

scheme as well. After the encryption, the size of the seed used to compress each of files is 3.27[KB]. The encrypted seed is stored on the second server. The rest of the files are stored over the rest of the servers, s.t. each server stores one file. This hybrid scheme is secured against both IT and Crypto-Eve's. The overall data rate of the proposed scheme is 0.79.

4) Finally, we assess the computational complexity of the proposed communication scheme. Complexity is measured in this paper, as the number of binary operations required to perform encoding and decoding of all the messages. We show that NU-HUNCC, which encrypts only a subset of links using McEliece, exhibits a more efficient run-time complexity compared to NUM. NU-HUNCC's efficiency makes it a promising candidate for practical applications.

The remainder of this paper is structured in the following manner. Sec. II presents NU-HUNCC setting, while Sec. III provides the comprehensive security definitions for IS and ISS-CCA1. In Sec. IV, we introduce the encoding/decoding algorithm for NU-HUNCC. In Sec. V, we provide the key findings and theorems of this paper. Sec. VI offers numerical results demonstrating the performance of NU-HUNCC. The proofs of the theorems provided in the paper are given in Sec. VII, VIII, IX, X, and Appendixes A and B. We conclude the paper is Sec. XI.

II. SYSTEM MODEL

We consider a communication system where Alice wishes to transmit ℓ non-uniform confidential message³ over ℓ noiseless links, $\mathcal{L} = \{1, \dots, \ell\}$, to Bob, in the presence of an eavesdropper, Eve. The messages are taken from a DMS (\mathcal{V}, p_V) s.t. $\mathcal{V} \in \{0, 1\}$. We denote the source message matrix by $\underline{V}_{\mathcal{L}} \in \mathbb{F}_2^{\ell \times n}$ when n is the size of each source message.

Bob's observations are denoted by $\underline{Y}_{\mathcal{L}}$. Those observations, provide Bob reliable decode $\underline{V}_{\mathcal{L}}$ with high probability. That is, $\mathbb{P}(\hat{\underline{V}}_{\mathcal{L}}(\underline{Y}_{\mathcal{L}}) \neq \underline{V}_{\mathcal{L}}) \leq \epsilon_e$, where $\hat{\underline{V}}_{\mathcal{L}}(\underline{Y}_{\mathcal{L}})$ is the estimation of $\underline{V}_{\mathcal{L}}$. We consider two types of Eve: 1) IT-Eve, which observes any subset $\mathcal{W} \subset \mathcal{L}$ of the links s.t. $|\mathcal{W}| \triangleq w < \ell$, but is computationally unbounded, and 2) Crypto-Eve which observes all the links, but is bounded computationally. We denote IT-Eve's observations by $\underline{Z}_{\mathcal{W}}$ and Crypto-Eve's observations by $\underline{Z}_{\mathcal{L}}$.

III. SECURITY DEFINITIONS

In this section, we provide the formal security definitions used throughout this paper.

A. Security against IT-Eve

Against IT-Eve, we consider information-theoretic security. For any subset of $k_s < \ell - w$ source messages, we use the notion of k_s individual security (k_s -IS). We measure the leakage of information to the eavesdropper using *non-normalized variational distance*, denoted by $\mathbb{V}(\cdot, \cdot)$. Additionally, we require the code to be reliable where the reliability is measured by the decoding error probability at Bob's. For a

code to be k_s -IS we require the information leakage and error probability to be negligible. We now formally define k_s -IS:

Definition 1. (k_s Individual Security) Let $\underline{V}_{\mathcal{L}} \in \mathbb{F}_q^{\ell \times n}$ be a set of ℓ confidential source messages Alice intends to send, $\underline{Y}_{\mathcal{L}}$ be Bob's observations of the encoded messages, and $\underline{Z}_{\mathcal{W}}$ be IT-Eve's observations of the encoded messages. We say that the coding scheme is k_s -IS if:

- 1) *Security*: $\forall \epsilon_s > 0, \forall \mathcal{W} \subset \mathcal{L}$ s.t. $|\mathcal{W}| = w < \ell$, and $\forall \underline{V}_{\mathcal{K}_s} \subset \underline{V}_{\mathcal{L}}$ s.t. $|\mathcal{K}_s| = k_s < \ell - w$, it holds that $\mathbb{V}(p_{\underline{Z}_{\mathcal{W}}|\underline{V}_{\mathcal{K}_s}=\underline{v}_{\mathcal{K}_s}}, p_{\underline{Z}_{\mathcal{W}}}) \leq \epsilon_s$.
- 2) *Reliability*: $\forall \epsilon_e > 0$ it holds that $\mathbb{P}(\hat{\underline{V}}_{\mathcal{L}}(\underline{Y}_{\mathcal{L}}) \neq \underline{V}_{\mathcal{L}}) \leq \epsilon_e$, where $\hat{\underline{V}}_{\mathcal{L}}(\underline{Y}_{\mathcal{L}})$ is the decoding estimation of the message matrix from Bob's observations.

Thus, IT-Eve that observes any subset of w links in the network can't obtain any information about any set of $k_s < \ell - w$ individual messages, $\underline{V}_{\mathcal{K}_s}$. However, IT-Eve might be able to obtain some insignificant information about the mixture of all the messages. Yet, this negligible information is controlled [12], [55], [56]. Bob can reliably decode the message matrix from his observations of the encoded messages.

B. Security against Crypto-Eve

Crypto-Eve may perform passive/active attacks against Alice and the ciphertexts she produces, to obtain information about confidential messages. Two of the most common attacks given in the literature are the chosen-plaintext attack (CPA) and the chosen-ciphertext attack (CCA) [57]. In both attacks, Crypto-Eve is given a ciphertext from which she tries to obtain information about the plaintext. In CCA Crypto-Eve is active and prior to receiving the ciphertext, she can question a decryption oracle to provide her the plaintexts for a limited number of ciphertexts of her choice. However, she can't use this decryption oracle after receiving the test ciphertext [57]. The information leakage is measured by Crypto-Eve's ability to distinguish between plaintexts given the test ciphertext provided by Alice. There are two ways in which this leakage is measured: 1) indistinguishability (IND) - by observing a ciphertext created from one of two possible plaintexts, Crypto-Eve can't distinguish between the two plaintexts better than a uniform coin-toss, 2) semantic security (SS) - by observing a ciphertext, Crypto-Eve can't obtain any information about the original plaintext or some function applied on it, that is more significant than the information she obtains from the plaintexts original probability distribution. Those two definitions are equivalent, i.e. a cryptosystem that is IND is also SS and vice versa [1]. The security level of a cryptosystem is defined by the combination of Crypto-Eve's attack model and its information leakage.

In this paper, we introduce a new notion of security, individual semantic security against a chosen ciphertext attack (ISS-CCA1). This notion of security is based on SS-CCA1 cryptographic security [1], [57], and usually requires the encryption scheme to be probabilistic⁴. To properly define ISS-

³In this paper, we assume the messages are independent to focus on the key methods and results. However, our proposed solution can be easily shown to be valid for dependent sources by using joint source coding schemes [54].

⁴ To focus on our main contributions, we choose to work with public key encryption schemes, but any other PQ probabilistic encryption schemes would have achieved similar results.