme of rate $\epsilon > 0$. James' strategy is as follows: he adds random noise on the links in $\mathcal{Z}_{\rm J}$, and eavesdrops on the links in $\mathcal{Z}_{\rm E}$. Note that $L - z_J \le z_{\rm E}$ in the strong adversary regime. Since the links in $\mathcal{Z}_{\rm J}$ do not carry any useful information, Bob must be able to decode from the remaining $L - z_J$ links. However, as the scheme satisfies the secrecy requirement, any subset of links of size $z_{\rm E}$ or less does not carry any information about the message. This results in a contradiction.

2) Overwrite jamming: The first goal is to show that, without the secrecy constraints, the rate cannot exceed $C^{\rm ow} = L - 2z_J$. The proof is similar to that for additive jamming, hence we only sketch the differences in the following. Suppose $\log|\mathcal{M}| = n(L-2z_J+\epsilon)$ for any $\epsilon > 0$. Since James is able to control the outputs on $\mathcal{Z}_{\rm JO}$ under overwrite jamming, he may carefully design the jamming patterns on $\mathcal{Z}_{\rm JO}$, by adopting the following observe-and-attack strategy (which is slightly different from that for additive jamming).

1) Choose $\mathcal{Z}_{\rm EO} = \{E_1, \ldots, E_{L-2z_J}\}$ to eavesdrop. This is possible since $z_{\rm EO} \ge L - 2z_J$ in the strong adversary regime $\mathcal{Z}_{\rm s}^{\rm ow}$.
2) For the remaining $2z_J$ links, let $\mathcal{Z}_a \triangleq \{E_{L-2z_J+1}, \ldots, E_{L-z_J}\}$ and $\mathcal{Z}_b \triangleq \{E_{L-z_J+1}, \ldots, E_L\}$, and choose $\mathcal{Z}_{\rm EJ} \cup \mathcal{Z}_{\rm JO}$ to be either $\mathcal{Z}_a$ or $\mathcal{Z}_b$ with equal probability;
3) The attack strategy is to first generate a fake message $M' \sim P_{M|\mathbf{X}_{\mathcal{Z}_{\rm EO}}}$ based on the observations $\mathbf{x}_{\mathcal{Z}_{\rm EO}}$, use Alice's encoder $P_{\mathbf{X}|M}$ to generate a fake codeword $\mathbf{X}'$, and then replace the original sub-codeword $\mathbf{X}_{\mathcal{Z}_{\rm EJ}\cup\mathcal{Z}_{\rm JO}}$ with the new sub-codeword $\mathbf{X}'_{\mathcal{Z}_{\rm EJ}\cup\mathcal{Z}_{\rm JO}}$.

By applying the same proof techniques like for additive jamming, one can show that the error probability $\mathbb{P}(M \ne \widehat{M}) \ge \frac{\epsilon^2}{12L^2}$. With the secrecy constraints, the converse proofs for additive jamming and overwrite jamming are exactly the same, hence we omit it here for brevity.

VI. Conclusion

This work investigates the problem of reliable and secure communication over the wiretap multipath network in the presence of a limited-view adversary. Our main contribution is to characterize the capacity and secrecy capacity of this network under two different settings — additive jamming and overwrite jamming. By combining appropriate MDS codes with pairwise hashing encoding/decoding strategies, we prove that our achievability scheme is robust to any adversarial jamming strategy as well as achieves information-theoretic secrecy. The converse proof also requires a non-trivial combination of various information-theoretic techniques.

Having characterized the fundamental limits of the wiretap multipath network, an interesting direction for future work is to extend the capacity and secrecy capacity characterizations to more generalized networks with internal nodes in the presence of adversaries (such as the secure network coding problem).

