2023 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-7554-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIT54713.2023.10206773

Secret Sharing Over a Gaussian Broadcast Channel: Optimal Coding Scheme Design and Deep Learning Approach at Short Blocklength

Rumia Sultana, Vidhi Rana, Rémi A. Chou
Department of EECS, Wichita State University, Wichita, KS 67260
Emails: {rxsultana@shockers.wichita, vxrana@shockers.wichita, remi.chou@wichita}.edu

***Abstract*—Consider a secret sharing model where a dealer shares a secret with several participants through a Gaussian broadcast channel such that predefined subsets of participants can reconstruct the secret and all other subsets of participants cannot learn any information about the secret. Our first contribution is to show that, in the asymptotic blocklength regime, it is optimal to consider coding schemes that rely on two coding layers, namely, a reliability layer and a secrecy layer, where the reliability layer is a channel code for a compound channel without any security constraint. Our second contribution is to design such a two-layer coding scheme at short blocklength. Specifically, we design the reliability layer via an autoencoder, and implement the secrecy layer with hash functions. To evaluate the performance of our coding scheme, we empirically evaluate the probability of error and information leakage, which is defined as the mutual information between the secret and the unauthorized sets of users channel outputs. We empirically evaluate this information leakage via a neural network-based mutual information estimator. Our simulation results demonstrate a precise control of the probability of error and leakage thanks to the two-layer coding design.**

I. Introduction

[1] and [2] pioneered the secret sharing model where a dealer distributes a secret among a set of participants with the requirement that only pre-defined sets of participants can recover the secret, while any other sets of colluding participants cannot learn any information about the secret. In such traditional secret sharing models (we refer to [3] for an excellent literature review of the subject), it is assumed that the dealer and each participant can communicate over an individual and perfectly secure channel at no cost. Later, with the goal to avoid this assumption, noisy resources aided secret sharing schemes have been studied for channel models [4] and source models [5]–[9], where no secure communication links are available between the dealer and the participants.

In this paper, we consider the same secret sharing model as in [4] where noisy resources, in the form of a Gaussian channel, are available between the dealer and participants. Specifically, the dealer can communicate with the participants over a Gaussian broadcast channel where each participant observes scalar Gaussian channel outputs. The dealer transmits a secret message by encoding it into a codeword, which is then sent over n uses of the channel and yields the channel output observations at the participants. In this setting, a reliability constraint ensures that any subset of participants with size t is able to recover the secret from their vector of t channel outputs, and a security constraint ensures that any subset of participants with size $z < t$ cannot learn any information about the secret from their vector of z channel outputs. These two constraints define a threshold access structure similar to traditional secret sharing models as in [1], [2], [10], [11].

A. Contributions

1) Optimal coding scheme design in the asymptotic regime: The secret sharing capacity has been established in [4] with a random coding argument that jointly considers the reliability and secrecy constraints. One of our contributions is to show that it is optimal to consider coding schemes that rely on two coding layers, namely, a reliability layer and a secrecy layer, to achieve the secret sharing capacity. Specifically, the secrecy layer can be implemented with hash functions, and the reliability layer can be implemented with a channel code for a compound channel without any security constraint.

The main insights and benefits of our result are (a) a modular approach that allows a simplified code design, for instance, if only one of the two layers need to be (re)designed, (b) a code design that offers a universal way of dealing with the secrecy constraint via hash functions, which is useful to ensure security against multiple subsets of colluding users that are associated with different channel statistics, (c) guidelines for a simplified code design at finite blocklength as discussed in Section I-A2.

2) Coding scheme design at finite blocklength: Following the two-layer coding approach described above, we design secret sharing schemes at finite blocklength. Specifically, we use a neural network-based autoencoder to design the reliability layer, and hash functions to design the security layer.

To evaluate the performance of our constructed code, we empirically evaluate the probability of error and estimate the information leakage for blocklengths n at most 20. Specifically, the information leakage is defined as the mutual information between the secret and the channel output observations for unauthorized sets of users. We evaluate the information leakage by using the mutual information neural estimator (MINE) from [12]. Our simulation results demonstrate a precise control of the probability of error and leakage thanks to the two separate coding layers.

This work was supported in part by NSF grant CCF-2047913.

B. Related works

1) Prior related works on compound wiretap channels: Theoretical and non-constructive results: The compound wiretap channel [13], [14] is a generalization of Wyner's wiretap channel [15] to the case of multiple unknown channel states, where secure and reliable communication needs to be guaranteed regardless of the channel state. The connection between compound wiretap channels and secret sharing over noisy channels has been established in [4] by remarking that, similar to compound settings, an access structure for secret sharing yields multiple security constraints and multiple reliability constraints that must be ensured simultaneously. While the capacity for the secret sharing model we consider has been established in [4], one of our contributions (see Section I-A1) is to show the optimality of a two-layer coding scheme design.

