MULTI-USER INFORMATION THEORETIC SECURITY FOR WIRELESS COMMUNICATION

A Dissertation by

Rumia Sultana

Master of Science, Wichita State University, 2018

Bachelor of Science, North South University, 2013

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

July 2023

MULTI-USER INFORMATION THEORETIC SECURITY FOR WIRELESS COMMUNICATION

The following faculty members have examined the final copy of this dissertation for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Doctor of Philosophy, with a major in Electrical Engineering and Computer Science.

Remi Chou, Committee Chair

Gamal Weheba, Committee Member

Abu Asaduzzaman, Committee Member

Ajita Rattani, Committee Member

Edwin Sawan, Committee Member

Accepted for the College of Engineering

Anthony Muscat, Dean

Accepted for the Graduate School

Coleen Pugh, Dean

DEDICATION

I dedicate this thesis to my family, friends, and colleagues in the Avengers, Defenders, and Illuminati.

"Do not lose hope, nor be sad." Qur'an 3:139

ACKNOWLEDGEMENTS

Special thanks to Dr. Remi Chou for his constant input and guidance in all of this work. I would also like to thank my wonderful parents, lovely husband, and sweetest sister for their steadfast devotion and inspiration.

ABSTRACT

We show that the problem of code construction for multiple access channel (MAC) resolvability can be reduced to the simpler problem of code construction for source resolvability. Specifically, we propose a MAC resolvability code construction which involves a combination of multiple source resolvability codes, used in a black-box manner, and leverages randomness recycling implemented via distributed hashing and block-Markov coding.

We consider secret sharing where a dealer wants to share a secret with several participants such that predefined subsets of participants can reconstruct the secret and all other subsets of participants cannot learn any information about the secret. To this end, the dealer and the participants have access to samples of correlated random variables and a one-way (from the dealer to the participants), authenticated, public, and rate-limited communication channel. For this problem, we propose the first constructive and low-complexity coding scheme able to handle arbitrary access structures. Our construction relies on a vector quantization coupled with distribution approximations with polar codes to handle the reliability constraints, followed by universal hashing to handle the security constraints. We stress that our coding scheme does not require symmetry or degradation assumptions on the correlated random variables, and does not need a pre-shared secret among the participants and dealer.

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.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Information-theoretic security assures that the security cannot be broken even if the adversary had unlimited computing power. In short, information-theoretic security means no assumption is made on the computational power of the opponent. From the wireless communication perspective, information-theoretic security provides physical layer security by exploiting the noisy resources of the channel.

Secret sharing is motivated by the need to distribute sensitive information among multiple parties while maintaining confidentiality and ensuring that the information can only be accessed by authorized subsets of those parties. Here are some key motivations behind secret sharing:

- Privacy and Confidentiality: Secret sharing allows sensitive information to be protected and kept confidential. By dividing the secret into shares and distributing them among different parties, no single party possesses the complete information. This ensures that even if one or several shares are compromised, the original secret remains secure.

- Security against Single Point of Failure: Secret sharing mitigates the risk associated with a single point of failure. If a single entity or party holds the entire secret and becomes compromised, the security of the secret is compromised as well. With secret sharing, the information is distributed across multiple parties, reducing the risk of a single party compromising the entire secret.

- Access Control and Authorization: Secret sharing enables access control mechanisms. By distributing shares to different parties, secret sharing schemes can be designed such that only authorized subsets of parties can reconstruct the original secret. This allows for fine-grained control over who can access the secret and ensures that unauthorized parties cannot gain access.

- Resilience and Fault Tolerance: Secret sharing provides resilience and fault tolerance. If one or more parties are unavailable or compromised, the secret can still be reconstructed as long as the required threshold of authorized parties is present. This makes secret sharing particularly useful in scenarios where system failures, natural disasters, or other disruptions can occur.

- Trust and Collaboration: Secret sharing encourages trust and collaboration among multiple parties. By distributing the secret among different entities, it promotes cooperation and eliminates the need for complete trust in a single party. This is particularly relevant in multi-party scenarios such as secure multi-party computation and secure data sharing.

Overall, secret sharing addresses the fundamental challenge of securely distributing sensitive information among multiple parties, ensuring privacy, security, access control, and resilience. It provides a foundation for various cryptographic protocols and applications where confidentiality and integrity of shared information are critical.

The brief introductions of the topics discussed in this dissertation are:

- Topic I: The concept of multiple access channel (MAC) resolvability has been introduced in [1] as a natural extension of channel resolvability for point-to-point channels [2].

- Topic II: Secret sharing has been introduced in [3] and [4]. Basic secret sharing models consist of a dealer that distributes a secret among a set of participants with the constraint 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.

- Topic III: Same secret sharing model as in [5] where noisy resources, in the form of a Gaussian channel, are available between the dealer and participants.

CHAPTER II

Multiple Access Channel Resolvability Codes from Source Resolvability Codes

We published two conference papers [6], [7], and one peer-reviewed journal paper [8].

2.1 Introduction

The concept of multiple access channel (MAC) resolvability has been introduced in [1] as a natural extension of channel resolvability for point-to-point channels [2]. MAC resolvability represents a fundamental primitive that finds applications in a large variety of network information-theoretic problems, including strong secrecy for multiple access wiretap channels [9, 10], cooperative jamming [9], semantic security for multiple access wiretap channels [11], and strong coordination in networks [12]. These applications are, however, restricted by the fact that no explicit coding scheme is known to optimally implement MAC resolvability. Note indeed that [1, 11] only provide existence results and no explicit code constructions. The objective of this work is to bridge this gap by providing explicit coding schemes that achieve the MAC resolvability region [11]. While previous works have been successful in providing explicit coding schemes for channel resolvability over point-to-point channels,[1] to the best of our knowledge, the only known explicit constructions for MAC resolvability are those of [17]. However, the explicit constructions in [17], one based on invertible extractors and a second one based on injective group homomorphisms, are limited to *symmetric* multiple access channels, and do not seem to generalize to *arbitrary* multiple access channels.

Here, we propose a novel approach to the construction of MAC resolvability codes

[1] Explicit constructions based on polar codes for channel resolvability have been proposed for binary *symmetric* point-to-point channels [13] and discrete memoryless point-to-point channels whose input alphabets have prime cardinalities [14]. Another explicit construction based on injective group homomorphisms has been proposed in [15] for channel resolvability over binary *symmetric* point-to-point channels. Low-complexity, but non-explicit, linear coding schemes for channel resolvability over arbitrary memoryless point-to-point channels have also been proposed in [16].

by showing that such a construction can be reduced to the simpler problem of code construction for source resolvability [18]. Since explicit constructions of source resolvability codes are known, e.g., [14], our results yield the first explicit construction of MAC resolvability codes that achieve the entire MAC resolvability region of arbitrary multiple access channels with binary input alphabets. More specifically, our approach to the construction of MAC resolvability codes relies on a combination of appropriately chosen source resolvability codes, and leverages randomness recycling implemented with distributed hashing and a block-Markov encoding scheme. In essence, the idea of block-Markov encoding to recycle randomness is closely related to recursive constructions of seeded extractors in the computer science literature, e.g., [19]. We stress that our construction is valid independently from the way those source resolvability codes are implemented. Additionally, to avoid time-sharing whenever it is known to be unnecessary, we also show how to implement the idea of rate splitting, first developed in [20] for multiple access channel coding, for the MAC resolvability problem with two transmitters. Note that the main difference with [17], is that our approach aims to reduce the construction of MAC resolvability codes to a simpler problem, namely the construction of source resolvability codes, whereas [17] attempts a code construction directly adapted to multiple access channels.

2.2 Problem Statement and Review of Source Resolvability

2.2.1 Notation

For $a, b \in \mathbb{R}$, define $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. The components of a vector $X^{1:N}$ of size N are denoted with superscripts, i.e., $X^{1:N} \triangleq (X^1, X^2, \ldots, X^N)$. For two probability distributions p and q defined over the same alphabet $\mathcal{X}$, the variational distance $\mathbb{V}(p, q)$ between p and q is defined as $\mathbb{V}(p, q) \triangleq \sum_{x \in \mathcal{X}} |p(x) - q(x)|$.

2.2.2 Problem Statement

Consider a discrete memoryless multiple access channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$, where $\mathcal{X} = \{0, 1\} = \mathcal{Y}$, and $\mathcal{Z}$ is a finite alphabet. A target distribution q_Z is defined as the channel output distribution when the input distributions are q_X and q_Y, i.e.,

$$\forall z \in \mathcal{Z}, q_Z(z) \triangleq \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} q_{Z|XY}(z|x, y) q_X(x) q_Y(y). \tag{1}$$

Definition 1. *A $(2^{NR_1}, 2^{NR_2}, N)$ code for the memoryless multiple access channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$ consists of*

- *Two randomization sequences S_1 and S_2 independent and uniformly distributed over $\mathcal{S}_1 \triangleq [\![1, 2^{NR_1}]\!]$ and $\mathcal{S}_2 \triangleq [\![1, 2^{NR_2}]\!]$, respectively;*
- *Two encoding functions $f_{1,N} : \mathcal{S}_1 \to \mathcal{X}^N$ and $f_{2,N} : \mathcal{S}_2 \to \mathcal{Y}^N$;*

and operates as follows: Transmitters 1 and 2 form $f_{1,N}(S_1)$ and $f_{2,N}(S_2)$, respectively, which are sent over the channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$.

Definition 2. *(R_1, R_2) is an achievable resolvability rate pair for the memoryless multiple access channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$ if there exists a sequence of $(2^{NR_1}, 2^{NR_2}, N)$ codes such that*

$$\lim_{N \to +\infty} \mathbb{V}(\widetilde{p}_{Z^{1:N}}, q_{Z^{1:N}}) = 0,$$

where $q_{Z^{1:N}} \triangleq \prod_{i=1}^{N} q_Z$ with q_Z defined in (1) and $\forall z^{1:N} \in \mathcal{Z}^N$,

$$\widetilde{p}_{Z^{1:N}}(z^{1:N}) \triangleq \sum_{(s_1, s_2) \in \mathcal{S}_1 \times \mathcal{S}_2} \frac{q_{Z^{1:N}|X^{1:N}Y^{1:N}}\left(z^{1:N} | f_{1,N}(s_1), f_{2,N}(s_2)\right)}{|\mathcal{S}_1||\mathcal{S}_2|}.$$

The multiple access channel resolvability region $\mathcal{R}_{q_Z}$ is defined as the closure of the set of all achievable rate pairs.

Theorem 1 ([11, Theorem 1])**.** *We have $\mathcal{R}_{q_Z} = \mathcal{R}'_{q_Z}$ with*

$$\mathcal{R}'_{q_Z} \triangleq \bigcup_{p_T, q_{X|T}, q_{Y|T}} \{(R_1, R_2) : I(XY; Z|T) \leq R_1 + R_2,$$

$$I(X;Z|T) \leq R_1,$$
$$I(Y;Z|T) \leq R_2\},$$

where p_T *is defined over* $\mathcal{T} \triangleq [\![1, |\mathcal{Z}| + 3]\!]$ *and* $q_{X|T}, q_{Y|T}$ *are such that, for any* $t \in \mathcal{T}$ *and* $z \in \mathcal{Z}$,

$$q_Z(z) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} q_{X|T}(x|t) q_{Y|T}(y|t) q_{Z|XY}(z|x,y).$$

Note that reference [11] provides only the existence of a coding scheme that achieves any rate pair in $\mathcal{R}_{q_Z}$. By contrast, *our goal is to provide explicit coding schemes that can achieve the region* $\mathcal{R}_{q_Z}$ by relying on source resolvability codes, which are used in a black box manner. The notion of source resolvability is reviewed next.

2.2.3 Review of Source Resolvability

Definition 3. *A* $(2^{NR}, N)$ *source resolvability code for* $(\mathcal{X}, q_X)$ *consists of*

- *A randomization sequence* S *uniformly distributed over* $\mathcal{S} \triangleq [\![1, 2^{NR}]\!]$*;*
- *An encoding function* $e_N : \mathcal{S} \to \mathcal{X}^N$*;*

and operates as follows: The encoder forms $\widetilde{X}^{1:N} \triangleq e_N(S)$ *and the distribution of* $\widetilde{X}^{1:N}$ *is denoted by* $\widetilde{p}_{X^{1:N}}$.

Definition 4. R *is an achievable resolution rate for a discrete memoryless source* $(\mathcal{X}, q_X)$ *if there exists a sequence of* $(2^{NR}, N)$ *source resolvability codes such that*

$$\lim_{N \to +\infty} \mathbb{V}(\widetilde{p}_{X^{1:N}}, q_{X^{1:N}}) = 0, \tag{2}$$

where $q_{X^{1:N}} \triangleq \prod_{i=1}^{N} q_X$. *The infimum of such achievable rates is called source resolvability.*

Theorem 2 ([2])**.** *The source resolvability of a discrete memoryless source* $(\mathcal{X}, q_X)$ *is* $H(X)$.

Note that explicit low-complexity source resolvability codes can, for instance, be obtained with polar codes as reviewed in Appendix 2.9.

2.3 Main result

Our main result is summarized as follows.

Theorem 3. *The coding scheme presented in Section 2.4, which solely relies on source resolvability codes, used as black boxes, and two-universal hash functions [21], achieves the entire multiple access channel resolvability region $\mathcal{R}_{qZ}$ for any discrete memoryless multiple access channel with binary input alphabets. Moreover, time-sharing is avoided whenever it is known to be unnecessary.*

As a corollary, we obtain the first explicit construction of multiple access channel resolvability codes that achieve the entire multiple access channel resolvability region $\mathcal{R}_{qZ}$ for any discrete memoryless multiple access channel with binary input alphabets.

Corollary 1. *Since explicit constructions for source resolvability codes and two-universal hash functions are known, e.g., [21, 22], Theorem 3 yields an explicit coding scheme that achieves $\mathcal{R}_{qZ}$ for any discrete memoryless multiple access channel with binary input alphabets.*

2.4 Coding Scheme

We explain in Section 2.5 that the general construction of MAC resolvability codes can be reduced to two special cases. Then, we provide a coding scheme for these two special cases in Sections 2.5.1, 2.6.

2.5 Reduction of the general construction of MAC resolvability codes to two special cases

Definition 5. *For the memoryless multiple access channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$ we define*

$$\mathcal{R}_{X,Y} \triangleq \{(R_1, R_2) : I(XY; Z) \leq R_1 + R_2,$$

$$I(X;Z) \leq R_1,$$
$$I(Y;Z) \leq R_2\},$$

for some product distribution $p_X p_Y$ *on* $\mathcal{X} \times \mathcal{Y}$.

To show the achievability of $\mathcal{R}'_{q_Z}$, it is sufficient to show the achievability of $\mathcal{R}_{X,Y}$. Indeed, note that if $\mathcal{R}_{X,Y}$ is achievable, then $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y})$ is also achievable, where Conv denotes the convex hull. Hence, $\mathcal{R}'_{q_Z}$ is achievable because $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y}) \supset \mathcal{R}'_{q_Z}$ by remarking that the corner points of $\mathcal{R}'_{q_Z}$ are in $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y})$. For instance, the point $(I(X;Z|T), I(Y;Z|XT)) \in \mathcal{R}'_{q_Z}$ belongs to $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y})$ since

$$\begin{aligned}&(I(X;Z|T), I(Y;Z|XT))\\ &= \sum_{t \in \mathcal{T}} p_T(t)(I(X;Z|T=t), I(Y;Z|X,T=t)).\end{aligned}$$

Similarly, all the corner points of $\mathcal{R}'_{q_Z}$ also belong to $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y})$. Next, we consider two cases to achieve the region $\mathcal{R}_{X,Y}$ for some fixed distribution $p_X p_Y$.