APPENDIX

Proof of Lemma 4. Consider a specific $\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}} \in \mathcal{A}_1$. Due to the independence of M and M', we have $H(M|M', \mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) = H(M|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) \geq \frac{n\epsilon}{2}$, and by Fano's inequality, we have

$$\begin{aligned}
&\frac{n\epsilon}{2} \leq H(M|M', \mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) \\
&\leq (\log|\mathcal{M}|) \cdot \mathbb{P}(M \neq M'|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) + H(\mathbb{P}(M \neq M'|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}})) \\
&\leq nL \cdot \mathbb{P}(M \neq M'|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) + 1.
\end{aligned}$$

Therefore, for sufficiently large n, we have

$$\begin{aligned}
&\sum_{m \neq m'} P_{M|\mathbf{X}_{\mathcal{Z}_{\mathrm{EO}}}}(m|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) P_{M|\mathbf{X}_{\mathcal{Z}_{\mathrm{EO}}}}(m'|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) \\
&= \mathbb{P}(M \neq M'|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}) \geq \frac{\epsilon}{2L} - \frac{1}{nL} \geq \frac{\epsilon}{3L}.
\end{aligned}$$

□

Proof of Lemma 5. Let $P_{\mathbf{Y}|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}}$ and $P_{\mathbf{Y}|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}}$ be the distributions of $\mathbf{Y}$ conditioned on the event $\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}$ and $\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}$, respectively. It is worth noting that these two distributions are exactly the same. This is because

$$\begin{aligned}
&\mathbf{Y}_{\mathcal{Z}_{\mathrm{EO}}} = \mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, && \mathbf{Y}_{\mathcal{Z}_{\mathrm{JO}}} = \mathbf{E}_{\mathcal{Z}_{\mathrm{JO}}}, \\
&\mathbf{Y}_{\mathcal{Z}_a} = \begin{cases} \mathbf{X}_{\mathcal{Z}_a}, & \text{w.p. } 1/2 \\ \mathbf{X}'_{\mathcal{Z}_a}, & \text{w.p. } 1/2, \end{cases} && \mathbf{Y}_{\mathcal{Z}_b} = \begin{cases} \mathbf{X}_{\mathcal{Z}_b}, & \text{w.p. } 1/2 \\ \mathbf{X}'_{\mathcal{Z}_b}, & \text{w.p. } 1/2, \end{cases}
\end{aligned}$$

and both Alice and James use the same encoder $P_{\mathbf{X}|M}$ with marginal conditional distributions $P_{\mathbf{X}_{\mathcal{Z}_a}|\mathbf{X}_{\mathcal{Z}_{\mathrm{EO}}},M}$ and $P_{\mathbf{X}_{\mathcal{Z}_b}|\mathbf{X}_{\mathcal{Z}_{\mathrm{EO}}},M}$ (whose subscripts will be omitted for convenience) such that

- Under $\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}$, $\mathbf{X}_{\mathcal{Z}_a} \sim P(\mathbf{X}_{\mathcal{Z}_a}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m)$, $\mathbf{X}'_{\mathcal{Z}_a} \sim P(\mathbf{X}_{\mathcal{Z}_a}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m')$, $\mathbf{X}_{\mathcal{Z}_b} \sim P(\mathbf{X}_{\mathcal{Z}_b}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m)$, $\mathbf{X}'_{\mathcal{Z}_b} \sim P(\mathbf{X}_{\mathcal{Z}_b}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m')$,
- Under $\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}$, $\mathbf{X}_{\mathcal{Z}_a} \sim P(\mathbf{X}_{\mathcal{Z}_a}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m')$, $\mathbf{X}'_{\mathcal{Z}_a} \sim P(\mathbf{X}_{\mathcal{Z}_a}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m)$, $\mathbf{X}_{\mathcal{Z}_b} \sim P(\mathbf{X}_{\mathcal{Z}_b}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m')$, $\mathbf{X}'_{\mathcal{Z}_b} \sim P(\mathbf{X}_{\mathcal{Z}_b}|\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}, m)$.