Results on code constructions: Explicit compound wiretap codes have been proposed for discrete memoryless channels for the asymptotic blocklength regime in [16]. Finite-length code constructions for scalar Gaussian compound channels have been studied in [17]. In contrast, in this paper, one of our contributions (see Section I-A2) is to not only design finite-length compound wiretap codes but to also consider vector Gaussian channel observations, which is needed in the context of the secret sharing problem we consider.

2) Prior related works on wiretap channels: While several wiretap code designs have been proposed for various channel models under non-information-theoretic security metrics, e.g., [18]–[25], we focus our discussion on works that, similar to our work, consider an information-theoretic security metric.

Results for the asymptotic blocklength regime: A coding strategy that separately handles the reliability and secrecy constraints with two separate coding layers has previously been used for the discrete wiretap channels in [26], [27], and the Gaussian wiretap channel in [28]. The above references consider the asymptotic blocklength regime. One of our contributions (see Section I-A1) is to not only generalize the result in [28] to a compound setting, but also to generalize it to vector, rather than scalar, Gaussian channel outputs.

Related code constructions in the non-asymptotic regime: Coding scheme designs based on feed-forward neural network autoencoders have also been proposed in [29], where the security and reliability constraints are handled jointly, and in [30], where the security and reliability constraints are handled separately. As discussed in Section I-A2, one of our contributions is to design a short blocklength coding scheme that, unlike the above references, handles (a) multiple reliability constraints and multiple security constraints simultaneously, i.e., a compound model, and (b) vector Gaussian channel outputs.

C. Organization of the paper

The remainder of the paper is organized as follows. The problem statement is provided in Section II. The main results are provided in Section III. A capacity-achieving two-layer coding scheme in the asymptotic regime is provided in Section IV, its analysis is omitted due to space constraints. In Section V, a finite blocklength implementation of the coding scheme of Section IV is proposed using a deep learning approach. Finally, Section VI provides concluding remarks.

II. Problem statement

Notation: For $a, b \in \mathbb{R}$, define $[a] \triangleq [1, \lceil a \rceil] \cap \mathbb{N}$, $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. The components of a vector X^n of length $n \in \mathbb{N}$ are denoted with subscripts, i.e., $X^n \triangleq (X_1, X_2, \dots, X_n)$. $\|.\|$ denotes the Euclidean norm and $\|.\|_1$ denotes the L^1 norm.

Consider a dealer and J participants indexed in $\mathcal{J} \triangleq [J]$. We assume that the dealer can communicate with the participants over a Gaussian broadcast channel defined as

$$Y_j^n \triangleq X^n + N_j^n, \quad \forall j \in \mathcal{J}, \tag{1}$$

where X^n is the signal transmitted by the dealer with the power constraint $\frac{1}{n}\sum_{i=1}^n X_i^2 \leq P$, Y_j^n is the channel observation at Participant $j \in \mathcal{J}$, $j \in \mathcal{J}$, and N_j^n is a random vector of length n with components independent and identically distributed according to a zero-mean Gaussian random variable with variance σ_j^2. The noise vectors N_j^n, $j \in \mathcal{J}$, are assumed independent.

For $t \in [J]$, the set of authorized sets of users is defined as $\mathbb{A}_t \triangleq \{\mathcal{A} \subseteq \mathcal{J} : |\mathcal{A}| \geq t\}$, and, for $z \in [t-1]$, the set of unauthorized sets of users is defined as $\mathbb{U}_z \triangleq \{\mathcal{U} \subseteq \mathcal{J} : |\mathcal{U}| \leq z\}$. The parameters t and z are chosen by the system designer. In the following, for any $\mathcal{U} \in \mathbb{U}_z$ and $\mathcal{A} \in \mathbb{A}_t$, we use the notation $Y_{\mathcal{U}}^n \triangleq (Y_j^n)_{j\in\mathcal{U}}$, $N_{\mathcal{U}}^n \triangleq (N_j^n)_{j\in\mathcal{U}}$, $Y_{\mathcal{A}}^n \triangleq (Y_j^n)_{j\in\mathcal{A}}$, and $N_{\mathcal{A}}^n \triangleq (N_j^n)_{j\in\mathcal{A}}$ such that

$$Y_{\mathcal{A}}^n \triangleq \mathbf{1}_t X^n + N_{\mathcal{A}}^n, \quad \mathcal{A} \in \mathbb{A}_t, \tag{2}$$

$$Y_{\mathcal{U}}^n \triangleq \mathbf{1}_z X^n + N_{\mathcal{U}}^n, \quad \mathcal{U} \in \mathbb{U}_z, \tag{3}$$

where $\mathbf{1}_t$ and $\mathbf{1}_z$ are all-ones column vectors of size t and z, respectively, and the covariance matrices of $N_{\mathcal{A}}$ and $N_{\mathcal{U}}$ are $\Sigma_{\mathcal{A}} \triangleq \text{diag}((\sigma_j^2)_{j\in\mathcal{A}})$ and $\Sigma_{\mathcal{U}} \triangleq \text{diag}((\sigma_j^2)_{j\in\mathcal{U}})$, respectively.