- Case 1 (depicted in Figure 1): $I(XY;Z) > I(X;Z) + I(Y;Z)$. In this case, it is sufficient to achieve the dominant face $\mathcal{D}$ of $\mathcal{R}_{X,Y}$, where

$$\begin{aligned}\mathcal{D} \triangleq \{(R_1, R_2) : R_1 \in &[I(X;Z), I(X;Z|Y)],\\ &R_2 = I(XY;Z) - R_1\}.\end{aligned}$$

- Case 2 (depicted in Figure 2): $I(XY;Z) = I(X;Z) + I(Y;Z)$. In this case, only the corner point C needs to be achieved. Note that it is impossible to have $I(XY;Z) < I(X;Z) + I(Y;Z)$ by independence of X and Y.

2.5.1 Encoding Scheme for Case 1

Consider the region $\mathcal{R}_{X,Y}$ for some product distribution $p_X p_Y$ on $\mathcal{X} \times \mathcal{Y}$ such that $I(XY;Z) > I(X;Z) + I(Y;Z)$. Since $\mathcal{R}_{X,Y}$ is a contrapolymatroid [23], to achieve the

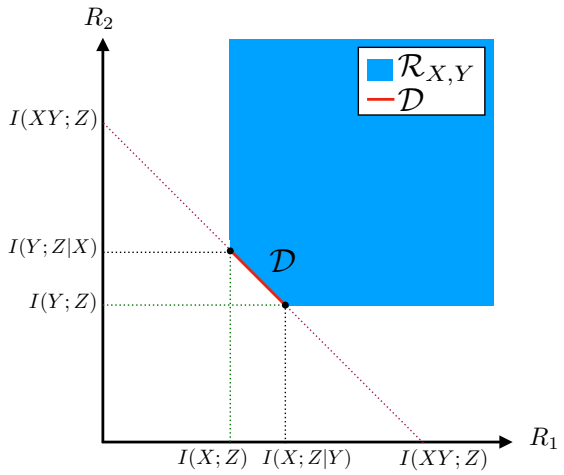


Figure 1: Region $\mathcal{R}_{X,Y}$ in Case 1: $I(XY;Z) > I(X;Z) + I(Y;Z)$.

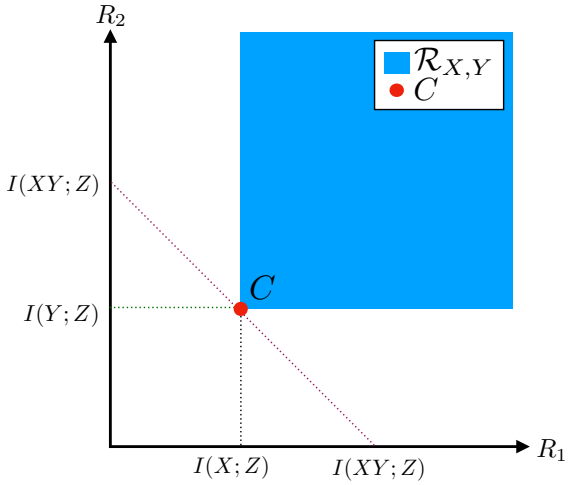


Figure 2: Region $\mathcal{R}_{X,Y}$ in Case 2: $I(XY;Z) = I(X;Z) + I(Y;Z)$.

region $\mathcal{R}_{X,Y}$, it is sufficient to achieve any rate pair (R_1, R_2) of the dominant face $\mathcal{D}$ of $\mathcal{R}_{X,Y}$. We next show that $\mathcal{D}$ can be achieved through rate-splitting using the following lemma proved in Appendix 2.9.

Lemma 1. *Consider* $f : \mathcal{Y} \times \mathcal{Y} \to \mathcal{Y}$, $(u, v) \mapsto \max(u, v)$, *and form* $(\mathcal{Y} \times \mathcal{Y}, p_{U_\epsilon} p_{V_\epsilon}), \epsilon \in [0, 1]$, *such that* $p_{U_\epsilon V_\epsilon} = p_{U_\epsilon} p_{V_\epsilon}$, $p_{f(U_\epsilon, V_\epsilon)} = p_Y$, *for fixed* $(y, u), p_{f(U_\epsilon, V_\epsilon)|U_\epsilon}(y|u)$ *is a continuous function of* ϵ, *and*

$$U_{\epsilon=0} = 0 = V_{\epsilon=1}, \tag{3}$$

$$U_{\epsilon=1} = f(U_{\epsilon=1}, V_{\epsilon=1}), \tag{4}$$

$$V_{\epsilon=0} = f(U_{\epsilon=0}, V_{\epsilon=0}). \tag{5}$$

The above construction is indeed possible as shown in [20, Example 3]. Then, we have $I(XY;Z) = R_1 + R_U + R_V$, *where we have defined the functions*

$$R_1 : [0, 1] \to \mathbb{R}^+, \epsilon \mapsto I(X; Z|U_\epsilon),$$

$$R_U : [0, 1] \to \mathbb{R}^+, \epsilon \mapsto I(U_\epsilon; Z),$$

$$R_V : [0, 1] \to \mathbb{R}^+, \epsilon \mapsto I(V_\epsilon; Z|U_\epsilon X).$$

Moreover, R_1 is continuous with respect to ϵ and $[I(X;Z), I(X;Z|Y)]$ is contained in its image.

When the context is clear, we do not explicitly write the dependence of U and V with respect to ϵ by dropping the subscript ϵ.

Fix a point (R_1, R_2) in $\mathcal{D}$. By Lemma 1, there exists a joint probability distribution q_{UVXYZ} over $\mathcal{Y} \times \mathcal{Y} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ such that $R_1 = I(X;Z|U)$, $R_2 = R_U + R_V$ with $R_U = I(U;Z)$ and $R_V = I(V;Z|UX)$. We provide next a coding scheme that will be shown to achieve the point (R_1, R_2). The encoding scheme operates over $k \in \mathbb{N}$ blocks of length N and is described in Algorithms 1 and 2. A high level description of the encoding scheme is as follows. For the first transmitter, we perform source resolvability for the discrete memoryless source $(\mathcal{X}, q_X)$ using randomness with rate $H(X)$ in Block 1. Using Lemma 1, we perform rate splitting for the second transmitter to get two virtual users such that one virtual user is associated with the discrete memoryless source $(\mathcal{Y}, q_U)$ and the other virtual user is associated with the discrete memoryless source $(\mathcal{Y}, q_V)$. Then, we perform source resolvability with rates $H(U)$ and $H(V)$ for the discrete memoryless sources$(\mathcal{Y}, q_U)$ and $(\mathcal{Y}, q_V)$, respectively. For the next encoding blocks, we proceed as in Block 1 using source resolvability and rate splitting except that part of the randomness is now recycled from the previous block. More precisely, we recycle the bits of randomness used at the inputs of the channel in the previous block that are almost independent from the channel output. The rates of those bits will be shown to approach $H(X|UZ)$, $H(U|Z)$, $H(V|UZX)$ for User 1 and the two virtual users, respectively.

- The encoding at Transmitter 1 is described in Algorithm 1 and uses
  - A hash function $G_X : \{0,1\}^N \longrightarrow \{0,1\}^{r_X}$ chosen uniformly at random in a family of two-universal hash functions, where the output length of the hash function G_X is defined as follows

$$r_X \triangleq N(H(X|UZ) - \epsilon_1/2), \tag{6}$$

where $\epsilon_1 \triangleq 2(\delta_{\mathcal{A}}(N)+\xi)$, $\delta_{\mathcal{A}}(N) \triangleq \log(|\mathcal{Y}|^2|\mathcal{X}|+3)\sqrt{\frac{2}{N}(3+\log N)}$, $\xi > 0$.

- A source resolvability code for the discrete memoryless source $(\mathcal{X}, q_X)$ with encoder function e_N^X and rate $H(X)+\frac{\epsilon_1}{2}$, such that the distribution of the encoder output $\widetilde{p}_{X^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{X^{1:N}}, q_{X^{1:N}}) \leq \delta(N)$, where $\delta(N)$ is such that $\lim_{N\to+\infty}\delta(N)=0$.

In Algorithm 1, the hash function output $\widetilde{E}_i$, $i \in [\![2,k]\!]$, with length r_X corresponds to recycled randomness from Block $i-1$.

- The encoding at Transmitter 2 is described in Algorithm 2 and uses
  - Two hash functions $G_U : \{0,1\}^N \longrightarrow \{0,1\}^{r_U}$ and $G_V : \{0,1\}^N \longrightarrow \{0,1\}^{r_V}$ chosen uniformly at random in families of two-universal hash functions, where the output lengths of the hash functions G_U and G_V are defined as follows

$$\begin{aligned} r_U &\triangleq N(H(U|Z)-\epsilon_1/2), \\ r_V &\triangleq N(H(V|UZX)-\epsilon_1/2). \end{aligned} \tag{7}$$

  - A source resolvability code for the discrete memoryless source $(\mathcal{U}, q_U)$ with encoding function e_N^U and rate $H(U)+\frac{\epsilon_1}{2}$, such that the distribution of the encoder output $\widetilde{p}_{U^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{U^{1:N}}, q_{U^{1:N}}) \leq \delta(N)$, where $\delta(N)$ is such that $\lim_{N\to+\infty}\delta(N)=0$.
  - A source resolvability code for the discrete memoryless source $(\mathcal{V}, q_V)$ with encoding function e_N^V and rate $H(V)+\frac{\epsilon_1}{2}$, such that the distribution of the encoder output $\widetilde{p}_{V^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{V^{1:N}}, q_{V^{1:N}}) \leq \delta(N)$, where $\delta(N)$ is such that $\lim_{N\to+\infty}\delta(N)=0$.

In Algorithm 2, the hash function outputs $\widetilde{D}_i$ and $\widetilde{F}_i$, $i \in [\![2,k]\!]$, with lengths r_U and r_V, respectively, correspond to recycled randomness from Block $i-1$.

The dependencies between the random variables involved in Algorithms 1 and 2 are represented in Figure 3.

Algorithm 1 Encoding algorithm at Transmitter 1 in Case 1

Require: A vector E_1 of $N(H(X)+\epsilon_1)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, a vector E_i of $N(I(X;UZ)+\epsilon_1)$ uniformly distributed bits.

1: **for** Block $i=1$ to k **do**
2: **if** $i=1$ **then**
3: Define $\widetilde{X}_1^{1:N} \triangleq e_N^X(E_1)$
4: **else if** $i>1$ **then**
5: Define $\widetilde{E}_i \triangleq G_X(\widetilde{X}_{i-1}^{1:N})$
6: Define $\widetilde{X}_i^{1:N} \triangleq e_N^X(\widetilde{E}_i \| E_i)$, where $\|$ denotes concatenation
7: **end if**
8: Send $\widetilde{X}_i^{1:N}$ over the channel
9: **end for**

Algorithm 2 Encoding algorithm at Transmitter 2 in Case 1

Require: A vector D_1 of $N(H(U)+\epsilon_1)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, a vector D_i of $N(I(U;Z)+\epsilon_1)$ uniformly distributed bits. A vector F_1 of $N(H(V)+\epsilon_1)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, a vector F_i of $N(I(V;UZX)+\epsilon_1)$ uniformly distributed bits.

1: **for** Block $i=1$ to k **do**
2: **if** $i=1$ **then**
3: Define $\widetilde{U}_1^{1:N} \triangleq e_N^U(D_1)$ and $\widetilde{V}_1^{1:N} \triangleq e_N^V(F_1)$
4: **else if** $i>1$ **then**
5: Define $\widetilde{D}_i \triangleq G_U(\widetilde{U}_{i-1}^{1:N})$ and $\widetilde{F}_i \triangleq G_V(\widetilde{V}_{i-1}^{1:N})$
6: Define $\widetilde{U}_i^{1:N} \triangleq e_N^U(\widetilde{D}_i \| D_i)$ and $\widetilde{V}_i^{1:N} \triangleq e_N^V(\widetilde{F}_i \| F_i)$
7: Define $\widetilde{Y}_i^{1:N} \triangleq f(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$, where f is defined in Lemma 18
8: **end if**
9: Send $\widetilde{Y}_i^{1:N}$ over the channel
10: **end for**

2.6 Encoding Scheme for Case 2

The encoding scheme for Case 2 is same as the encoding for Case 1 with the substitutions $U \leftarrow \emptyset$ and $V \leftarrow Y$.

2.7 Coding Scheme Analysis

2.7.1 Coding Scheme Analysis for Case 1

First, we show that in each encoding Block $i \in [\![1,k]\!]$, the random variables $\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, \widetilde{X}_i^{1:N}, \widetilde{Y}_i^{1:N}, \widetilde{Z}_i^{1:N}$ induced by the coding scheme approximate well the target distribution $q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}$. Then, we show that the target output distribution $q_{Z^{1:kN}}$ is well approximated jointly over all blocks. To do so, we show that the recycled randomness $\widetilde{E}_i, \widetilde{D}_i, \widetilde{F}_i$ in Block $i \in [\![2,k]\!]$ that appears in Line 5 of Algorithms 1 and 2 is

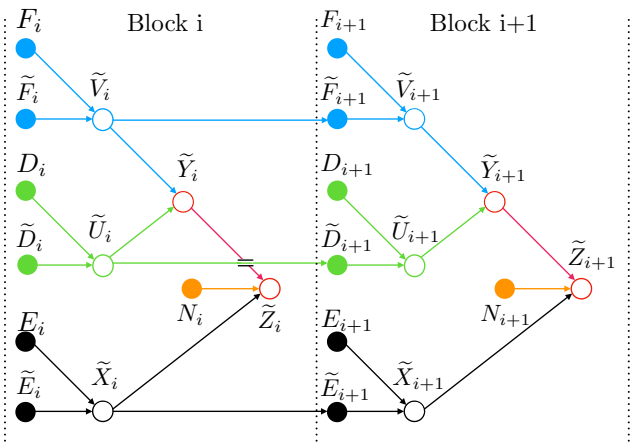


Figure 3: Dependence graph for the random variables involved in the encoding for Case 1. N_i, $i \in [\![1,k]\!]$, is the channel noise corresponding to the transmission over Block i. For Block $i \in [\![2,k]\!]$, $(D_i, \widetilde{D}_i)$, $(F_i, \widetilde{F}_i)$, $(E_i, \widetilde{E}_i)$ are the random sequences used at the encoders to form $\widetilde{U}_i^{1:N}$, $\widetilde{V}_i^{1:N}$, $\widetilde{X}_i^{1:N}$, respectively.

almost independent of the channel output in Block $i-1$. Note that randomness recycling is studied via a distributed version of the leftover hash lemma stated in Lemma 17. Finally, we prove that the encoding scheme of Section 2.5.1 achieves the desired rate-tuple. For convenience, define $\widetilde{E}_1 \triangleq \emptyset$, $\widetilde{D}_1 \triangleq \emptyset$, and $\widetilde{F}_1 \triangleq \emptyset$. Let

$$\widetilde{p}_{E_i D_i F_i X_i^{1:N} U_i^{1:N} V_i^{1:N} Y_i^{1:N} Z_i^{1:N}} \tag{8}$$

denote the joint probability distribution of the random variables $\widetilde{E}_i, \widetilde{D}_i, \widetilde{F}_i, \widetilde{X}_i^{1:N}, \widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, \widetilde{Y}_i^{1:N}$, and $\widetilde{Z}_i^{1:N}$ created in Block $i \in [\![1,k]\!]$ of the coding scheme of Section 2.5.1.