Therefore, we have

$$\begin{aligned}
&\mathbb{P}(\widehat{M} \neq m|\mathcal{E}_{m,m',\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}) + \mathbb{P}(\widehat{M} \neq m'|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}) \\
&= \sum_{\mathbf{y}} P_{\mathbf{Y}|\mathcal{E}_{m,m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}}(\mathbf{y}) \mathbb{1}\{\gamma(\mathbf{y}) \neq m\} \\
&\qquad + \sum_{\mathbf{y}} P_{\mathbf{Y}|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}}(\mathbf{y}) \mathbb{1}\{\gamma(\mathbf{y}) \neq m'\} \\
&= \sum_{\mathbf{y}} \left(\mathbb{1}\{\gamma(\mathbf{y}) \neq m\} + \mathbb{1}\{\gamma(\mathbf{y}) \neq m'\}\right) P_{\mathbf{Y}|\mathcal{E}_{m',m,\mathbf{x}_{\mathcal{Z}_{\mathrm{EO}}}}}(\mathbf{y}) \\
&\geq 1.
\end{aligned}$$

□

REFERENCES

[1] Q. Zhang, S. Kadhe, M. Bakshi, S. Jaggi, and A. Sprintson, "Talking reliably, secretly, and efficiently: A "complete" characterization," in *IEEE Information Theory Workshop (ITW)*, 2015, pp. 1–5.

[2] R. C. Singleton, "Maximum distance q-nary codes," *IEEE Transactions on Information Theory*, vol. 10, no. 2, pp. 116–118, Apr 1964.

[3] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," in *Proceedings of IEEE International Symposium on Information Theory*, 2005, pp. 1455–1459.

[5] I. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[6] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. EUROCRYPT 84 workshop on Advances in cryptology: theory and applicationof cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 33–51.

[7] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.

[8] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network codes resilient to jamming and eavesdropping," *Networking, IEEE/ACM Transactions on Networking*, vol. 22, no. 6, pp. 1978–1987, Dec 2014.

[9] W. Guo, D. He, and N. Cai, "Some results on network error correction with time-varying adversarial errors," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 1797–1808, 2018.

[10] 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)*, 2017, pp. 1172–1176.

[11] N. Cai and M. Hayashi, "Secure network code for adaptive and active attacks with no-randomness in intermediate nodes," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1428–1448, 2019.

[12] M. Hayashi and N. Cai, "Asymptotically secure network code for active attacks," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 3245–3259, 2021.

[13] M. Hayashi, M. Owari, G. Kato, and N. Cai, "Reduction theorem for secrecy over linear network code for active attacks," *Entropy*, vol. 22, no. 9, p. 1053, 2020.

[14] S. Jaggi, "Design and analysis of network codes," Ph.D. dissertation, California Institute of Technology, 2005.

[15] S. Jaggi and M. Langberg, "Network security," in *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, Eds. Academic Press, 2012.

[16] S. Li, R. Bitar, S. Jaggi, and Y. Zhang, "Network coding with myopic adversaries," *arXiv preprint arXiv:2102.09885*, 2021.

[17] 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.

[18] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Transactions On information theory*, vol. 61, no. 7, pp. 3912–3936, 2015.

[19] S. Kadhe, S. Jaggi, M. Bakshi, and A. Sprintson, "Reliable, deniable, and hidable communication over multipath networks," in *IEEE International Symposium on Information Theory*, 2014, pp. 611–615.

[20] J. Song, Q. Zhang, M. Bakshi, S. Jaggi, and S. Kadhe, "Multipath stealth communication with jammers," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 761–765.

[21] J. Song, Q. Zhang, S. Kadhe, M. Bakshi, and S. Jaggi, "Stealthy communication over adversarially jammed multipath networks," *IEEE Transactions on Communications*, 2020.

[22] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 970–983, 2016.

[23] C. Hofmeister, R. Bitar, M. Xhemrishi, and A. Wachter-Zeh, "Secure private and adaptive matrix multiplication beyond the singleton bound," *IEEE Journal on Selected Areas in Information Theory*, 2022.

[24] V. Aggarwal, L. Lai, A. R. Calderbank, and H. V. Poor, "Wiretap channel type ii with an active eavesdropper," in *2009 IEEE International Symposium on Information Theory (ISIT)*, 2009, pp. 1944–1948.

[25] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *Journal of the ACM (JACM)*, vol. 40, no. 1, pp. 17–47, 1993.