Definition 1. *A $(2^{nR_s}, t, z, n)$ secret sharing strategy consists of*

- *A secret S uniformly distributed over $\mathcal{S} \triangleq [2^{nR_s}]$;*
- *An encoding function $f : \mathcal{S} \to \mathbb{R}^n$;*
- *A decoding function $g_{\mathcal{A}} : \mathbb{R}^{nt} \to \mathcal{S}$ for each set $\mathcal{A} \in \mathbb{A}_t$;*

and operates as follows:

1) *The dealer encodes the secret $S \in \mathcal{S}$ as X^n;*
2) *The dealer sends X^n over the channel and Participant $j \in \mathcal{J}$ observes Y_j^n;*
3) *Any subset of participants $\mathcal{A} \in \mathbb{A}_t$ can form an estimate of S as $\hat{S}(\mathcal{A}) \triangleq g_{\mathcal{A}}(Y_{\mathcal{A}}^n)$.*

Definition 2. *A secret sharing rate R_s is achievable if there exists a sequence of $(2^{nR_s}, t, z, n)$ secret sharing strategies such that*

$$\lim_{n\to+\infty} \max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = 0, \qquad (\textit{Reliability}) \tag{4}$$

$$\lim_{n\to+\infty} \max_{\mathcal{U}\in\mathbb{U}_z} I(S; Y_{\mathcal{U}}^n) = 0. \qquad (\textit{Security}) \tag{5}$$

(4) *means that any subset of at least t participants is able to recover the secret, and* (5) *means that any subset of at most*

z participants cannot learn any information about the secret. The secret sharing capacity C_s is defined as the supremum of all achievable secret sharing rates.

Note that when the secret sharing capacity is positive, the length of each share always scales linearly with the size of the secret, since, by definition, the size of the secret is linear with the number of channel observations n.

Theorem 1 (Adapted from [4])**.** *The secret sharing capacity is given by*

$$C_s = \frac{1}{2}\min_{\mathcal{A}\in\mathbb{A}_t}\min_{\mathcal{U}\in\mathbb{U}_z}\log\frac{1+\sum_{l\in\mathcal{A}}\frac{P}{\sigma_l^2}}{1+\sum_{l\in\mathcal{U}}\frac{P}{\sigma_l^2}}.$$

III. Main results

A. Asymptotic optimality of two-layer coding scheme

We first introduce two-layer coding schemes in Definition 3.

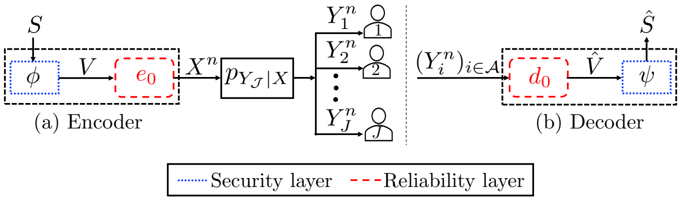


Fig. 1. Two-layer code design. The reliability layer is implemented using a channel code (e_0, d_0) without any security constraints, and the security layer is implemented using the functions ψ and ϕ.

Definition 3. *A two-layer secret sharing coding scheme consists of*

- *A reliability layer defined by an encoder/decoder pair (e_0, d_0) without any security constraints for the compound channel defined in* (2) *such that if $X^n \triangleq e_0(V)$ is the channel input, where V is uniformly distributed over $\{0,1\}^r$, $r\in\mathbb{N}$, and $\|X^n\|^2 \leq nP$ and $Y_{\mathcal{A}}^n$, $\mathcal{A}\in\mathbb{A}_t$, are the channel outputs, then $\lim_{n\to+\infty}\max_{\mathcal{A}\in\mathbb{A}_t}\mathbb{P}[d_0(Y_{\mathcal{A}}^n)\neq V]=0$;*
- *A secrecy layer is defined by two functions $\psi : \{0,1\}^k \to \{0,1\}^r$ and $\phi : \{0,1\}^r \to \{0,1\}^k$, for some $k\in\mathbb{N}$;*

and operates as follows:

1) *Encoding: The dealer encodes a secret message S that is uniformly distributed over $\mathcal{S}\triangleq\{0,1\}^k$ as $e_0(\phi(S))$. Hence, the encoder e of a two-layer secret sharing coding scheme is*

$$\begin{aligned} e : \mathcal{S} &\to \mathbb{R}^n \\ s &\mapsto e_0(\phi(s)). \end{aligned}$$

2) *Decoding: From the channel output observations $Y_{\mathcal{A}}^n$, $\mathcal{A}\in\mathbb{A}_t$, the participants in $\mathcal{A}$ estimate S as $\hat{S}(\mathcal{A})\triangleq\psi(d_0(Y_{\mathcal{A}}^n))$. Hence, the decoder d of a two-layer secret sharing coding scheme is*

$$\begin{aligned} d : \mathbb{R}^{nt} &\to \mathcal{S} \\ y^{nt} &\mapsto \psi(d_0(y^{nt})). \end{aligned}$$