We first prove in the following lemma that in Block $i \in [\![2,k]\!]$, if the inputs $\widetilde{X}_{i-1}^{1:N}$, $\widetilde{U}_{i-1}^{1:N}$, $\widetilde{V}_{i-1}^{1:N}$ of the hash functions G_X, G_U, G_V, respectively, are replaced by $X^{1:N}$, $U^{1:N}$, $V^{1:N}$ distributed according to $q_{X^{1:N}U^{1:N}V^{1:N}} \triangleq \prod_{i=1}^N q_{XUV}$, then the output of these hash functions are almost jointly uniformly distributed.

Lemma 2. *Let $p_{\bar{E}}^{unif}, p_{\bar{D}}^{unif}, p_{\bar{F}}^{unif}$ denote the uniform distributions over $\{0,1\}^{r_X}$, $\{0,1\}^{r_U}$, $\{0,1\}^{r_V}$, respectively. Then,*

$$\mathbb{V}\left(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})Z^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}}\right)$$

$$\leq \delta^{(0)}(N),$$

where $\delta^{(0)}(N) \triangleq 2/N + \sqrt{7} \cdot 2^{-\frac{N\xi}{2}}$.

Proof. Define $\mathcal{A} \triangleq \{U, V, X\}$ and, for any $\mathcal{S} \subseteq \mathcal{A}$, define $T_{\mathcal{S}} \triangleq (W)_{W \in \mathcal{S}}$. Hence, we have

$$T_{\mathcal{A}}^{1:N} = (X^{1:N}, U^{1:N}, V^{1:N}),$$
$$q_{T_{\mathcal{A}}^{1:N} Z^{1:N}} = q_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}.$$

Then, by Lemma 16 in Appendix 2.9, applied to the product distribution $q_{T_{\mathcal{A}}^{1:N} Z^{1:N}}$, there exists a subnormalized non-negative function $w_{T_{\mathcal{A}}^{1:N} Z^{1:N}}$ such that, for any $\mathcal{S} \subseteq \mathcal{A}$,

$$\mathbb{V}(w_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}, q_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}) \leq 1/N, \tag{9}$$
$$H_\infty(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}}) \geq N H(T_{\mathcal{S}}|Z) - N\delta_{\mathcal{S}}(N), \tag{10}$$

where the min-entropy $H_\infty(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}})$ is defined in Lemma 16 in Appendix 2.9, and $\delta_{\mathcal{S}}(N) \triangleq \log(|\mathcal{T}_{\mathcal{S}}| + 3)\sqrt{\frac{2}{N}(3 + \log N)}$ with $\mathcal{T}_{\mathcal{S}}$ is the domain over which $T_{\mathcal{S}}$ is defined. Next, let q_{EDF} define the joint distribution of

$$E \triangleq G_X(X^{1:N}), D \triangleq G_U(U^{1:N}), F \triangleq G_V(V^{1:N}), \tag{11}$$

where $U^{1:N}$, $V^{1:N}$, and $X^{1:N}$ are distributed according to $q_{U^{1:N} V^{1:N} X^{1:N}}$. Then, we have

$$\begin{aligned}
&\mathbb{V}(q_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}}) \\
&\overset{(a)}{\leq} \mathbb{V}(q_{EDFZ^{1:N}}, w_{EDFZ^{1:N}}) \\
&\quad + \mathbb{V}(w_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}}) \\
&\overset{(b)}{=} \mathbb{V}(q_{G_X(X^{1:N}) G_U(U^{1:N}) G_V(V^{1:N}) Z^{1:N}}, \\
&\qquad w_{G_X(X^{1:N}) G_U(U^{1:N}) G_V(V^{1:N}) Z^{1:N}}) \\
&\quad + \mathbb{V}(w_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}})
\end{aligned}$$

$$
\begin{aligned}
&\overset{(c)}{\leq} \mathbb{V}(q_{X^{1:N}U^{1:N}V^{1:N}Z^{1:N}}, w_{X^{1:N}U^{1:N}V^{1:N}Z^{1:N}}) \\
&\quad + \mathbb{V}(w_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}}) \\
&\overset{(d)}{\leq} 1/N + \mathbb{V}(w_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} w_{Z^{1:N}}) \\
&\quad + \mathbb{V}(p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} w_{Z^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} q_{Z^{1:N}}) \\
&\overset{(e)}{\leq} 2/N + \mathbb{V}(w_{EDFZ^{1:N}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif} w_{Z^{1:N}}) \\
&\overset{(f)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{A},\mathcal{S}\neq\emptyset} 2^{r_{\mathcal{S}} - H_\infty(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}})}} \\
&\overset{(g)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{A},\mathcal{S}\neq\emptyset} 2^{r_{\mathcal{S}} - NH(T_{\mathcal{S}}|Z) + N\delta_{\mathcal{S}}(N)}} \\
&\overset{(h)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{A},\mathcal{S}\neq\emptyset} 2^{r_{\mathcal{S}} - NH(T_{\mathcal{S}}|Z) + N\delta_{\mathcal{A}}(N)}}
\end{aligned}
$$

where (a) holds by the triangle inequality, (b) holds by (11), (c) holds by the data processing inequality, (d) holds by (9) and the triangle inequality, (e) holds by (9), (f) holds by Lemma 17 in Appendix 2.9 and $r_{\mathcal{S}} \triangleq \sum_{i\in\mathcal{S}} r_i$ similar to the notation of Lemma 17, (g) holds by (10), (h) holds because for any $\mathcal{S} \subseteq \mathcal{A}$, $\delta_{\mathcal{S}}(N) \leq \delta_{\mathcal{A}}(N)$. Next, we have

$$
\begin{aligned}
&\sqrt{\sum_{\mathcal{S}\subseteq\mathcal{A},\mathcal{S}\neq\emptyset} 2^{r_{\mathcal{S}} - NH(T_{\mathcal{S}}|Z) + N\delta_{\mathcal{A}}(N)}} \\
&\overset{(a)}{=} \Big(2^{N(H(X|UZ)-\frac{\epsilon_1}{2}) - NH(X|Z)} \\
&\quad + 2^{N(H(U|Z)-\frac{\epsilon_1}{2}) - NH(U|Z)} \\
&\quad + 2^{N(H(V|UZX)-\frac{\epsilon_1}{2}) - NH(V|Z)} \\
&\quad + 2^{N(H(X|UZ)-\frac{\epsilon_1}{2}) + N(H(U|Z)-\frac{\epsilon_1}{2}) - NH(XU|Z)} \\
&\quad + 2^{N(H(U|Z)-\frac{\epsilon_1}{2}) + N(H(V|UZX)-\frac{\epsilon_1}{2}) - NH(UV|Z)} \\
&\quad + 2^{N(H(V|UZX)-\frac{\epsilon_1}{2}) + N(H(X|UZ)-\frac{\epsilon_1}{2}) - NH(VX|Z)} \\
&\quad + 2^{N(H(X|UZ)-\frac{\epsilon_1}{2}) + N(H(U|Z)-\frac{\epsilon_1}{2}) + N(H(V|UZX)-\frac{\epsilon_1}{2})} \\
&\qquad \times 2^{-NH(XUV|Z)}\Big)^{\frac{1}{2}} \times 2^{\frac{1}{2}N\delta_{\mathcal{A}}(N)}
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(b)}{=} \Big(2^{-NI(X;U|Z)-N\frac{\epsilon_1}{2}} + 2^{-N\frac{\epsilon_1}{2}} + 2^{-NI(V;UX|Z)-N\frac{\epsilon_1}{2}} \\
&\quad + 2^{-N\epsilon_1} + 2^{-N\epsilon_1-NI(V;X|UZ)} + 2^{-N\frac{3\epsilon_1}{2}} \\
&\quad + 2^{-NI(V;U|ZX)-NI(X;U|Z)-N\epsilon_1}\Big)^{\frac{1}{2}} \times 2^{\frac{1}{2}N\delta_{\mathcal{A}}(N)} \\
&\overset{(c)}{\leq} \delta^{(0)}(N) - 2/N \xrightarrow{N\to+\infty} 0,
\end{aligned}
$$

where (a) holds by (6) and (7), (b) holds by the definition of mutual information and the chain rule for entropy, (c) holds by the definition of $\delta^{(0)}(N)$ and because $\epsilon_1 = 2(\delta_{\mathcal{A}}(N) + \xi)$. □

We now show that in each encoding block, the random variables induced by the coding scheme approximate well the target distribution.

Lemma 3. *For Block $i \in [\![1, k]\!]$, we have*

$$
\mathbb{V}(\widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}Z_i^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}) \leq \delta_i(N),
$$

where $\delta_i(N) \triangleq \frac{3}{2}(\delta(N) + \delta^{(0)}(N))(3^i - 1) + 3^{i+1}\delta(N)$.

Proof. We prove the result by induction. We first prove that the lemma holds for $i = 1$. Remark that

$$
\begin{aligned}
\widetilde{p}_{Y_1^{1:N}|U_1^{1:N}V_1^{1:N}X_1^{1:N}} &\overset{(a)}{=} \widetilde{p}_{Y_1^{1:N}|U_1^{1:N}V_1^{1:N}} \\
&\overset{(b)}{=} q_{Y^{1:N}|U^{1:N}V^{1:N}} \\
&\overset{(c)}{=} q_{Y^{1:N}|U^{1:N}V^{1:N}X^{1:N}},
\end{aligned} \tag{12}
$$

where (a) holds because $\widetilde{X}_1^{1:N}$ is independent from $(\widetilde{U}_1^{1:N}, \widetilde{V}_1^{1:N}, \widetilde{Y}_1^{1:N})$, (b) holds by the construction of $Y^{1:N}$ and $\widetilde{Y}_1^{1:N}$, (c) holds because $X^{1:N}$ is independent from $(U^{1:N}, V^{1:N}, Y^{1:N})$. Next, we have

$$
\begin{aligned}
&\mathbb{V}(\widetilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}Z_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}) \\
&\overset{(a)}{=} \mathbb{V}(\widetilde{p}_{Z_1^{1:N}|X_1^{1:N}Y_1^{1:N}}\widetilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}},
\end{aligned}
$$

$$
\begin{aligned}
&\quad q_{Z^{1:N}|X^{1:N}Y^{1:N}} q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}}\big) \\
&\overset{(b)}{=} \mathbb{V}(\widetilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}}\big) \\
&\overset{(c)}{=} \mathbb{V}(\widetilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}}\big) \\
&\overset{(d)}{=} \mathbb{V}(\widetilde{p}_{X_1^{1:N}}\widetilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}q_{U^{1:N}V^{1:N}}\big) \\
&\overset{(e)}{\leq} \mathbb{V}(\widetilde{p}_{X_1^{1:N}}\widetilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}\widetilde{p}_{U_1^{1:N}V_1^{1:N}}\big) \\
&\quad + \mathbb{V}(q_{X^{1:N}}\widetilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}q_{U^{1:N}V^{1:N}}\big) \\
&\overset{(f)}{=} \mathbb{V}(\widetilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\widetilde{p}_{U_1^{1:N}}\widetilde{p}_{V_1^{1:N}}, q_{U^{1:N}}q_{V^{1:N}}\big) \\
&\overset{(g)}{\leq} \mathbb{V}(\widetilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\widetilde{p}_{U_1^{1:N}}\widetilde{p}_{V_1^{1:N}}, q_{U^{1:N}}\widetilde{p}_{V_1^{1:N}}\big) \\
&\quad + \mathbb{V}(q_{U^{1:N}}\widetilde{p}_{V_1^{1:N}}, q_{U^{1:N}}q_{V^{1:N}}\big) \\
&= \mathbb{V}(\widetilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\widetilde{p}_{U_1^{1:N}}, q_{U^{1:N}}) + \mathbb{V}(\widetilde{p}_{V_1^{1:N}}, q_{V^{1:N}}) \qquad (13) \\
&\overset{(h)}{\leq} 3\delta(N),
\end{aligned}
$$

where (a) holds by the two Markov chains $(U^{1:N}, V^{1:N}) - (X^{1:N}, Y^{1:N}) - Z^{1:N}$ and $(\widetilde{U}_1^{1:N}, \widetilde{V}_1^{1:N}) - (\widetilde{X}_1^{1:N}, \widetilde{Y}_1^{1:N}) - \widetilde{Z}_1^{1:N}$, (b) holds because $q_{Z^{1:N}|X^{1:N}Y^{1:N}} = \widetilde{p}_{Z_1^{1:N}|X_1^{1:N}Y_1^{1:N}}$, (c) holds by (12), (d) holds because $X^{1:N}$ is independent from $(U^{1:N}, V^{1:N})$ and $\widetilde{X}_1^{1:N}$ is independent from $(\widetilde{U}_1^{1:N}, \widetilde{V}_1^{1:N})$, (e) holds by the triangle inequality, (f) holds because $U^{1:N}$ is independent from $V^{1:N}$ and $\widetilde{U}_1^{1:N}$ is independent from $\widetilde{V}_1^{1:N}$, (g) holds by the triangle inequality, (h) holds by the source resolvability codes used at the transmitters because $\frac{|E_1|}{N} > H(X) + \epsilon_1/2$, $\frac{|D_1|}{N} > H(U) + \epsilon_1/2$, $\frac{|F_1|}{N} > H(V) + \epsilon_1/2$.

Assume now that, for $i \in [\![2, k-1]\!]$, the lemma holds. For $i \in [\![2, k]\!]$, consider $\bar{E}_i, \bar{D}_i, \bar{F}_i$ distributed according to $p_{\bar{E}}^{unif}, p_{\bar{D}}^{unif}, p_{\bar{F}}^{unif}$, respectively. Let $p_{\bar{X}_i^{1:N}}, p_{\bar{U}_i^{1:N}}, p_{\bar{V}_i^{1:N}}$ denote the distribution of $\bar{X}_i^{1:N} \triangleq e_N^X(\bar{E}_i, E_i), \bar{U}_i^{1:N} \triangleq e_N^U(\bar{D}_i, D_i), \bar{V}_i^{1:N} \triangleq e_N^V(\bar{F}_i, F_i)$, respectively. Then, for $i \in [\![1, k-1]\!]$, we have

$$
\begin{aligned}
&\mathbb{V}(\widetilde{p}_{U_{i+1}^{1:N}V_{i+1}^{1:N}X_{i+1}^{1:N}Y_{i+1}^{1:N}Z_{i+1}^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}\big) \\
&\overset{(a)}{\leq} \mathbb{V}(\widetilde{p}_{X_{i+1}^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\widetilde{p}_{U_{i+1}^{1:N}}, q_{U^{1:N}}) + \mathbb{V}(\widetilde{p}_{V_{i+1}^{1:N}}, q_{V^{1:N}})
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(b)}{\leq} \mathbb{V}(\widetilde{p}_{X_{i+1}^{1:N}}, p_{\bar{X}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{X}_{i+1}^{1:N}}, q_{X^{1:N}}) \\
&\quad + \mathbb{V}(\widetilde{p}_{U_{i+1}^{1:N}}, p_{\bar{U}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{U}_{i+1}^{1:N}}, q_{U^{1:N}}) \\
&\quad + \mathbb{V}(\widetilde{p}_{V_{i+1}^{1:N}}, p_{\bar{V}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{V}_{i+1}^{1:N}}, q_{V^{1:N}}) \\
&\overset{(c)}{\leq} 3\delta(N) + \mathbb{V}(\widetilde{p}_{X_{i+1}^{1:N}}, p_{\bar{X}_{i+1}^{1:N}}) + \mathbb{V}(\widetilde{p}_{U_{i+1}^{1:N}}, p_{\bar{U}_{i+1}^{1:N}}) \\
&\quad + \mathbb{V}(\widetilde{p}_{V_{i+1}^{1:N}}, p_{\bar{V}_{i+1}^{1:N}}) \\
&\overset{(d)}{\leq} 3\delta(N) + \mathbb{V}(\widetilde{p}_{E_{i+1}}, p_{\bar{E}}^{unif}) + \mathbb{V}(\widetilde{p}_{D_{i+1}}, p_{\bar{D}}^{unif}) \\
&\quad + \mathbb{V}(\widetilde{p}_{F_{i+1}}, p_{\bar{F}}^{unif}),
\end{aligned} \tag{14}
$$