[26] A. Patra, A. Choudhury, C. Pandu Rangan, and K. Srinathan, "Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality," *International Journal of Applied Cryptography*, vol. 2, no. 2, pp. 159–197, 2010.
[27] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2000, pp. 351–368.
[28] K. Konstantinidis and A. Ramamoorthy, "Aspis: Robust detection for distributed learning," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 2058–2063.
[29] M. R. Gary and D. S. Johnson, "Computers and intractability: A guide to the theory of np-completeness," 1979.
[30] F. P. Preparata and D. V. Sarwate, "Computational complexity of fourier transforms over finite fields," *Mathematics of Computation*, vol. 31, no. 139, pp. 740–751, 1977.
[31] S. B. Wicker, *Error control systems for digital communication and storage*. Prentice hall Englewood Cliffs, 1995, vol. 1.

Qiaosheng (Eric) Zhang received his B.Eng. (Hons.) and Ph.D. degrees from the Department of Information Engineering, The Chinese University of Hong Kong (CUHK), in 2015 and 2019, respectively. From 2019 to 2022, he was a Research Fellow with the Department of Electrical and Computer Engineering, National University of Singapore (NUS). He is currently a Researcher with the Shanghai Artificial Intelligence Laboratory. His research interests include information theory and machine learning. Specifically, he focuses on covert communication, community detection, and (multi-agent) reinforcement learning.

Swanand Ravindra Kadhe is a Senior Research Scientist in IBM Research, San Jose, CA. Prior to joining IBM, he was a postdoctoral researcher in the EECS Department at the University of California Berkeley. He earned his Ph.D. degree in Electrical and Computer Engineering from Texas A&M University in 2017. He is a recipient of the 2016 Graduate Teaching Fellowship from the College of Engineering at Texas A&M University. He has been a visiting researcher at Nokia Bell Labs, Duke University, and The Chinese University of Hong Kong. From 2009 to 2012, he was an R&D engineer at the TCS Innovation Labs, Bangalore. His research interests lie broadly in privacy and security of machine learning, information and coding theory, and blockchains.

Mayank Bakshi (Member, IEEE) received his B.Tech. and M.Tech. degrees from the Indian Institute of Technology Kanpur, in 2003 and 2005, respectively, and the Ph.D. degree from the California Institute of Technology (Caltech) in 2011. Subsequently, he was a postdoctoral scholar and a research assistant professor at the Chinese University of Hong Kong from 2012-19 and a principal researcher at Theory Lab, Huawei Hong Kong from 2019-21. Currently, he is a research scientist at Arizona State University. His research interests include physical layer security, adversarially robust communications and learning, and sparse recovery.

Sidharth (Sid) Jaggi (Senior Member, IEEE) received his B. Tech. from I.I.T. Bombay 2000, his M.S. and Ph.D. degrees from the CalTech in 2001 and 2006 respectively, all in EE. He spent 2006 as a Postdoctoral Associate at LIDS MIT. He joined the Department of Information Engineering at the Chinese University of Hong Kong in 2007, and the School of Mathematics at the University of Bristol in 2020. His interests lie at the intersection of network information theory, coding theory, and algorithms. His research group thus (somewhat unwillingly) calls itself the CAN-DO-IT team (Codes, Algorithms, Networks: Design and Optimization for Information Theory). Examples of topics he has dabbled in include network coding, sparse recovery/group-testing, covert communication, and his current obsession is with adversarial channels.

Alex Sprintson (Senior Member, IEEE) is a faculty member in the Department of Electrical and Computer Engineering, Texas A&M University, College Station, where he conducts research on security and privacy, network coding, wireless networks, and distributed storage systems. Dr. Sprintson received the Wolf Award for Distinguished Ph.D.students, the Viterbi Postdoctoral Fellowship, the TAMU College of Engineering Outstanding Contribution Award, and the NSF CAREER award. From 2013 and 2019 he served as an Associate Editor of the IEEE Transactions on Wireless Communications. He has been a member of the Technical Program Committee for the IEEE Infocom 2006-2023 From Sept. 2018 to Sept. 2022, Dr. Sprintson served as a rotating program director at the US National Science Foundation (NSF).