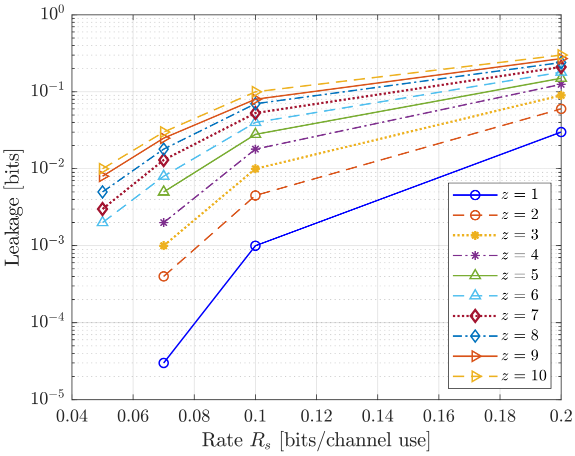


Fig. 2. Information leakage $\max_{\mathcal{U}\in\mathbb{U}_z} I(S;Y_{\mathcal{U}}^n)$ versus secret sharing rate $R_s = \frac{k}{n}$ for $z\in[10]$.

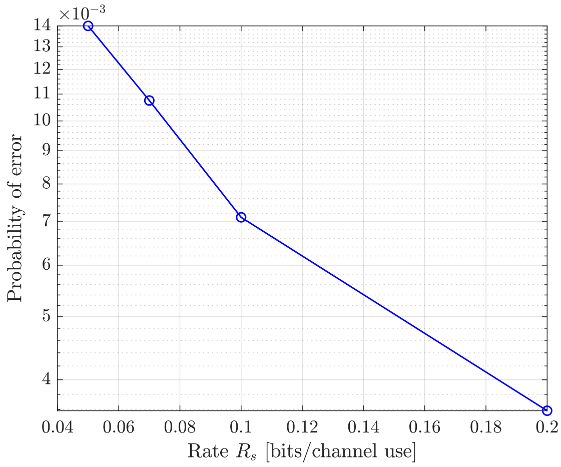


Fig. 3. Probability of error $\max_{\mathcal{A}\in\mathbb{A}_t}\mathbb{P}[\hat{S}(\mathcal{A})\neq S]$ versus secret sharing rate $R_s = \frac{k}{n}$.

The architecture of a two-layer coding scheme, as described in Definition 3, is depicted in Figure 1.

Theorem 2. *There exists a two-layer secret sharing scheme, as in Definition 3, that achieves the secret sharing capacity C_s. A two-layer secret sharing scheme that achieves C_s is presented in Section IV, its analysis is omitted due to space constraints.*

B. Design of a secret sharing coding scheme at short blocklength and performance evaluation

We design a two-layer coding scheme at finite blocklength, as defined in Definition 3. As detailed in Section V-A, we design the reliability layer using an autoencoder (e_0, d_0) and the secrecy layer via a two-universal hash function ψ.

In our simulations, detailed in Section V-B, we consider $J = 200$ participants, $t = 100$, $z \in [10]$, and $\sigma_j^2 \triangleq 10^{-\mathrm{SNR}/10}$, $j \in \mathcal{J}$, with a signal-to-noise ratio (SNR), $\mathrm{SNR} = -16$dB. Figure 2 shows the information leakage $\max_{U \in \mathbb{U}_z} I(S; Y_{\mathcal{U}}^n)$ with respect to the secret sharing rate $R_s = \frac{k}{n}$ when z varies in $[10]$, $k = 1$, and $n \in \{5, 10, 15, 20\}$. Figure 2 confirms the intuition that the information leakage increases as the secret rate increases, and, for a fixed rate, decreases as z decreases. Figure 3 shows the average probability of error $\max_{\mathcal{A} \in \mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S]$ with respect to the secret sharing rate $R_s = \frac{k}{n}$ when $k = 1$, and $n \in \{5, 10, 15, 20\}$.

IV. A TWO-LAYER CODING SCHEME

A. *Sufficient statistics*

Using Lemma 1 below, one can prove that there is no loss of generality in considering the following Equations (6) and (7) as channel model instead of (2) and (3). Hence, in this section, we consider the following channel model: For any $i \in [n]$,

$$\tilde{Y}_{\mathcal{A},i} \triangleq \sigma^2_{\tilde{Y}_{\mathcal{A}}} X_i + \tilde{N}_{\mathcal{A},i}, \quad \mathcal{A} \in \mathbb{A}_t, \tag{6}$$

$$\tilde{Y}_{\mathcal{U},i} \triangleq \sigma^2_{\tilde{Y}_{\mathcal{U}}} X_i + \tilde{N}_{\mathcal{U},i}, \quad \mathcal{U} \in \mathbb{U}_z, \tag{7}$$

where

$$\sigma^2_{\tilde{Y}_{\mathcal{A}}} \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}}^{-1} \mathbf{1}_t, \tag{8}$$

$$\sigma^2_{\tilde{Y}_{\mathcal{U}}} \triangleq \mathbf{1}_z^T \Sigma_{\mathcal{U}}^{-1} \mathbf{1}_z, \tag{9}$$

$$\tilde{N}_{\mathcal{A},i} \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}}^{-1} N_{\mathcal{A},i} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y}_{\mathcal{A}}}), \tag{10}$$

$$\tilde{N}_{\mathcal{U},i} \triangleq \mathbf{1}_z^T \Sigma_{\mathcal{U}}^{-1} N_{\mathcal{U},i} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y}_{\mathcal{U}}}). \tag{11}$$