where (a) holds similar to (13), (b) holds by the triangle inequality, (c) holds by the source resolvability codes used at the transmitters because $\frac{|\bar{E}_i|+|E_i|}{N} = H(X) + \epsilon_1/2$, $\frac{|\bar{F}_i|+|F_i|}{N} = H(V) + \epsilon_1/2$, $\frac{|\bar{D}_i|+|D_i|}{N} = H(U) + \epsilon_1/2$, (d) holds by the data processing inequality. Next, we have

$$
\begin{aligned}
&\max\Big(\mathbb{V}(\widetilde{p}_{E_{i+1}}, p_{\bar{E}}^{unif}), \mathbb{V}(\widetilde{p}_{D_{i+1}}, p_{\bar{D}}^{unif}), \mathbb{V}(\widetilde{p}_{F_{i+1}}, p_{\bar{F}}^{unif})\Big) \\
&\leq \mathbb{V}(\widetilde{p}_{E_{i+1}D_{i+1}F_{i+1}}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif}) \\
&\overset{(a)}{\leq} \mathbb{V}(\widetilde{p}_{E_{i+1}D_{i+1}F_{i+1}}, q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}) \\
&\quad + \mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif}) \\
&\overset{(b)}{=} \mathbb{V}(\widetilde{p}_{G_X(X_i^{1:N})G_U(U_i^{1:N})G_V(V_i^{1:N})}, \\
&\qquad\quad q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}) \\
&\quad + \mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V_i^{1:N})}, p_{\bar{E}}^{unif} p_{\bar{D}}^{unif} p_{\bar{F}}^{unif}) \\
&\overset{(c)}{\leq} \mathbb{V}(\widetilde{p}_{X_i^{1:N}U_i^{1:N}V_i^{1:N}}, q_{X^{1:N}U^{1:N}V^{1:N}}) + \delta^{(0)}(N) \\
&\overset{(d)}{\leq} \delta_i(N) + \delta^{(0)}(N),
\end{aligned} \tag{15}
$$

where (a) holds by the triangle inequality, (b) holds because $\widetilde{E}_{i+1} \triangleq G_X(\widetilde{X}_i^{1:N}), \widetilde{D}_{i+1} \triangleq G_U(\widetilde{U}_i^{1:N}), \widetilde{F}_{i+1} \triangleq G_V(\widetilde{V}_i^{1:N})$ by Line 5 of Algorithm 1 and Algorithm 2 , (c) holds by the data processing inequality and Lemma 2, (d) holds by the

induction hypothesis. By combining (14) and (15), we have

$$\begin{aligned}
&\mathbb{V}(\widetilde{p}_{U_{i+1}^{1:N}V_{i+1}^{1:N}X_{i+1}^{1:N}Y_{i+1}^{1:N}Z_{i+1}^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}) \\
&\leq 3(\delta(N) + \delta_i(N) + \delta^{(0)}(N)) \\
&= \delta_{i+1}(N).
\end{aligned}$$

□

The next lemma shows that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent of the channel output in Block $i-1$.

Lemma 4. *For $i \in [\![2, k]\!]$, we have*

$$\mathbb{V}(\widetilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_iD_iF_i}) \leq \delta_i^{(1)}(N),$$

where $\delta_i^{(1)}(N) \triangleq 4\delta_{i-1}(N) + 2\delta^{(0)}(N)$.

Proof. We have

$$\begin{aligned}
&\mathbb{V}(\widetilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_iD_iF_i}) \\
&\overset{(a)}{\leq} \mathbb{V}(\widetilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \widetilde{p}_{Z_{i-1}^{1:N}}p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}) \\
&\quad + \mathbb{V}(\widetilde{p}_{Z_{i-1}^{1:N}}p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}, \widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_iD_iF_i}) \\
&\leq 2\mathbb{V}(\widetilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \widetilde{p}_{Z_{i-1}^{1:N}}p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}) \\
&\overset{(b)}{\leq} 2\Big(\mathbb{V}(\widetilde{p}_{E_iD_iF_iZ_{i-1}^{1:N}}, q_{EDFZ^{1:N}}) \\
&\quad + \mathbb{V}(q_{EDFZ^{1:N}}, p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}q_{Z^{1:N}}) \\
&\quad + \mathbb{V}(p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}q_{Z^{1:N}}, p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}\widetilde{p}_{Z_{i-1}^{1:N}})\Big) \\
&\overset{(c)}{\leq} 2\Big(\mathbb{V}(\widetilde{p}_{X_{i-1}^{1:N}U_{i-1}^{1:N}V_{i-1}^{1:N}Z_{i-1}^{1:N}}, q_{X^{1:N}U^{1:N}V^{1:N}Z^{1:N}}) \\
&\quad + \mathbb{V}(q_{EDFZ^{1:N}}, p_{\bar{E}}^{unif}p_{\bar{D}}^{unif}p_{\bar{F}}^{unif}q_{Z^{1:N}}) \\
&\quad + \mathbb{V}(q_{Z^{1:N}}, \widetilde{p}_{Z_{i-1}^{1:N}})\Big)
\end{aligned}$$

$$\overset{(d)}{\leq} 2(2\mathbb{V}(\widetilde{p}_{X_{i-1}^{1:N}U_{i-1}^{1:N}V_{i-1}^{1:N}Z_{i-1}^{1:N}}, q_{X^{1:N}U^{1:N}V^{1:N}Z^{1:N}})+\delta^{(0)}(N))$$
$$\overset{(e)}{\leq} 4\delta_{i-1}(N) + 2\delta^{(0)}(N),$$

where (a) and (b) hold by the triangle inequality, (c) holds by the data processing inequality using (11) and $\widetilde{E}_i \triangleq G_X(\widetilde{X}_{i-1}^{1:N}), \widetilde{D}_i \triangleq G_U(\widetilde{U}_{i-1}^{1:N}), \widetilde{F}_i \triangleq G_V(\widetilde{V}_{i-1}^{1:N})$ from Line 5 of Algorithm 1 and Algorithm 2, (d) holds by (11) and Lemma 2, (e) holds by Lemma 3. $\square$

The next lemma shows that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent of the channel outputs in Blocks 1 to $i-1$ considered jointly.

Lemma 5. *For $i \in [\![2, k]\!]$, we have*

$$\mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}\right) \leq \delta_i^{(2)}(N),$$

where $\delta_i^{(2)}(N) \triangleq (2^{i-1}-1)(4\delta_{i-1}(N) + 2\delta^{(0)}(N))$.

Proof. We prove the result by induction. The lemma is true for $i = 2$ by Lemma 4. Assume now that the lemma holds for $i \in [\![2, k-1]\!]$. Then, for $i \in [\![3, k]\!]$, we have

$$\mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}D_{i-1}E_{i-1}F_{i-1}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{D_{i-1}E_{i-1}F_{i-1}}\right) \leq \delta_{i-1}^{(2)}(N).$$

We have

$$\begin{aligned}
&\mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}\right)\\
&\overset{(a)}{\leq} \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}D_iE_iF_i}\right)\\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}\right)\\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}\right)\\
&= \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}D_iE_iF_i}\right)\\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{i-1}^{1:N}D_iE_iF_i}, \widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{D_iE_iF_i}\right)\\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\right)
\end{aligned}$$

$$
\begin{aligned}
&\overset{(b)}{\leq} \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i}, \widetilde{p}_{Z_{1:i-2}^{1:N}} \widetilde{p}_{Z_{i-1}^{1:N} D_i E_i F_i}\right) \\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}} \widetilde{p}_{Z_{i-1}^{1:N}}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\right) + \delta_i^{(1)}(N) \\
&\overset{(c)}{\leq} 2\mathbb{V}\Big(\widetilde{p}_{Z_{1:i-1}^{1:N} D_{i-1:i} E_{i-1:i} F_{i-1:i}}, \\
&\qquad \widetilde{p}_{Z_{1:i-2}^{1:N}} \widetilde{p}_{Z_{i-1}^{1:N} D_{i-1:i} E_{i-1:i} F_{i-1:i}}\Big) + \delta_i^{(1)}(N) \\
&\overset{(d)}{=} 2\mathbb{V}\Big(\widetilde{p}_{Z_{1:i-2}^{1:N} D_{i-1} E_{i-1} F_{i-1}} \widetilde{p}_{Z_{i-1}^{1:N} D_i E_i F_i | D_{i-1} E_{i-1} F_{i-1}}, \\
&\qquad \widetilde{p}_{Z_{1:i-2}^{1:N}} \widetilde{p}_{Z_{i-1}^{1:N} D_{i-1:i} E_{i-1:i} F_{i-1:i}}\Big) + \delta_i^{(1)}(N) \\
&= 2\mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N} D_{i-1} E_{i-1} F_{i-1}}, \widetilde{p}_{Z_{1:i-2}^{1:N}} \widetilde{p}_{D_{i-1} E_{i-1} F_{i-1}}\right) \\
&\quad + \delta_i^{(1)}(N) \\
&\overset{(e)}{\leq} \delta_i^{(1)}(N) + 2\delta_{i-1}^{(2)}(N) \\
&\leq \delta_i^{(2)}(N),
\end{aligned}
$$

where (a) holds by the triangle inequality, (b) holds by Lemma 4, (c) follows from the data processing inequality, (d) holds by the Markov chain $(\widetilde{D}_i, \widetilde{E}_i, \widetilde{F}_i, \widetilde{Z}_{i-1}^{1:N}) - (\widetilde{D}_{i-1}, \widetilde{E}_{i-1}, \widetilde{F}_{i-1}) - \widetilde{Z}_{1:i-2}^{1:N}$, (e) holds by the induction hypothesis. □

The next lemma shows that the channel outputs of all the blocks are asymptotically independent.

Lemma 6. *We have*

$$
\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right) \leq (k-1)\delta_k^{(2)}(N),
$$

where $\delta_k^{(2)}(N)$ is defined in Lemma 5.

Proof. We have

$$
\begin{aligned}
&\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right) \\
&\overset{(a)}{\leq} \sum_{i=2}^{k} \mathbb{V}\left(\widetilde{p}_{Z_{1:i}^{1:N}} \prod_{j=i+1}^{k} \widetilde{p}_{Z_j^{1:N}}, \widetilde{p}_{Z_{1:i-1}^{1:N}} \prod_{j=i}^{k} \widetilde{p}_{Z_j^{1:N}}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=2}^{k} \mathbb{V}\left(\widetilde{p}_{Z_{1:i}^{1:N}}, \widetilde{p}_{Z_{1:i-1}^{1:N}} \widetilde{p}_{Z_i^{1:N}}\right) \\
&\leq \sum_{i=2}^{k} \mathbb{V}\left(\widetilde{p}_{Z_{1:i}^{1:N} D_i E_i F_i}, \widetilde{p}_{Z_i^{1:N} D_i E_i F_i} \widetilde{p}_{Z_{1:i-1}^{1:N}}\right) \\
&\overset{(b)}{=} \sum_{i=2}^{k} \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N} | D_i E_i F_i} \widetilde{p}_{Z_i^{1:N} D_i E_i F_i}, \widetilde{p}_{Z_i^{1:N} D_i E_i F_i} \widetilde{p}_{Z_{1:i-1}^{1:N}}\right) \\
&= \sum_{i=2}^{k} \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i}, \widetilde{p}_{Z_{1:i-1}^{1:N}} \widetilde{p}_{D_i E_i F_i}\right) \\
&\overset{(c)}{\leq} \sum_{i=2}^{k} \delta_i^{(2)}(N) \\
&\leq (k-1) \max_{j \in [\![2,k]\!]} \delta_j^{(2)}(N),
\end{aligned}
$$

where (a) holds by the triangle inequality, (b) holds by the Markov chain $\widetilde{Z}_i^{1:N} - (\widetilde{D}_i, \widetilde{E}_i, \widetilde{F}_i) - \widetilde{Z}_{1:i-1}^{1:N}$, (c) holds by Lemma 5. □

We now show that the target output distribution is well approximated jointly over all blocks.

Lemma 7. *For Block $i \in [\![1, k]\!]$, we have*

$$
\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, q_{Z^{1:kN}}\right) \leq (k-1)\delta_k^{(2)}(N) + k\delta_k(N),
$$

where $\delta_k^{(2)}(N)$ is defined in Lemma 5 and $\delta_k(N)$ is defined in Lemma 3.

Proof. We have

$$
\begin{aligned}
&\mathbb{V}(\widetilde{p}_{Z_{1:k}^{1:N}}, q_{Z^{1:kN}}) \\
&\overset{(a)}{\leq} (k-1)\delta_k^{(2)}(N) + \mathbb{V}(\prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}, q_{Z^{1:kN}}) \\
&\overset{(b)}{\leq} (k-1)\delta_k^{(2)}(N) + \mathbb{V}(\widetilde{p}_{Z_1^{1:N}} \prod_{i=2}^{k} \widetilde{p}_{Z_i^{1:N}}, q_{Z^{1:N}} \prod_{i=2}^{k} \widetilde{p}_{Z_i^{1:N}}) \\
&\quad + \mathbb{V}(q_{Z^{1:N}} \prod_{i=2}^{k} \widetilde{p}_{Z_i^{1:N}}, q_{Z^{1:kN}})
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(c)}{\leq} (k-1)\delta_k^{(2)}(N) + \delta_1(N) + \mathbb{V}(\prod_{i=2}^{k} \widetilde{p}_{Z_i^{1:N}}, q_{Z^{1:(k-1)N}}) \\
&\overset{(d)}{\leq} (k-1)\delta_k^{(2)}(N) + \sum_{i=1}^{k} \delta_i(N) \\
&\leq (k-1)\delta_k^{(2)}(N) + k \max_{j \in [\![1,k]\!]} \delta_j(N),
\end{aligned}
$$

where (a) holds by the triangle inequality and Lemma 6, (b) holds by the triangle inequality, (c) holds by Lemma 3, (d) holds by induction. □

Finally, the next lemma shows that the encoding scheme of Section 2.5.1 achieves the desired rate-tuple.