Lemma 1 ([31, Lemma 3.1]). *Consider the channel model*

$$Y_{\mathcal{S}} = \mathbf{1}_{|\mathcal{S}|} X + N_{\mathcal{S}}, \quad \mathcal{S} \subset \mathcal{J},$$

where $N_{\mathcal{S}}$ is a Gaussian vector of length $|\mathcal{S}|$ with zero mean and covariance matrix $\Sigma_{\mathcal{S}}$. A sufficient statistic to correctly determine X from $Y_{\mathcal{S}}$ is the scalar $\tilde{Y}_{\mathcal{S}} = \mathbf{1}_{|\mathcal{S}|}^T \Sigma_{\mathcal{S}}^{-1} Y_{\mathcal{S}}, \mathcal{S} \subset \mathcal{J}$.

B. *Coding scheme*

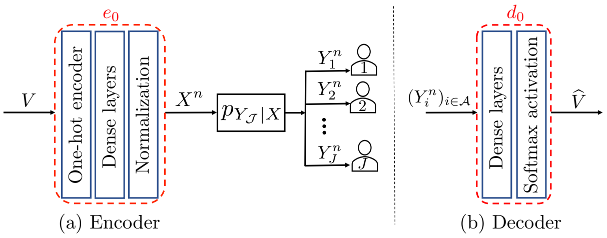
We first describe the reliability layer and secrecy layer in Sections IV-B1 and IV-B2, respectively. Then, in Section IV-B3, we describe the encoding and decoding of our proposed secret sharing scheme.

1) Reliability layer: By a random coding argument, there exists an encoder $e_0 : \{0,1\}^r \to \mathbb{R}$, $v \mapsto e_0(v)$ such that $\forall v \in \mathcal{V}$, $\frac{1}{n}\|e_0(v)\|^2 \leq P$, and a decoder $d_0 : \mathbb{R}^{nt} \to \{0,1\}^r$, $y^{nt} \mapsto v$, where

$$\lim_{n \to \infty} \frac{r}{n} = \frac{1}{2} \min_{\mathcal{A} \in \mathbb{A}_t} \log\Big(1 + \sigma^2_{\tilde{Y}_{\mathcal{A}}} P\Big), \tag{12}$$

such that if V is uniformly distributed over $\{0,1\}^r$ and $e_0(V)$ is sent over the channel described by (6), then

$$\lim_{n \to +\infty} \max_{\mathcal{A} \in \mathbb{A}_t} \mathbb{P}[d_0(\tilde{Y}_{\mathcal{A}}^n)) \neq V] = 0. \tag{13}$$



(a) Encoder (b) Decoder

Fig. 4. Architecture of the autoencoder (e_0, d_0) via feed-forward neural networks.

2) Secrecy layer: Define $\mathcal{L} \triangleq \{0,1\}^r \backslash \{\mathbf{0}\}$, and consider the two-universal hash family of functions $\mathcal{P} \triangleq \{v \mapsto \psi(\lambda, v)\}_{\lambda \in \mathcal{L}}$ [32], where ψ is defined as

$$\begin{aligned} \psi : \mathcal{L} \times \{0,1\}^r &\to \{0,1\}^k \\ (\lambda, v) &\mapsto (\lambda \odot v)_k, \end{aligned} \tag{14}$$

where $\odot$ is the multiplication in GF(2^r), and $(\cdot)_k$ selects the k most significant bits. Define also the mapping ϕ

$$\begin{aligned} \phi : \mathcal{L} \times \{0,1\}^k \times \{0,1\}^{r-k} &\to \{0,1\}^r \\ (\lambda, s, b) &\mapsto \lambda^{-1} \odot (s \| b), \end{aligned} \tag{15}$$

where $(\cdot \| \cdot)$ represents concatenation of two sequences of bits.

3) Encoding and decoding: The dealer draws a seed Λ uniformly at random from $\mathcal{L}$. This random seed Λ corresponds to a random choice of a hash function in the family $\mathcal{P}$ and is assumed to be known by all parties. Then, the dealer generates $r - k$ bits, denoted by B, uniformly at random from $\mathcal{B} \triangleq \{0,1\}^{r-k}$.

Encoding: The dealer encodes a secret S that is uniformly distributed over $\mathcal{S} \triangleq \{0,1\}^k$ as $X^n \triangleq e_0(\phi(\Lambda, S, B))$.

Decoding: From $\tilde{Y}_{\mathcal{A}}^n$, the set of participants in $\mathcal{A} \in \mathbb{A}_t$ estimates $V \triangleq \phi(\Lambda, S, B)$ as $\hat{V}(\mathcal{A}) \triangleq d_0(\tilde{Y}_{\mathcal{A}}^n)$, and forms an estimate of S as $\hat{S}(\mathcal{A}) \triangleq \psi(\Lambda, \hat{V}(\mathcal{A}))$.

V. SECRET SHARING SCHEME AT FINITE BLOCKLENGTH

A. *Secret sharing scheme design*

1) Reliability layer design: The design of the reliability layer consists in designing an encoder/decoder pair (e_0, d_0) as described in Definition 3. Let $\mathcal{V} \triangleq [2^r]$ be the message set. (e_0, d_0) is implemented with an autoencoder as in [33]. As depicted in Figure 4, the encoder e_0 consists of three layers. An embedding layer, where the input $v \in \mathcal{V}$ is mapped to a one-hot vector $1_v \in \mathbb{R}^{2^r}$, which is a vector whose components are all zeros except the v-th component which is one. Dense hidden layers that take v as input and return an n-dimensional vector. And, a normalization layer that ensures that the codeword $e_0(v)$, $v \in \mathcal{V}$, meets the average power constraint $\frac{1}{n}\|e_0(v)\|^2 \leq P$. As depicted in Figure 4, the decoder consists of dense hidden layers and a softmax layer. More specifically, let $\mu^{|\mathcal{V}|}$ be the output of the last dense layer in the decoder. The softmax layer takes $\mu^{|\mathcal{V}|}$ as input and returns a vector of probabilities $p^{|\mathcal{V}|} \in [0,1]^{|\mathcal{V}|}$, whose components p_v, $v \in \mathcal{V}$, are $p_v \triangleq \exp(\mu_v)(\sum_{i=1}^{|\mathcal{V}|}\exp(\mu_i))^{-1}$. Finally, the decoded message $\hat{v}$ corresponds to the index of the component of $p^{|\mathcal{V}|}$ associated with the highest probability, i.e., $\hat{v} \in \arg\max_{v\in\mathcal{V}} p_v$. The autoencoder is trained over all messages $v \in \mathcal{V}$ using a stochastic gradient descent (SGD) as in [34] and the categorical cross-entropy loss function.

2) Secrecy layer design: We implement the secrecy layer with the functions ψ and ϕ defined in Equations (14) and (15), respectively. Note that, unlike the asymptotic regime, we will choose a fixed seed $\lambda \in \mathcal{L}$ rather than a random seed.

3) Encoding and decoding for secret sharing scheme: The idea of the coding scheme below is to repeat $\gamma \in \mathbb{N}$ times the coding scheme described in Section IV-B. Hence, after the γ repetitions, γ secrets have been shared. With the objective to reduce the information leakage, the dealer and the participants extract another secret from these γ secrets with a two-universal hash function. The price paid for this reduced leakage is a decrease of the secret sharing rate.

Fix a seed $\lambda \in \mathcal{L}$, a seed $\alpha \in \{0,1\}^\gamma\backslash\{\mathbf{0}\}$, and set the length of the secret to $k = 1$.

Encoding: For $i \in [\gamma]$, the dealer generates $r - k$ bits, denoted by B_i, uniformly at random from $\{0,1\}^{r-k}$, and a bit M_i uniformly at random in $\{0,1\}$. The dealer sends the codeword $X_i^n \triangleq e_0(\phi(\lambda, M_i, B_i))$, $i \in [\gamma]$, such that the channel observations of the participants in $\mathcal{A} \in \mathbb{A}_t$ are $\tilde{Y}_{\mathcal{A},i}^n \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}}^{-1} Y_{\mathcal{A},i}^n$. Then, the dealer forms the secret $S \triangleq \psi(\alpha, M_{1:\gamma})$, where $M_{1:\gamma} \triangleq (M_i)_{i\in[\gamma]}$.

Decoding: From $\tilde{Y}_{\mathcal{A},i}^n$, $i \in [\gamma]$, the participants in $\mathcal{A} \in \mathbb{A}_t$ estimate $V_i \triangleq \phi(\lambda, S, B_i)$ as $\hat{V}_i \triangleq d_0(\tilde{Y}_{\mathcal{A},i}^n)$, M_i as $\hat{M}_i \triangleq \psi(\lambda, \hat{V}_i)$, and the secret S as $\hat{S}(\mathcal{A}) \triangleq \psi(\alpha, \hat{M}_{1:\gamma})$.

B. Performance evaluation

1) Simulation parameters: In our simulations, we consider $J = 200$ participants, $t = 100$, $z \in [10]$, and $\sigma_j^2 \triangleq 10^{-\text{SNR}/10}$, $j \in \mathcal{J}$, with a signal-to-noise ratio (SNR), SNR $= -16$dB. We also consider a secret of length $k = 1$ and power $P = 1$. Note that since the SNR is the same for all the participants, we have for $\mathcal{A}^* \triangleq [t]$ and $\mathcal{U}^* \triangleq [z]$, $\max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = \mathbb{P}[\hat{S}(\mathcal{A}^*) \neq S]$, and $\max_{\mathcal{U}\in\mathbb{U}_z} I(S; Y_{\mathcal{U}}^n) = I(S; Y_{\mathcal{U}^*}^n)$.