Lemma 8. *Let $\epsilon_0 > 0$. For k large enough and $\xi > 0$, we have*

$$
\begin{aligned}
\lim_{N \to +\infty} R_1 &= I(X; ZU) + \epsilon_0 + 2\xi, \\
\lim_{N \to +\infty} R_U &= I(U; Z) + \epsilon_0 + 2\xi, \\
\lim_{N \to +\infty} R_V &= I(V; ZUX) + \epsilon_0 + 2\xi.
\end{aligned}
$$

Proof. Let k be such that $\frac{1}{k}\max(H(X), H(U), H(V)) < \epsilon_0$. Then, by the definition of ϵ_1, we have

$$
\begin{aligned}
R_1 &= \frac{\sum_{i=1}^{k} |E_i|}{kN} \\
&= \frac{N(H(X) + \epsilon_1) + (k-1)N(I(X; ZU) + \epsilon_1)}{kN} \\
&\leq \frac{H(X)}{k} + I(X; ZU) + \epsilon_1 \\
&\leq \epsilon_0 + I(X; ZU) + \epsilon_1 \\
&\xrightarrow{N \to +\infty} I(X; ZU) + \epsilon_0 + 2\xi,
\end{aligned}
$$

$$
\begin{aligned}
R_U &= \frac{\sum_{i=1}^{k} |D_i|}{kN} \\
&= \frac{N(H(U) + \epsilon_1 + (k-1)N(I(U;Z) + \epsilon_1)}{kN} \\
&\leq \frac{H(U)}{k} + I(U;Z) + \epsilon_1 \\
&\leq \epsilon_0 + I(U;Z) + \epsilon_1 \\
&\xrightarrow{N \to +\infty} I(U;Z) + \epsilon_0 + 2\xi,
\end{aligned}
$$

$$
\begin{aligned}
R_V &= \frac{\sum_{i=1}^{k} |F_i|}{kN} \\
&= \frac{N(H(V) + \epsilon_1) + (k-1)N(I(V;ZUX) + \epsilon_1)}{kN} \\
&\leq \frac{H(V)}{k} + I(V;ZUX) + \epsilon_1 \\
&\leq \epsilon_0 + I(V;ZUX) + \epsilon_1 \\
&\xrightarrow{N \to +\infty} I(V;ZUX) + \epsilon_0 + 2\xi.
\end{aligned}
$$

□

2.7.2 Coding scheme analysis for Case 2

For Case 2, $U = \emptyset$ and $V = Y$, so that by Lemma 8, the achieved rate pair is such that

$$
\begin{aligned}
\lim_{N \to +\infty} R_1 &= I(X;Z) + \epsilon_0 + 2\xi, \\
\lim_{N \to +\infty} R_2 &= \lim_{N \to +\infty} (R_V + R_U) \\
&= I(Y;ZX) + \epsilon_0 + 2\xi \\
&\overset{(a)}{=} I(Y;Z|X) + \epsilon_0 + 2\xi \\
&\overset{(b)}{=} I(Y;Z) + \epsilon_0 + 2\xi,
\end{aligned}
$$

where (a) holds by independence between X and Y, and (b) holds because $I(XY;Z) = I(X;Z) + I(Y;Z)$ in Case 2.

2.8 Extension to more than two transmitters

Consider a discrete memoryless multiple access channel $(\mathcal{X}_{\mathcal{L}}, q_{Z|X_{\mathcal{L}}}, \mathcal{Z})$, where $\mathcal{X}_l = \{0,1\}$, $l \in \mathcal{L} \triangleq [\![1, L]\!]$, $\mathcal{Z}$ is a finite alphabet, and $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$. The definitions in Section 2.2.2 immediately extend to this multiple access channel with L transmitters and we have the following counterpart of Theorem 1.

Theorem 4. *We have $\mathcal{R}_{q_Z} = \mathcal{R}'_{q_Z}$ with*

$$\mathcal{R}'_{q_Z} \triangleq \bigcup_{p_T, (q_{X_l|T})_{l\in\mathcal{L}}} \{(R_l)_{l\in\mathcal{L}} : I(X_{\mathcal{S}}; Z|T) \leq R_{\mathcal{S}}, \forall \mathcal{S} \subseteq \mathcal{L}\},$$

where p_T is defined over $\mathcal{T} \triangleq [\![1, |\mathcal{Z}| + 2^L - 1]\!]$ and $(q_{X_l|T})_{l\in\mathcal{L}}$ are such that, for any $t \in \mathcal{T}$ and $z \in \mathcal{Z}$,

$$q_Z(z) = \sum_{x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}} q_{Z|X_{\mathcal{L}}}(z|x_{\mathcal{L}}) \prod_{l\in\mathcal{L}} q_{X_l|T}(x_l|t).$$

Proof. The converse is an immediate extension of the converse of Theorem 1 from [11]. The achievability follows from Theorem 5. □

Theorem 5. *The coding scheme presented in Section 2.8.1, which solely relies on source resolvability codes, used as black boxes, and two-universal hash functions, achieves the entire multiple access channel resolvability region $\mathcal{R}_{q_Z}$ of Theorem 4 for any discrete memoryless multiple access channel with binary input alphabets.*

2.8.1 Achievability Scheme

In the following, we use the notation $X_{\mathcal{S}} \triangleq (X_l)_{l\in\mathcal{S}}$ for $\mathcal{S} \subseteq \mathcal{L}$, and $X_{1:l} \triangleq X_{[\![1,l]\!]}$ for $l \in \mathcal{L}$. Let $p_{X_{\mathcal{L}}} \triangleq \prod_{l\in\mathcal{L}} p_{X_l}$. We will show the achievability of the region

$$\mathcal{R}\left(p_{X_{\mathcal{L}}}\right) \triangleq \{(R_l)_{l\in\mathcal{L}} : I(X_{\mathcal{S}}; Z) \leq R_{\mathcal{S}}, \forall \mathcal{S} \subseteq \mathcal{L}\},$$

which reduces to showing the achievability of the rate-tuple $(I(X_l; Z|X_{1:l-1}))_{l\in\mathcal{L}}$. Indeed, the set function $\mathcal{S} \mapsto -I(X_{\mathcal{S}}; Z)$ is submodular, e.g., [24], and the region $\mathcal{R}\left(p_{X_{\mathcal{L}}}\right)$ thus forms a contrapolymatroid [23] whose dominant face is the convex hull of its extreme points given by $\{(I(X_{\sigma(l)}; Z|X_{\{\sigma(i):i\in[\![1,l-1]\!]\}}))_{l\in\mathcal{L}} : \sigma \in \mathfrak{S}(L)\}$, where $\mathfrak{S}(L)$ is the symmetric group over $\mathcal{L}$. By time-sharing and symmetry of the extreme points, the achievability of the dominant face reduces to showing the achievability of one extreme point, which without loss of generality can be chosen as $(I(X_l; Z|X_{1:l-1}))_{l\in\mathcal{L}}$.

The encoding scheme to achieve $(I(X_l; Z|X_{1:l-1}))_{l\in\mathcal{L}}$ operates over $k \in \mathbb{N}$ blocks of length N. In this section, we use the double subscripts notation $X_{l,i}$, where the first subscript corresponds to Transmitter $l \in \mathcal{L}$ and the second subscript corresponds to Block $i \in [\![1, k]\!]$. The encoding at Transmitter $l \in \mathcal{L}$ is described in Algorithm 3 and uses

- A hash function $G_{X_l} : \{0,1\}^N \longrightarrow \{0,1\}^{r_{X_l}}$ chosen uniformly at random in a family of two-universal hash functions, where the output length of the hash function G_{X_l} is defined as follows

$$r_{X_l} \triangleq N(H(X_l|ZX_{1:l-1}) - \epsilon_2/2). \tag{16}$$

- A source resolvability code for the discrete memoryless source $(\mathcal{X}_l, q_{X_l})$ with encoder function $e_N^{X_l}$ and rate $H(X_l) + \frac{\epsilon_2}{2}$, where $\epsilon_2 \triangleq 2(\delta^*_{\mathcal{L}}(N) + \xi)$, $\delta^*_{\mathcal{L}}(N) \triangleq \log(|\mathcal{X}_{\mathcal{L}}| + 3)\sqrt{\frac{2}{N}(L + \log N)}$, $\xi > 0$, such that the distribution of the encoder output $\widetilde{p}_{X_l^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{X_l^{1:N}}, q_{X_l^{1:N}}) \leq \delta(N)$, where $\delta(N)$ is such that $\lim_{N\to+\infty} \delta(N) = 0$.

In Algorithm 3 and for any $l \in \mathcal{L}$, the hash function output $\widetilde{E}_{l,i}$, $i \in [\![2, k]\!]$, with length r_{X_l} corresponds to recycled randomness from Block $i - 1$.

2.8.2 Achievability Scheme Analysis

For convenience, define, for any $l \in \mathcal{L}$, $\widetilde{E}_{l,1} \triangleq \emptyset$. Let $\widetilde{p}_{E_{1:L,i}X_{1:L,i}^{1:N}Z_i^{1:N}}$ denote the joint probability distribution of the random variables $\widetilde{E}_{l,i}, \widetilde{X}_{l,i}^{1:N}$, and $\widetilde{Z}_i^{1:N}$, $l \in \mathcal{L}$, created in

Algorithm 3 Encoding algorithm at Transmitter $l \in \mathcal{L}$

Require: A vector $E_{l,1}$ of $N(H(X_l)+\epsilon_2)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, a vector $E_{l,i}$ of $N(I(X_l;ZX_{1:l-1})+\epsilon_2)$ uniformly distributed bits.

for Block $i=1$ to k **do**
  if $i=1$ **then**
    Define $\widetilde{X}_{l,1}^{1:N} \triangleq e_N^{X_l}(E_{l,1})$
  else if $i>1$ **then**
    Define $\widetilde{E}_{l,i} \triangleq G_{X_l}(\widetilde{X}_{l,i-1}^{1:N})$
    Define $\widetilde{X}_{l,i}^{1:N} \triangleq e_N^{X_l}(\widetilde{E}_{l,i} \| E_{l,i})$
  end if
  Send $\widetilde{X}_{l,i}^{1:N}$ over the channel
end for

Block $i \in [\![1,k]\!]$ of the coding scheme of Section 2.8.1.

We prove in the following lemma that in Block $i \in [\![2,k]\!]$, if the inputs $\widetilde{X}_{1:L,i-1}^{1:N}$ of the hash functions $(G_{X_l})_{l\in\mathcal{L}}$ are replaced by $X_{1:L}^{1:N}$ distributed according to $q_{X_{1:L}^{1:N}} \triangleq \prod_{i=1}^N q_{X_{1:L}}$, then the outputs of these hash functions are almost jointly uniformly distributed. Define

$$G_{X_{1:L}}(X_{1:L}^{1:N}) \triangleq \left(G_{X_l}(X_l^{1:N})\right)_{l\in\mathcal{L}}.$$

Lemma 9. *Let $p_{\bar{E}_{1:L}}^{unif}$ denote the uniform distribution over $\{0,1\}^{\sum_{l\in\mathcal{L}} r_{X_l}}$. Then, we have*

$$\mathbb{V}\left(q_{G_{X_{1:L}}(X_{1:L}^{1:N})Z^{1:N}}, p_{\bar{E}_{1:L}}^{unif} q_{Z^{1:N}}\right) \leq \delta^{*(0)}(N),$$

where $\delta^{*(0)}(N) \triangleq 2/N + 2^{\frac{L}{2}} 2^{-\frac{N\xi}{2}}$.

Proof. Using Lemma 16 in Appendix 2.9, with the substitutions $\mathcal{A} \leftarrow \mathcal{L}, T_{\mathcal{A}}^{1:N} \leftarrow X_{\mathcal{L}}^{1:N}$, applied to the product distribution $q_{X_{\mathcal{L}}^{1:N}Z^{1:N}}$, there exists a subnormalized non-negative function $w_{X_{\mathcal{L}}^{1:N}Z^{1:N}}$ such that for any $\mathcal{S} \subseteq \mathcal{L}$

$$\mathbb{V}(w_{X_{1:L}^{1:N}Z^{1:N}}, q_{X_{1:L}^{1:N}Z^{1:N}}) \leq 1/N, \tag{17}$$

$$H_\infty(w_{X_{\mathcal{S}}^{1:N}Z^{1:N}} | q_{Z^{1:N}}) \geq NH(X_{\mathcal{S}}|Z) - N\delta_{\mathcal{S}}^*(N), \tag{18}$$

where the min-entropy $H_\infty(w_{X_{\mathcal{S}}^{1:N}Z^{1:N}}|q_{Z^{1:N}})$ is defined in Lemma 16 in Appendix 2.9, and

$\delta^*_{\mathcal{S}}(N) \triangleq \log(|\mathcal{X}_{\mathcal{S}}|+3)\sqrt{\frac{2}{N}(L+\log N)}$. Let $q_{E_{1:L}}$ define the distribution of

$$E_{1:L} \triangleq G_{X_{1:L}}(X_{1:L}^{1:N}), \tag{19}$$

where $X_{1:L}^{1:N}$ is distributed according to $q_{X_{1:L}^{1:N}}$. We have

$$\begin{aligned}
&\mathbb{V}(q_{E_{1:L}Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} q_{Z^{1:N}}) \\
&\overset{(a)}{\leq} \mathbb{V}(q_{E_{1:L}Z^{1:N}}, w_{E_{1:L}Z^{1:N}}) + \mathbb{V}(w_{E_{1:L}Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} q_{Z^{1:N}}) \\
&\overset{(b)}{\leq} \mathbb{V}(q_{X_{1:L}^{1:N}Z^{1:N}}, w_{X_{1:L}^{1:N}Z^{1:N}}) + \mathbb{V}(w_{E_{1:L}Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} q_{Z^{1:N}}) \\
&\overset{(c)}{\leq} 1/N + \mathbb{V}(w_{E_{1:L}Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} w_{Z^{1:N}}) \\
&\quad + \mathbb{V}(p^{unif}_{\bar{E}_{1:L}} w_{Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} q_{Z^{1:N}}) \\
&\overset{(d)}{\leq} 2/N + \mathbb{V}(w_{E_{1:L}Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}} w_{Z^{1:N}}) \\
&\overset{(e)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{r_{X_{\mathcal{S}}} - H_\infty(w_{X_{\mathcal{S}}^{1:N}Z^{1:N}}|q_{Z^{1:N}})}} \\
&\overset{(f)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{r_{X_{\mathcal{S}}} - NH(X_{\mathcal{S}}|Z) + N\delta^*_{\mathcal{L}}(N)}} \\
&\overset{(g)}{=} 2/N + \Bigg(\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{\sum_{l\in\mathcal{S}}(N(H(X_l|ZX_{1:l-1}) - \frac{\epsilon_2}{2}))} \\
&\quad \times 2^{-N\sum_{l\in\mathcal{S}} H(X_l|ZX_{[\![1,l-1]\!]\cap\mathcal{S}}) + N\delta^*_{\mathcal{L}}(N)}\Bigg)^{1/2} \\
&\overset{(h)}{\leq} 2/N + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{\sum_{l\in\mathcal{S}} N(-\frac{\epsilon_2}{2} + \delta^*_{\mathcal{L}}(N))}} \\
&\overset{(i)}{\leq} 2/N + \sqrt{2^L 2^{-N\xi}} \xrightarrow{N\to+\infty} 0,
\end{aligned}$$

where (a) holds by the triangle inequality, (b) holds by (19) and the data processing inequality, (c) holds by (17) and the triangle inequality, (d) holds by (17), (e) holds by Lemma 17 in Appendix 2.9, (f) holds by (18) and because for any $\mathcal{S}\subseteq\mathcal{L}$, $\delta^*_{\mathcal{S}}(N) \leq \delta^*_{\mathcal{L}}(N)$, (g) holds by (16) and the chain rule, (h) holds because conditioning reduces entropy, (i) holds because $|\mathcal{S}| \geq 1$ and $\epsilon_2 = 2(\delta^*_{\mathcal{L}}(N) + \xi)$. □

We now show that in each encoding block, the random variables induced by the coding scheme approximate well the target distribution.

Lemma 10. *For Block $i \in [\![1, k]\!]$,*

$$\mathbb{V}(\widetilde{p}_{X_{1:L,i}^{1:N} Z_i^{1:N}}, q_{X_{1:L}^{1:N} Z^{1:N}}) \leq \delta_i^*(N), \tag{20}$$

where $\delta_i^*(N) \triangleq L(\delta(N) + \delta^{*(0)}(N))(\frac{L^i - 1}{L-1}) + L^{i+1}\delta(N)$.