2) Performance evaluation of the reliability layer: For the parameters defined in Section V-B1, using Python 3.7 and Tensorflow 2.3, we train the autoencoder for $(n, r) = (5, 2)$ using SGD with the Adam optimizer [34] at a learning rate of 0.0001 over 100,000 random encoder input messages. To evaluate the performance of (e_0, d_0), we first generate the input $V \in \{0,1\}^r$. Then, V is passed through the trained encoder e_0, which generates the codewords X^n and the channel output $Y_{\mathcal{A}^*}^n$. By Lemma 1, without loss of generality, we consider $\tilde{Y}_{\mathcal{A}^*}^n \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}^*}^{-1} Y_{\mathcal{A}^*}^n$, where $\Sigma_{\mathcal{A}^*} \triangleq \text{diag}((\sigma_j^2)_{j\in\mathcal{A}^*})$. Finally, the trained decoder d_0 forms an estimate of V, $\hat{V}(\mathcal{A}^*) \triangleq d_0(\tilde{Y}_{\mathcal{A}^*}^n)$.

3) Information leakage: Consider ϕ and ψ with $n = 5$ and $r = 2$. Generate uniformly at random $M_{1:\gamma} \in \{0,1\}^\gamma$ and $B_{1:\gamma} \in \{0,1\}^{(r-k)\gamma}$. For $i \in [\gamma]$, generate

$$X_i^n \triangleq e_0(\phi(\lambda, M_i, B_i)), \tag{16}$$

such that the channel observations of the participants in $\mathcal{U}^*$ are $Y_{\mathcal{U}^*,i}^n \triangleq X_i^n + N_{\mathcal{U}^*,i}^n$. Using Lemma 1, there is no loss of generality in considering $\tilde{Y}_{\mathcal{U}^*,i}^n \triangleq \mathbf{1}_z^T \Sigma_{\mathcal{U}^*}^{-1} Y_{\mathcal{U}^*,i}^n$ instead of $Y_{\mathcal{U}^*,i}^n$. Finally, generate the secret as

$$S \triangleq \psi(\alpha, M_{1:\gamma}). \tag{17}$$

All possible combinations of λ and α are tested to minimize the leakage. The optimal seeds found are $\lambda = 11$, $\alpha = 10$ when $\gamma = 2$, $\alpha = 110$ when $\gamma = 3$, and $\alpha = 1110$ when $\gamma = 4$.

Then, to evaluate the leakage $I(S; \tilde{Y}_{\mathcal{U}^*,1:\gamma}^n)$, we use the mutual information estimator MINE from [12]. Specifically, we use a fully connected feed-forward neural network with 4 hidden layers, each having 400 neurons, and used rectified linear unit (ReLU) as an activation function. The input layer has $k+n$ neurons, and the Adam optimizer with a learning rate of 0.0001 is used for the training. The samples of the joint distribution $p_{S\tilde{Y}_{\mathcal{U}^*,1:\gamma}^n}$ are produced as described above. The samples of the marginal distributions are generated by dropping either s or $y_{\mathcal{U}^*,1:\gamma}^n$, from the joint samples $(s, y_{\mathcal{U}^*,1:\gamma}^n)$. We trained the neural network over 40000 epochs of $20,000$ messages with a batch size of 2500. Figure 2 shows the information leakage $I(S; \tilde{Y}_{\mathcal{U}^*,1:\gamma}^n)$ with respect to the secret sharing rate $R_s = \frac{k}{\gamma n}$ when z varies in [10].

4) Probability of error: To evaluate the probability of error between S and $\hat{S}(\mathcal{A}^*)$, generate uniformly at random $M_{1:\gamma} \in \{0,1\}^\gamma$ and $B_{1:\gamma} \in \{0,1\}^{(r-k)\gamma}$. Then, for $i \in [\gamma]$, generate the codeword X_i^n as in (16) so that the channel outputs at the participants in $\mathcal{A}^*$ are $Y_{\mathcal{A}^*,i}^n \triangleq X_i^n + N_{\mathcal{A}^*,i}^n$. Using Lemma 1, there is no loss of generality in considering $\tilde{Y}_{\mathcal{A}^*,i}^n \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}^*}^{-1} Y_{\mathcal{A}^*,i}^n$ instead of $Y_{\mathcal{A}^*,i}^n$. Finally, generate the secret S as in (17).

At the participants in $\mathcal{A}^*$, for $i \in [\gamma]$, M_i is estimated from $\tilde{Y}_{\mathcal{A}^*,i}^n$ as $\hat{M}_i \triangleq \psi(\lambda, d_0(\tilde{Y}_{\mathcal{A}^*,i}^n))$. Then, the secret is estimated as $\hat{S}(\mathcal{A}^*) \triangleq \psi(\alpha, \hat{M}_{1:\gamma})$. Figure 3 shows the average probability of error $\mathbb{P}[\hat{S}(\mathcal{A}^*) \neq S]$ with respect to the secret sharing rate $R_s = \frac{k}{\gamma n}$.