Proof. We prove the result by induction. For $i = 1$, we have

$$\begin{aligned}
&\mathbb{V}(\widetilde{p}_{X_{1:L,1}^{1:N} Z_1^{1:N}}, q_{X_{1:L}^{1:N} Z^{1:N}}) \\
&= \mathbb{V}(\widetilde{p}_{Z_1^{1:N}|X_{1:L,1}^{1:N}} \widetilde{p}_{X_{1:L,1}^{1:N}}, q_{Z^{1:N}|X_{1:L}^{1:N}} q_{X_{1:L}^{1:N}}) \\
&\overset{(a)}{=} \mathbb{V}(\widetilde{p}_{X_{1:L,1}^{1:N}}, q_{X_{1:L}^{1:N}}) \\
&\overset{(b)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\widetilde{p}_{X_{l,1}^{1:N}}, q_{X_l^{1:N}}) \\
&\overset{(c)}{\leq} L\delta(N),
\end{aligned} \tag{21}$$

where (a) holds because $q_{Z^{1:N}|X_{1:L}^{1:N}} = \widetilde{p}_{Z_1^{1:N}|X_{1:L,1}^{1:N}}$, (b) holds by the triangle inequality and because $(\widetilde{X}_{l,1}^{1:N})_{l \in \mathcal{L}}$ are jointly independent, and $(X_l^{1:N})_{l \in \mathcal{L}}$ are jointly independent, (c) holds by the source resolvability codes used at the transmitters because $\frac{|E_{l,1}|}{N} > H(X_l) + \epsilon_2/2, l \in \mathcal{L}$.

Assume now that, for $i \in [\![2, k-1]\!]$, (20) holds. For any $l \in \mathcal{L}$ and $i \in [\![2, k]\!]$, consider $\bar{E}_{l,i}$ distributed according to $p_{\bar{E}_l}^{unif}$, the uniform distribution over $\{0,1\}^{r_{X_l}}$, and let $p_{\bar{X}_{l,i}^{1:N}}$ denote the distribution of $\bar{X}_{l,i}^{1:N} \triangleq e_N^{X_l}(\bar{E}_{l,i}, E_{l,i})$. For $i \in [\![1, k-1]\!]$, we have

$$\begin{aligned}
&\mathbb{V}(\widetilde{p}_{X_{1:L,i+1}^{1:N} Z_{i+1}^{1:N}}, q_{X_{1:L}^{1:N} Z^{1:N}}) \\
&\overset{(a)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\widetilde{p}_{X_{l,i+1}^{1:N}}, q_{X_l^{1:N}}) \\
&\overset{(b)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\widetilde{p}_{X_{l,i+1}^{1:N}}, p_{\bar{X}_{l,i+1}^{1:N}}) + \mathbb{V}(p_{\bar{X}_{l,i+1}^{1:N}}, q_{X_l^{1:N}})
\end{aligned}$$

$$
\begin{aligned}
&\overset{(c)}{\leq} \sum_{l\in\mathcal{L}} \mathbb{V}(\widetilde{p}_{X_{l,i+1}^{1:N}}, p_{\bar{X}_{l,i+1}^{1:N}}) + \delta(N) \\
&\overset{(d)}{\leq} \sum_{l\in\mathcal{L}} \mathbb{V}(\widetilde{p}_{E_{l,i+1}}, p_{\bar{E}_l}^{unif}) + \delta(N) \\
&\overset{(e)}{\leq} \sum_{l\in\mathcal{L}} \Big(\delta(N) + \mathbb{V}(\widetilde{p}_{E_{l,i+1}}, q_{G_{X_l}(X_l^{1:N})}) \\
&\qquad +\mathbb{V}(q_{G_{X_l}(X_l^{1:N})}, p_{\bar{E}_l}^{unif})\Big) \\
&\overset{(f)}{=} \sum_{l\in\mathcal{L}} \Big(\delta(N) + \mathbb{V}(\widetilde{p}_{G_{X_l}(X_{l,i}^{1:N})}, q_{G_{X_l}(X_l^{1:N})}) \\
&\qquad +\mathbb{V}(q_{G_{X_l}(X_l^{1:N})}, p_{\bar{E}_l}^{unif})\Big) \\
&\overset{(g)}{\leq} \sum_{l\in\mathcal{L}} \delta(N) + \mathbb{V}(\widetilde{p}_{X_{l,i}^{1:N}}, q_{X_l^{1:N}}) + \delta^{*(0)}(N) \\
&\overset{(h)}{\leq} \sum_{l\in\mathcal{L}} \delta(N) + \delta_i^*(N) + \delta^{*(0)}(N) \\
&= L\left(\delta(N) + \delta_i^*(N) + \delta^{*(0)}(N)\right),
\end{aligned}
$$

where (a) holds similar to (21), (b) holds by the triangle inequality, (c) holds by the source resolvability codes used at the transmitters because $\frac{|\bar{E}_{l,i}|+|E_{l,i}|}{N} = H(X_l) + \epsilon_2/2, l \in \mathcal{L}$, (d) holds by the data processing inequality, (e) holds by the triangle inequality, (f) holds because for any $l \in \mathcal{L}$, $\widetilde{E}_{l,i+1} \triangleq G_{X_l}(X_{l,i}^{1:N})$ by Line 5 of Algorithm 3, (g) holds by the data processing inequality and Lemma 9, (h) holds by the induction hypothesis. □

Next, we show that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent from the channel outputs of Block $i-1$.

Lemma 11. *For $i \in [\![2, k]\!]$, we have*

$$
\mathbb{V}(\widetilde{p}_{E_{1:L,i}Z_{i-1}^{1:N}}, \widetilde{p}_{E_{1:L,i}}\widetilde{p}_{Z_{i-1}^{1:N}}) \leq \delta_i^{*(1)}(N).
$$

where $\delta_i^{*(1)}(N) \triangleq 4\delta_{i-1}^*(N) + 2\delta^{*(0)}(N)$.

Proof. We have

$$
\begin{aligned}
&\mathbb{V}(\widetilde{p}_{E_{1:L,i}Z_{i-1}^{1:N}}, \widetilde{p}_{E_{1:L,i}}\widetilde{p}_{Z_{i-1}^{1:N}}) \\
&\overset{(a)}{\leq} \mathbb{V}(\widetilde{p}_{E_{1:L,i}Z_{i-1}^{1:N}}, p^{unif}_{\bar{E}_{1:L}}\widetilde{p}_{Z_{i-1}^{1:N}}) \\
&\quad + \mathbb{V}(p^{unif}_{\bar{E}_{1:L}}\widetilde{p}_{Z_{i-1}^{1:N}}, \widetilde{p}_{E_{1:L,i}}\widetilde{p}_{Z_{i-1}^{1:N}}) \\
&\leq 2\mathbb{V}(\widetilde{p}_{E_{1:L,i}Z_{i-1}^{1:N}}, p^{unif}_{\bar{E}_{1:L}}\widetilde{p}_{Z_{i-1}^{1:N}}) \\
&\overset{(b)}{\leq} 2\Big(\mathbb{V}(\widetilde{p}_{E_{1:L,i}Z_{i-1}^{1:N}}, q_{G_{X_{1:L}}(X_{1:L}^{1:N})Z^{1:N}}) \\
&\quad + \mathbb{V}(q_{G_{X_{1:L}}(X_{1:L}^{1:N})Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}}q_{Z^{1:N}}) \\
&\quad + \mathbb{V}(p^{unif}_{\bar{E}_{1:L}}q_{Z^{1:N}}, p^{unif}_{\bar{E}_{1:L}}\widetilde{p}_{Z_{i-1}^{1:N}})\Big) \\
&\overset{(c)}{\leq} 2(\mathbb{V}(\widetilde{p}_{X_{1:L,i-1}^{1:N}Z_{i-1}^{1:N}}, q_{X_{1:L}^{1:N}Z^{1:N}}) + \delta^{*(0)}(N) \\
&\quad + \mathbb{V}(q_{Z^{1:N}}, \widetilde{p}_{Z_{i-1}^{1:N}})) \\
&\overset{(d)}{\leq} 4\delta^*_{i-1}(N) + 2\delta^{*(0)}(N),
\end{aligned}
$$

where (a) and (b) hold by the triangle inequality, (c) holds by the data processing inequality because $\widetilde{E}_{1:L,i} \triangleq G_{X_{1:L}}(X_{1:L,i-1}^{1:N})$ by Line 5 of Algorithm 3, and by Lemma 9, (d) holds by Lemma 10. □

Next, we show that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent of the channel outputs in Blocks 1 to $i-1$ considered jointly.

Lemma 12. *For $i \in [\![2, k]\!]$, we have*

$$
\mathbb{V}\left(\widetilde{p}_{E_{1:L,i}Z_{1:i-1}^{1:N}}, \widetilde{p}_{E_{1:L,i}}\widetilde{p}_{Z_{1:i-1}^{1:N}}\right) \leq \delta_i^{*(2)}(N),
$$

where $\delta_i^{*(2)}(N) \triangleq (2^{i-1}-1)(4\delta^*_{i-1}(N) + 2\delta^{*(0)}(N))$.

Proof. We prove the result by induction. The lemma is true for $i = 2$ by Lemma 11. Assume now that the lemma holds for $i \in [\![2, k-1]\!]$. Then, for $i \in [\![3, k]\!]$, we have

$$
\mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}E_{1:L,i}}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\widetilde{p}_{E_{1:L,i}}\right)
$$

$$
\begin{aligned}
&\overset{(a)}{\leq} \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}E_{1:L,i}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i}}\right) \\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_{1:L,i}}\right) \\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_{1:L,i}}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\widetilde{p}_{E_{1:L,i}}\right) \\
&= \mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}E_{1:L,i}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i}}\right) \\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i}}, \widetilde{p}_{Z_{i-1}^{1:N}}\widetilde{p}_{E_{1:L,i}}\right) \\
&\quad + \mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}}, \widetilde{p}_{Z_{1:i-1}^{1:N}}\right) \\
&\overset{(b)}{\leq} \delta_i^{*(1)}(N) + 2\mathbb{V}\left(\widetilde{p}_{Z_{1:i-1}^{1:N}E_{1:L,i-1:i}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i-1:i}}\right) \\
&\overset{(c)}{=} \delta_i^{*(1)}(N) + 2\mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}E_{1:L,i-1}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i}|E_{1:L,i-1}}, \right. \\
&\quad \left. \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{Z_{i-1}^{1:N}E_{1:L,i-1:i}}\right) \\
&= \delta_i^{*(1)}(N) + 2\mathbb{V}\left(\widetilde{p}_{Z_{1:i-2}^{1:N}E_{1:L,i-1}}, \widetilde{p}_{Z_{1:i-2}^{1:N}}\widetilde{p}_{E_{1:L,i-1}}\right) \\
&\overset{(d)}{\leq} \delta_i^{*(1)}(N) + 2\delta_{i-1}^{*(2)}(N),
\end{aligned}
$$

where (a) holds by the triangle inequality, (b) holds by Lemma 11, (c) holds by the Markov chain $(\widetilde{E}_{1:L,i}, \widetilde{Z}_{i-1}^{1:N}) - \widetilde{E}_{1:L,i-1} - \widetilde{Z}_{1:i-2}^{1:N}$, (d) holds by the induction hypothesis. □

The following lemmas show that the channel outputs of all the blocks are asymptotically independent, and that the target output distribution is well approximated jointly over all blocks.

Lemma 13. *We have*

$$
\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, \prod_{i=1}^{k}\widetilde{p}_{Z_i^{1:N}}\right) \leq (k-1)\delta_k^{*(2)}(N),
$$

where $\delta_k^{*(2)}(N)$ is defined in Lemma 12.

Lemma 14. *For block $i \in [\![1, k]\!]$, we have*

$$
\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, q_{Z^{1:kN}}\right) \leq (k-1)\delta_k^{*(2)}(N) + k\delta_k^{*}(N),
$$

where $\delta_k^{*(2)}(N)$ is defined in Lemma 12 and $\delta_k^*(N)$ is defined in Lemma 10.

The proofs of Lemmas 13 and 14 are similar to the proofs of Lemmas 6 and 7, respectively, and are thus omitted. Finally, the next lemma shows that the encoding scheme of Section 2.8.1 achieves the desired rate-tuple.

Lemma 15. *Let $\epsilon_0 > 0$. For k large enough and any $l \in \mathcal{L}$, we have* $\lim_{N\to+\infty} R_l = I(X_l; Z|X_{1:l-1}) + \epsilon_0 + 2\xi$.

Proof. Let k be such that for any $l \in \mathcal{L}$ we have $\frac{H(X_l)}{k} < \epsilon_0$. Then, by the definition of ϵ_2, for any $l \in \mathcal{L}$, we have

$$\begin{aligned} R_l &= \frac{\sum_{i=1}^k |E_{l,i}|}{kN} \\ &= \frac{N(H(X_l) + \epsilon_2) + (k-1)N(I(X_l; ZX_{1:l-1}) + \epsilon_2)}{kN} \\ &\leq \frac{H(X_l)}{k} + I(X_l; ZX_{1:l-1}) + \epsilon_2 \\ &\leq \epsilon_0 + I(X_l; ZX_{1:l-1}) + \epsilon_2 \\ &\xrightarrow{N\to+\infty} I(X_l; ZX_{1:l-1}) + \epsilon_0 + 2\xi. \end{aligned}$$

□

2.9 Concluding Remarks

We showed that codes for MAC resolvability can be obtained solely from source resolvability codes, used as black boxes, and two-universal hash functions. The crux of our approach is randomness recycling implemented with distributed hashing across a block-Markov coding scheme. Since explicit constructions for source resolvability codes and two-universal hash functions are known, our approach provides explicit codes to achieve the entire multiple access channel resolvability region for arbitrary channels with binary input alphabets.

APPENDICES

APPENDIX A

An explicit coding scheme for source resolvability

Let $n \in \mathbb{N}$ and $N \triangleq 2^n$. Let $G_n \triangleq \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]^{\otimes n}$ be the source polarization matrix defined in [25]. For any set $\mathcal{A} \subseteq [\![1, N]\!]$ and any sequence $X^{1:N}$, let $X^{1:N}[\mathcal{A}]$ be the components of $X^{1:N}$ whose indices are in $\mathcal{A}$. Next, consider a binary memoryless source $(\mathcal{X}, q_X)$, where $|\mathcal{X}| = 2$. Let $X^{1:N}$ be distributed according to $q_{X^{1:N}} \triangleq \prod_{i=1}^{N} q_X$, and define $A^{1:N} \triangleq G_n X^{1:N}$. Define also for $\beta < 1/2$, $\delta_N \triangleq 2^{-N^\beta}$, the sets

$$\mathcal{V}_X \triangleq \left\{ i \in [\![1, N]\!] : H(A^i | A^{1:i-1}) > 1 - \delta_N \right\},$$
$$\mathcal{H}_X \triangleq \left\{ i \in [\![1, N]\!] : H(A^i | A^{1:i-1}) > \delta_N \right\}.$$

Algorithm 4 Encoding algorithm for source resolvability

Require: A vector R of $|\mathcal{V}_X|$ uniformly distributed bits
1: Define $\widetilde{A}^{1:N}[\mathcal{V}_X] \triangleq R$
2: Define $\widetilde{A}^j$ according to $q_{A^j|A^{1:j-1}}$ for $j \in \mathcal{V}_X^c \backslash \mathcal{H}_X^c$ and as $\widetilde{A}^j \triangleq \underset{a \in \{0,1\}}{\arg\max}\, q_{A^j|A^{1:j-1}}(a|a^{1:j-1})$ for $j \in \mathcal{H}_X^c$
3: Define $\widetilde{X}^{1:N} \triangleq \widetilde{A}^{1:N} G_n$

In Algorithm 4, the distribution of $\widetilde{X}^{1:N}$ is such that $\lim_{N\to\infty} \mathbb{V}(\widetilde{p}_{X^{1:N}}, q_{X^{1:N}}) = 0$ by [26, 27]. Moreover, the rate of R is $\frac{|\mathcal{V}_X|}{N} \xrightarrow{N\to+\infty} H(X)$ by [28, Lemma 1], and the rate of randomness used in Line 2 is 0 by [14, Lemma 20]. Hence, Algorithm 4 achieves the source resolvability of $(\mathcal{X}, q_X)$.