VI. Concluding remarks

We considered a secret sharing model where a dealer can communicate with participants over a Gaussian broadcast channel. We proposed a coding approach that consists in separating the code design into a secrecy layer and a reliability layer. Our first contribution was to show that, in the asymptotic blocklength regime, it is optimal to consider such two-layer coding schemes. Our second contribution was to design a two-layer coding scheme at finite blocklength, where we implemented the reliability layer with an autoencoder and the secrecy layer with two-universal hash functions. We empirically evaluated the probability of error and estimated the leakage for blocklength at most 20 with neural network-based mutual information estimator. Our simulation results demonstrated a precise control of the probability of error and leakage thanks to the two separate coding layers.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing Requirements Knowledge, Int. Workshop*, 1979, pp. 313–313.

[3] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. of Int. Conf. on Coding and Cryptology*, 2011, pp. 11–46.

[4] S. Zou, Y. Liang, L. Lai, and S. Shamai, "An information theoretic approach to secret sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, 2015.

[5] I. Csiszár and P. Narayan, "Capacity of a shared secret key," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2010, pp. 2593–2596.

[6] R. A. Chou, "Secret sharing over a public channel from correlated random variables," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2018, pp. 991–995.

[7] ——, "Distributed secret sharing over a public channel from correlated random variables," *arXiv preprint arXiv:2110.10307*, 2021.

[8] V. Rana, R. A. Chou, and H. Kwon, "Information-theoretic secret sharing from correlated Gaussian random variables and public communication." in *IEEE Trans. Inf. Theory*, vol. 68, no. 1, 2022, pp. 549–559.

[9] R. Sultana and R. A. Chou, "Low-complexity secret sharing schemes using correlated random variables and rate-limited public communication," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2021, pp. 970–975.

[10] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," *Electron. Commun. Jpn.*, vol. 69, no. 9, pp. 46–54, 1986.

[11] G. R. Blakley and C. Meadows, "Security of Ramp Schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, 1985, pp. 242–268.

[12] M. I. Belghazi, A. Baratin, S. Rajeswar, S. Ozair, Y. Bengio, A. Courville, and R. D. Hjelm, "MINE: Mutual information neural estimation," *arXiv preprint arXiv:1801.04062*, 2018.

[13] Y. Liang, G. Kramer, H. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, no. 142374, pp. 1–12, 2009.

[14] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Problems Inf. Transmission*, vol. 49, no. 1, pp. 73–98, 2013.

[15] A. D. Wyner, "The wire-tap channel," *The Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] R. A. Chou, "Explicit wiretap channel codes via source coding, universal hashing, and distribution approximation, when the channels' statistics are uncertain," *IEEE Trans. Inf. Forensics Security*, 2022.

[17] V. Rana and R. A. Chou, "Short blocklength wiretap channel codes via deep learning: Design and performance evaluation," *IEEE Transactions on Communications*, vol. 71, no. 3, pp. 1462–1474, 2023.

[18] A. Nooraiepour and T. M. Duman, "Randomized convolutional codes for the wiretap channel," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3442–3452, 2017.

[19] ——, "Randomized turbo codes for the wiretap channel," in *IEEE Global Commun. Conf.*, 2017, pp. 1–6.

[20] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

[21] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *IEEE Inf. Theory Workshop*, 2010, pp. 1–5.

[22] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forensics and Security*, vol. 9, no. 11, pp. 1765–1779, 2014.

[23] W. K. Harrison, E. Beard, S. Dye, E. Holmes, K. Nelson, M. A. Gomes, and J. P. Vilela, "Implications of coding layers on physical-layer security: A secrecy benefit approach," *Entropy*, vol. 21, no. 8, p. 755, 2019.

[24] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for channel coding via neural mutual information estimation," in *IEEE Int. Workshop on Signal Processing Advances Wirel. Commun.*, 2019, pp. 1–5.

[25] ——, "Deep learning based wiretap coding via mutual information estimation," in *Proc. of ACM Workshop on Wireless Security and Machine Learning*, 2020, pp. 74–79.

[26] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2010, pp. 2538–2542.

[27] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Annual Cryptology Conf. Springer*, 2012, pp. 294–311.

[28] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2014, pp. 956–960.

[29] K.-L. Besser, P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap code design by neural network autoencoders," *IEEE Trans. Inf. Forensics and Security*, vol. 15, pp. 3374–3386, 2019.

[30] V. Rana and R. A. Chou, "Design of short blocklength wiretap channel codes: Deep learning and cryptography working hand in hand," in *IEEE Inf. Theory Workshop*, 2021, pp. 1–6.

[31] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2005, pp. 2152–2155.

[32] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[33] T. O'shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. on Cognitive Commun. Networking*, vol. 3, no. 4, pp. 563–575, 2017.

[34] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.