APPENDIX B

Supporting Lemmas

A function f_X defined over a finite alphabet $\mathcal{X}$ is subnormalized non-negative if $f_X(x) \geq 0, \forall x \in \mathcal{X}$ and $\sum_{x\in\mathcal{X}} f_X(x) \leq 1$. Additionally, for a subnormalized non-negative function f_{XY} defined over a finite alphabet $\mathcal{X} \times \mathcal{Y}$, its marginals are defined as

$f_X(x) \triangleq \sum_{y\in\mathcal{Y}} f_{XY}(x,y), \forall x \in \mathcal{X}$ and $f_Y(y) \triangleq \sum_{x\in\mathcal{X}} f_{XY}(x,y), \forall y \in \mathcal{Y}$, similar to probability distributions.

Lemma 16 ([29],[30, Lemma 2]). *Define $\mathcal{A} \triangleq [\![1, A]\!]$. Let $(\mathcal{T}_a)_{a\in\mathcal{A}}$ be A finite alphabets and define for $\mathcal{S} \subseteq \mathcal{A}$, $\mathcal{T}_{\mathcal{S}} \triangleq \bigtimes_{a\in\mathcal{S}} \mathcal{T}_a$. Consider the random variables $T_{\mathcal{A}}^{1:N} \triangleq (T_a^{1:N})_{a\in\mathcal{A}}$ and $Z^{1:N}$ defined over $\mathcal{T}_{\mathcal{A}}^N \times \mathcal{Z}^N$ with probability distribution $q_{T_{\mathcal{A}}^{1:N} Z^{1:N}} \triangleq \prod_{i=1}^N q_{T_{\mathcal{A}} Z}$. For any $\epsilon > 0$, there exists a subnormalized non-negative function $w_{T_{\mathcal{A}}^{1:N} Z^{1:N}}$ defined over $\mathcal{T}_{\mathcal{A}}^N \times \mathcal{Z}^N$ such that $\mathbb{V}(q_{T_{\mathcal{A}}^{1:N} Z^{1:N}}, w_{T_{\mathcal{A}}^{1:N} Z^{1:N}}) \leq \epsilon$ and*

$$H_\infty(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}}) \geq N H(T_{\mathcal{S}}|Z) - N\delta_{\mathcal{S}}(N), \forall \mathcal{S} \subseteq \mathcal{A},$$

where $\delta_{\mathcal{S}}(N) \triangleq \log(|\mathcal{T}_{\mathcal{S}}| + 3)\sqrt{\frac{2}{N}(A - \log\epsilon)}$, and we have defined the min-entropy as in [31, 32], i.e.,

$$H_\infty(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}}) \triangleq -\log \max_{\substack{t_{\mathcal{S}}^{1:N} \in \mathcal{T}_{\mathcal{S}}^N \\ z^{1:N} \in \mathrm{supp}(q_{Z^{1:N}})}} \frac{w_{T_{\mathcal{S}}^{1:N} Z^{1:N}}(t_{\mathcal{S}}^{1:N}, z^{1:N})}{q_{Z^{1:N}}(z^{1:N})}.$$

Lemma 17 ([29],[30, Lemma 1]). *Consider a sub-normalized non-negative function $p_{X_{\mathcal{L}} Z}$ defined over $\bigtimes_{l\in\mathcal{L}} \mathcal{X}_l \times \mathcal{Z}$, where $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$ and, $\mathcal{Z}$, $\mathcal{X}_l$, $l \in \mathcal{L}$, are finite alphabets. For $l \in \mathcal{L}$, let $F_l : \{0,1\}^{n_l} \longrightarrow \{0,1\}^{r_l}$, be uniformly chosen in a family $\mathcal{F}_l$ of two-universal hash functions. Define $s_{\mathcal{L}} \triangleq \prod_{l\in\mathcal{L}} |\mathcal{F}_l|$, and for any $\mathcal{S} \subseteq \mathcal{L}$, define $r_{\mathcal{S}} \triangleq \sum_{i\in\mathcal{S}} r_i$. Define also $F_{\mathcal{L}} \triangleq (F_l)_{l\in\mathcal{L}}$ and $F_{\mathcal{L}}(X_{\mathcal{L}}) \triangleq (F_l(X_l))_{l\in\mathcal{L}}$. Then, for any q_Z defined over $\mathcal{Z}$ such that $\mathrm{supp}(q_Z) \subseteq \mathrm{supp}(p_Z)$, we have*

$$\begin{aligned} &\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}), F_{\mathcal{L}}, Z}, p_{U_{\mathcal{K}}} p_{U_{\mathcal{F}}} p_Z) \\ &\leq \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L}, \mathcal{S}\neq\emptyset} 2^{r_{\mathcal{S}} - H_\infty(p_{X_{\mathcal{S}} Z} | q_Z)}}, \end{aligned}$$

where $p_{U_{\mathcal{K}}}$ and $p_{U_{\mathcal{F}}}$ are the uniform distributions over $[\![1, 2^{r_{\mathcal{L}}}]\!]$ and $[\![1, s_{\mathcal{L}}]\!]$, respectively.

APPENDIX C

Proof of Lemma 1

The proof is similar to [20]. We have

$$\begin{aligned} I(XY;Z) &\overset{(a)}{=} I(XUV;Z) \\ &\overset{(b)}{=} I(U;Z) + I(X;Z|U) + I(V;Z|UX), \end{aligned}$$

where (a) holds because $I(XUV;Z) \geq I(XY;Z)$ since $Y = f(U,V)$, and $I(XUV;Z) \leq I(XY;Z)$ since $(X,U,V) - (X,Y) - Z$ forms a Markov chain, (b) holds by the chain rule.

We know by [20, Lemma 6] that $I(X;ZU)$ is a continuous function of ϵ, hence so is

$$R_1 = I(X;Z|U) = I(X;ZU),$$

where the last equality holds by the independence between X and U. Then, $I(X;Z)$ and $I(X;Z|Y)$ are in the image of R_1 by (3), and hence, using $I(X;Z) \leq I(X;YZ) = I(X;Z|Y)$, $[I(X;Z), I(X;Z|Y)]$ is also in the image of R_1 by continuity.

CHAPTER III

Secret Sharing Schemes from Correlated Random Variables and Rate-Limited Public Communication

We published one conference paper [33].

A Introduction

Secret sharing has first been introduced in [3] and [4]. Basic secret sharing models consist of a dealer who distributes a secret among a set of participants with the constraint 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 this work, unlike in [3, 4], we consider a secret sharing problem where noisy resources are available to the dealer and the participants. Specifically, the participants and dealer have access to samples of correlated random variables (e.g., obtained in a wireless communication network from channel gain measurements after appropriate manipulations [34, 35, 36, 37, 38]), in addition to a one-way (from the dealer to the participants), authenticated, public, and rate-limited communication channel. Such secret sharing models that rely on noisy resources have been introduced in [5] for wireless channels and in [39, 40] for source models to avoid the assumption, made in [3, 4], that individual secure channels are available for free between each participant and the dealer. Another feature of secret sharing from noisy resources is that, unlike traditional secret sharing schemes, the creation and distribution phases of the protocol are no longer restricted to be independently designed but can now be jointly designed. As a consequence, in this work, the length of each share always scales linearly with the size of the secret for any access structures. Indeed, the size of the secret is linear with the number of source observations N, and a share corresponds to the public communication plus N source observations, whose lengths are both linear with N.

A.1 Contributions

In this work, we propose the first constructive and low-complexity secret sharing scheme for source models with arbitrary access structures and rate-limited public communication.

Our construction relies on two coding layers. The first coding layer handles the reliability constraints via vector quantization to support rate-limited public communication. While constructive coding schemes exist to perform the related task of Wyner-Ziv coding, e.g., with polar codes [41], in our model we face two additional challenges: (i) one needs to precisely control the distribution output of the encoder to enable a precise analysis of the security guarantees when one combines the first coding layer with the second coding layer, (ii) unlike the standard problem of Wyner-Ziv coding, because of the presence of an access structure in our setting, the statistics of the side information available at the decoder is not fully known at the encoder but only known to belong to a given set of probability distributions. One can partially reuse a Block-Markov coding idea from [42], which considers the simpler problem of lossless source coding with compound side information, but we need to develop a novel scheme able to simultaneously perform lossy source coding with compound side information and precisely control the encoder distribution output. The second coding layer handles the security constraints via universal hashing [21]. The main difficulty is the analysis of the security guarantees after combining the first and second coding layer. Specifically, through each steps of the coding scheme, one needs to characterize the joint distributions of the random variables involved in the coding scheme.

We stress that in our construction one does *not* need any assumptions on the correlation of the random variables, e.g., symmetry or degradation assumptions on the source, and do *not* need a pre-shared secret among the participants and dealer.

As a by-product, our construction enables constructive and capacity-achieving coding schemes for the related problem of secret-key generation from correlated random variable and rate-limited one-way public communication [43]. This improves previous

known constructive and capacity-achieving coding schemes, e.g., [28], that, unlike our construction, require a pre-shared secret key to obtain strong secrecy.

A.2 Related works

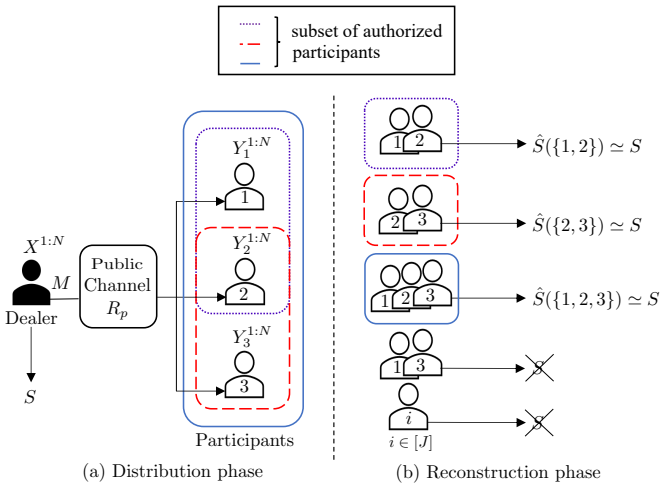
Secret sharing models with noisy resources available to the dealer and the participants have been studied for channel models [5] and source models [30, 39, 40, 44, 45] which are related to compound wiretap channels [46] and compound secret-key generation [47, 48], respectively, in that multiple reliability and security constraints need to be satisfied simultaneously. However, all these references only prove the existence of coding schemes, whereas in this work we focus on constructive coding schemes.

While no constructive coding scheme has been proposed in the literature for secret sharing source models with arbitrary access structures, several works have focused on the simpler problem of secret-key generation between two parties from correlated random variables and public communication [49], [50]. Specifically, constructive coding schemes that achieve optimal secret-key rates for this problem have been developed in the case of rate-unlimited public communication by successively handling the reliability requirement and the secrecy requirement employing source coding with side information and universal hashing, respectively [51, 52, 53]. While such methods lead to low-complexity coding schemes for unlimited public communication, their application to rate-limited public communication [54, 55] requires vector quantization for which, the construction of low-complexity schemes is challenging and has not been proposed in this context. For this reason and the fact that the secret sharing problem in this work involves more than two parties, all these previous works do not provide a constructive solution to the secret sharing problem with rate-limited public communication considered in this work. Going back to the problem of secret-key generation between two parties, another approach that jointly handles the reliability and secrecy requirements via polar codes also yields optimal secret-key rates for rate-unlimited communication [28, 56] and rate-limited communication [28]. However, these works do not seem to easily extend to the secret

sharing problem in this work because, for arbitrary source correlations, [28, 56] only consider two parties, and in the case of rate-limited public communication, [28] requires a pre-shared secret between the users. While this pre-shared secret has a negligible rate in [28], such a resource is forbidden in this work. Finally, note that constructive coding schemes for secret-key generation involving more than two parties have also been proposed in [28, 57, 58, 59] but only when the correlations of the random variables observed by the participants have specific structures. Hence, these works cannot be applied to our setting as we consider a source with arbitrary correlations. Finally, note that a recent result provides constructive coding schemes for secret sharing channel models with arbitrary access structures [60]. But, again, the coding scheme in [60] cannot be applied to our setting as, here, public communication is rate-limited and requires vector quantization.

B Notation

For $a, b \in \mathbb{R}$, define $[a] \triangleq [1, \lceil a \rceil] \cap \mathbb{N}$, $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$, and $[a]^+ \triangleq \max(0, a)$. The components of a vector $X^{1:N}$ of length $N \in \mathbb{N}$ are denoted with superscripts, i.e., $X^{1:N} \triangleq (X^1, X^2, \ldots, X^N)$. For any set $\mathcal{A} \subset [N]$, let $X^{1:N}[\mathcal{A}]$ be the components of $X^{1:N}$ whose indices are in $\mathcal{A}$. For two probability distributions p_X and q_X defined over the same alphabet $\mathcal{X}$, define the relative entropy between p_X and q_X as $\mathbb{D}(p_X \| q_X) \triangleq \sum_{x \in \mathcal{X}} p_X(x) \log \frac{p_X(x)}{q_X(x)}$, and define the variational distance between p_X and q_X as $\mathbb{V}(p_X, q_X) \triangleq \sum_{x \in \mathcal{X}} |p_X(x) - q_X(x)|$. For two joint probability distributions p_{XY} and q_{XY}, both defined over $\mathcal{X} \times \mathcal{Y}$, define the conditional relative entropy between $p_{Y|X}$ and $q_{Y|X}$ as $\mathbb{D}(p_{Y|X} \| q_{Y|X}) \triangleq \sum_{x \in \mathcal{X}} p_X(x) \sum_{y \in \mathcal{Y}} p_{Y|X}(y|x) \log \frac{p_{Y|X}(y|x)}{q_{Y|X}(y|x)}$. For a probability distribution p_X defined over the alphabet $\mathcal{X}$, define $\mu_{p_X} \triangleq \min_{x \in \mathcal{X}} p_X(x)$. For a set $\mathcal{S}$, let $2^{\mathcal{S}}$ denote the power set of $\mathcal{S}$. In this work, all the logarithms are taken base two. Finally, let $\times$ denote the Cartesian product.



(a) Distribution phase (b) Reconstruction phase

Figure 4: Source $((\mathcal{X} \times \mathcal{Y}_j)_{j\in[3]}, (p_{XY_j})_{j\in[3]})$, access structure $\mathbb{A} \triangleq \{\{1,2\},\{2,3\},\{1,2,3\}\}$, $\mathbb{U} \triangleq 2^{[J]}\backslash\mathbb{A} = \{\{1,3\},\{1\},\{2\},\{3\}\}$. Dashed, dotted, and solid contour lines represent subsets of participants that are authorized to reconstruct the secret.

C Problem Statement

Consider a dealer and J participants. Let $\mathcal{Y}_{[J]} \triangleq \bigtimes_{j\in[J]} \mathcal{Y}_j$ be the Cartesian product of J finite alphabets $(\mathcal{Y}_j)_{j\in[J]}$. Consider a discrete memoryless source $(\mathcal{X} \times \mathcal{Y}_{[J]}, p_{XY_{[J]}})$ with $\mathcal{X} \triangleq \{0,1\}$. Let $\mathbb{A}$ be a set of subsets of $[J]$ such that for any $\mathcal{T} \subseteq [J]$, if $\mathcal{T}$ contains a set that belongs to $\mathbb{A}$, then $\mathcal{T}$ also belongs to $\mathbb{A}$, i.e., $\mathbb{A}$ is a monotone access structure [61]. We also define $\mathbb{U} \triangleq 2^{[J]}\backslash\mathbb{A}$ as the set of all colluding subsets of users who must not learn any information about the secret. In the following, for any $\mathcal{U} \in \mathbb{U}$ and $\mathcal{A} \in \mathbb{A}$, we use the notation $Y_{\mathcal{U}}^{1:N} \triangleq (Y_j^{1:N})_{j\in\mathcal{U}}$ and $Y_{\mathcal{A}}^{1:N} \triangleq (Y_j^{1:N})_{j\in\mathcal{A}}$. Moreover, we assume that the dealer can communicate with the participants over an authenticated, one-way, rate-limited, noiseless, and public communication channel.

Definition 6. *A $(2^{NR_s}, R_p, \mathbb{A}, N)$ secret sharing scheme consists of:*

- *A public message alphabet $\mathcal{M} \triangleq [2^{NR_p}]$;*
- *An alphabet $\mathcal{S} \triangleq [2^{NR_s}]$;*
- *An encoding function $f : \mathcal{X}^N \to \mathcal{M}$;*
- *An encoding function $h : \mathcal{X}^N \to \mathcal{S}$;*

- $|\mathbb{A}|$ *decoding functions* $g_{\mathcal{A}} : \mathcal{M} \times \mathcal{Y}_{\mathcal{A}}^N \to \mathcal{S}$ *for any* $\mathcal{A} \in \mathbb{A}$*;*

and operates as follows

1. *The dealer observes* $X^{1:N}$ *and Participant* $j \in [J]$ *observes* $Y_j^{1:N}$*;*
2. *The dealer transmits* $M \triangleq f(X^{1:N}) \in \mathcal{M}$ *over the public communication channel;*
3. *The dealer computes the secret* $S \triangleq h(X^{1:N}) \in \mathcal{S}$*;*
4. *Any subset of participants* $\mathcal{A} \in \mathbb{A}$ *can compute an estimate of* S *as* $\hat{S}(\mathcal{A}) \triangleq g_{\mathcal{A}}(M, Y_{\mathcal{A}}^{1:N})$.

Definition 7. *A rate pair* (R_p, R_s) *is achievable if there exists a sequence of* $(2^{NR_s}, R_p, \mathbb{A}, N)$ *secret sharing schemes such that*

$$\lim_{N\to+\infty} \max_{\mathcal{A}\in\mathbb{A}} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = 0, \quad (\textit{Reliability}) \tag{22}$$

$$\lim_{N\to+\infty} \max_{\mathcal{U}\in\mathbb{U}} I(S; MY_{\mathcal{U}}^{1:N}) = 0, \quad (\textit{Strong Security}) \tag{23}$$

$$\lim_{N\to+\infty} \log|\mathcal{S}| - H(S) = 0. \quad (\textit{Secret Uniformity}) \tag{24}$$

(22) *means that any subset of participants in* $\mathbb{A}$ *is able to recover the secret,* (23) *means that any subset of participants in* $\mathbb{U}$ *cannot obtain information about the secret, while* (24) *means that the secret is nearly uniform. The secret capacity is defined as* $C_s(R_p) \triangleq \sup\{R_s : (R_p, R_s) \textit{ is achievable}\}$.

The setting is illustrated in Figure 4 for $J = 3$ participants and $\mathbb{A} \triangleq \{\{1,2\},\{2,3\},\{1,2,3\}\}$.

D Main Results

Theorem 6. *The secret rate*

$$R_s = \max_{\substack{U \\ U-X-Y_{[J]}}} \left[\min_{\mathcal{A}\in\mathbb{A}} I(U; Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(U; Y_{\mathcal{U}})\right]^+$$

$$\textit{subject to} \quad R_p \geq \max_{\mathcal{A}\in\mathbb{A}} I(U;X|Y_{\mathcal{A}}) \tag{25}$$

is achievable with an encoder and decoders that operate over k blocks of source observation sequences of length N, and have complexity $O(\mathbb{C}(kN))$, where $\mathbb{C}(kN)$ is the complexity of field multiplication in $GF(2^{kN})$.

Theorem 7. *The secret rate*

$$R_s = \max_{\substack{U,V \\ U-V-X-Y_{[J]}}} \left[\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}|U) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}|U)\right]^+$$
$$\textit{subject to } R_p \geq \max_{\mathcal{A}\in\mathbb{A}} I(U;X|Y_{\mathcal{A}}) + \max_{\mathcal{A}\in\mathbb{A}} I(V;X|UY_{\mathcal{A}}) \tag{26}$$

is achievable with an encoder and decoders that operate over k blocks of source observation sequences of length N, and have complexity $O(\mathbb{C}(kN))$.

Note that the achievable rates in Theorems 6 and 7 could be obtained from [47]. However, [47] only provides an existence result and not a constructive coding scheme to achieve these rates.

Next, we have the following corollary for rate-unlimited public communication when all the participants are needed to reconstruct the secret, i.e., any strict subsets of participants in $[J]$ must not learn any information about the secret.

Corollary 2. *When $R_p = +\infty$ and $\mathbb{A} = \{[J]\}$, the secret capacity*

$$\lim_{R_p\to+\infty} C_s(R_p) = \min_{\mathcal{U}\subsetneq[J]} I(X;Y_{[J]}|Y_{\mathcal{U}})$$

is achievable with an encoder and decoders that operate over k blocks of source observation sequences of length N, and have complexity $O(\mathbb{C}(kN))$.

Proof. The achievability follows from Theorem 6, the Markov Chains $X - Y_{[J]} - Y_{\mathcal{U}}, \mathcal{U} \in \mathbb{U}$, and because $\mathbb{U} = \{\mathcal{S} \subseteq [J] : |\mathcal{S}| < J\}$. The converse follows from [49, 50]. □

One main feature of secret sharing from correlated randomness, compared to

traditional secret sharing, is that one does not assume the availability at no cost of perfectly secure communication channels between each participant and the dealer. Specifically, the amount of randomness shared through the source observations at the participants and the dealer quantifies this cost.

E Auxiliary result

In this section, we use the same notation as in Section C and provide an auxiliary result to construct a coding scheme for the secret sharing problem described in Section C. Specifically, we consider a setting similar to the one in Section C with the following modifications. Instead of considering the constraints (22), (23), and (24), the dealer creates a quantized version $\widetilde{U}^{1:N}$ of the source observations $X^{1:N}$, with the requirements that (i) $\widetilde{U}^{1:N}$ follows a pre-determined product distribution, and (ii) any subsets of participants in the access structure can reconstruct $\widetilde{U}^{1:N}$. Next, we formalize this problem statement and construct a coding scheme for this setting.

Consider a discrete memoryless source $((\mathcal{X} \times \mathcal{Y}_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}}, (p_{XY_{\mathcal{A}}})_{\mathcal{A}\in\mathbb{A}})$ with $\mathcal{X} \triangleq \{0,1\}$. Define the joint probability distribution $p_{XUY_{\mathcal{A}}} \triangleq p_{XY_{\mathcal{A}}} p_{U|X}$, $\mathcal{A} \in \mathbb{A}$. For any $\mathcal{A} \in \mathbb{A}$, let $(X^{1:N}, U^{1:N}, Y_{\mathcal{A}}^{1:N})$ be distributed according to the joint probability distribution $p_{X^{1:N}U^{1:N}Y_{\mathcal{A}}^{1:N}} \triangleq \prod_{i=1}^{N} p_{XUY_{\mathcal{A}}}$.

Definition 8. *A $(2^{NR_M}, N)$ code for a source model $((\mathcal{U} \times \mathcal{X} \times \mathcal{Y}_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}}, (p_{UXY_{\mathcal{A}}})_{\mathcal{A}\in\mathbb{A}})$ consists of*

- *An alphabet $\mathcal{M} \triangleq [2^{NR_M}]$;*
- *An encoding function $f : \mathcal{X}^N \to \mathcal{U}^N \times \mathcal{M}$, where $|\mathcal{U}| = 2$;*
- *$|\mathbb{A}|$ decoding functions $g_{\mathcal{A}} : \mathcal{M} \times \mathcal{Y}_{\mathcal{A}}^N \to \mathcal{U}^N$ for any $\mathcal{A} \in \mathbb{A}$;*

and operates as follows:

1. *The dealer observes $X^{1:N}$ and Participant $j \in [J]$ observes $Y_j^{1:N}$;*

2. *The dealer encodes* $X^{1:N}$ *with* f *to form a vector quantized version* $\widetilde{U}^{1:N}$ *of* $X^{1:N}$ *and a message* M*, where* $(\widetilde{U}^{1:N}, M) \triangleq f(X^{1:N})$*. Let the joint probability distribution of* $(\widetilde{U}^{1:N}, X^{1:N})$ *be denoted by* $\widetilde{p}_{U^{1:N}X^{1:N}}$*;*

3. *The dealer transmits* M *to the participants over the public channel;*

4. *Any subset of participants* $\mathcal{A} \in \mathbb{A}$ *can create* $\hat{U}_{\mathcal{A}}^{1:N} \triangleq g_{\mathcal{A}}(M, Y_{\mathcal{A}}^{1:N})$*, an estimate of* $\widetilde{U}^{1:N}$*.*

Definition 9. *A rate* R_M *is achievable for a source model* $((\mathcal{U} \times \mathcal{X} \times \mathcal{Y}_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}}, (p_{UXY_{\mathcal{A}}})_{\mathcal{A}\in\mathbb{A}})$ *if there exists a sequence of* $(2^{NR_M}, N)$ *codes such that*

$$\lim_{N\to+\infty} \max_{\mathcal{A}\in\mathbb{A}} \mathbb{P}[\hat{U}_{\mathcal{A}}^{1:N} \neq \widetilde{U}^{1:N}] = 0, \tag{27}$$

$$\lim_{N\to+\infty} \mathbb{D}(\widetilde{p}_{U^{1:N}X^{1:N}} \| p_{U^{1:N}X^{1:N}}) = 0. \tag{28}$$

Note that the problem described in Definitions 8 and 9 is a generalization of the problem of lossless source coding where the encoder output distribution must follow a given distribution [62, 63, 64].

Theorem 8. *For any* $\epsilon, \delta > 0$*, there exist* $k, n_0 \in \mathbb{N}$ *such that for any* $n \geq n_0$ *and* $N \triangleq 2^n$*, there exists an encoder*

$$f : \mathcal{X}^{kN} \to \mathcal{U}^{kN} \times \mathcal{M}, \tag{29}$$

and $|\mathbb{A}|$ *decoders*

$$g_{\mathcal{A}} : \mathcal{M} \times \mathcal{Y}_{\mathcal{A}}^{kN} \to \mathcal{U}^{kN}, \forall \mathcal{A} \in \mathbb{A},$$

such that the public communication rate satisfies

$$R_M \leq \max_{\mathcal{A}\in\mathbb{A}} I(U; X|Y_{\mathcal{A}}) + \delta, \tag{30}$$

the probability of error at Decoder $\mathcal{A} \in \mathbb{A}$ *satisfies*

$$\mathbb{P}[g_{\mathcal{A}}(M, Y_{\mathcal{A}}^{1:kN}) \neq \widetilde{U}^{1:kN}] < \epsilon, \forall \mathcal{A} \in \mathbb{A}, \tag{31}$$

where $X_{1:k}^{1:N} \triangleq (X_i^{1:N})_{i\in[k]}$ *is the source observation at the encoder with* $X_i^{1:N}$, $i \in [k]$, *a sequence of length* N, $Y_{\mathcal{A},1:k}^{1:N} \triangleq (Y_{\mathcal{A},i}^{1:N})_{i\in[k]}$ *is the source observation at Decoder* $\mathcal{A} \in \mathbb{A}$ *with* $Y_{\mathcal{A},i}^{1:N}$, $i \in [k]$, *a sequence of length* N, $p_{X_{1:k}^{1:N} Y_{\mathcal{A},1:k}^{1:N}} \triangleq \prod_{i=1}^{kN} p_{XY_{\mathcal{A}}}$, $\mathcal{A} \in \mathbb{A}$, *and* $(\widetilde{U}_{1:k}^{1:N}, M) \triangleq f(X_{1:k}^{1:N})$. *The probability distribution induced by the encoding scheme* $\widetilde{p}_{U_i^{1:N} X_i^{1:N}}, i \in [k]$ *also satisfies*

$$\mathbb{D}\left(\widetilde{p}_{U_i^{1:N} X_i^{1:N}} \left\| p_{U^{1:N} X^{1:N}} \right.\right) \leq N\delta_N, \tag{32}$$

where

$$\delta_N \triangleq 2^{-N^\beta}, \beta \in]0, \tfrac{1}{2}[. \tag{33}$$

Moreover, the complexity of the encoder and decoders is $O(kN \log N)$.

F Application to secret-key generation

Our framework enables a constructive and capacity-achieving coding scheme for the problem of secret-key generation under one-way rate-limited public communication between two parties in the presence or absence of an eavesdropper. The secret-key capacities in these settings have been established in [43] via non-constructive proofs and are reviewed next.

Theorem 9 ([43, Th. 2.4])**.** *The one-way secret-key capacity under rate-limited public communication* $R_p > 0$ *and in the absence of an eavesdropper is*

$$\max_{\substack{U \\ U-X-Y}} I(Y;U) \text{ subject to } R_p \geq I(U;X) - I(U;Y).$$

Theorem 10 ([43, Th. 2.6])**.** *The one-way secret-key capacity under rate-limited public communication $R_p > 0$ and the presence of an eavesdropper is*

$$\max_{\substack{U \\ U-V-X-(Y,Z)}} [I(Y;V|U) - I(Z;V|U)]^+ \text{ subject to}$$

$$R_p \geq I(V;X) - I(V;Y).$$

By Theorem 7, the secret-key capacities in Theorems 9 and 10 are achievable with an encoder and decoders that operate over t blocks of source observation sequences of length N and have complexity $O(\mathbb{C}(tN))$.

G Concluding Remarks

We considered secret sharing from correlated random variables and rate-limited public communication. For this problem, we proposed the first constructive and low-complexity coding scheme able to handle arbitrary access structures. Our construction relies on a vector quantization coupled with distribution approximations to handle the reliability constraints, followed by universal hashing to handle the security constraints. We stress that our coding scheme does not require symmetry or degradation assumptions on the correlated random variables, and does not need a pre-shared secret among the participants and dealer. Our result is optimal in the special case of rate-unlimited public communication when all the participants are needed to reconstruct the secret. As a by-product, our construction enables improved capacity-achieving coding schemes for a secret-key generation that do not require a pre-shared secret between legitimate users.

CHAPTER III

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

We published one conference paper [65].

A Introduction

[3] and [4] 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 [66] 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. Subsequently, with the goal to avoid this assumption, secret sharing schemes from noisy resources have been studied for channel models [5] and source models [39, 40, 67], where no secure communication links are available between the dealer and the participants. Another feature of secret sharing from noisy resources is that, unlike traditional secret sharing schemes, the creation and distribution phases of the protocol are no longer restricted to being independently designed but can now be jointly designed.

A.1 Overview of the model studied in this work

We consider the secret sharing model of [5] 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 can 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 [3, 4, 68, 69].

A.2 Contributions

a) *Optimal coding scheme design in the asymptotic regime:* The secret sharing capacity has been established in [5] 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 through the use of hash functions, which is particularly useful to handle an access structure and, in particular, to ensure security against multiple subsets of colluding users that are associated with different channel statistics, (c) guidelines for a practical code design at finite blocklength as discussed next.

b) *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, information leakage is defined as the mutual information between the secret and the channel output observations for unauthorized sets of users. Note that, even for small values of n, this information leakage estimation is challenging with standard techniques such as binning of the probability space [70], k-nearest neighbor statistics [71], or maximum likelihood estimation [72], we thus evaluate the information leakage by using the mutual information neural estimator (MINE) from [73]. Our simulation results demonstrate a precise control of the probability of error and leakage thanks to the two separate coding layers.

A.3 Related works

1) *Related works on compound wiretap channels:*

   a) *Theoretical and non-constructive results*: The compound wiretap channel [46, 74] is a generalization of Wyner's wiretap channel [75] 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 [5] 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 [5], one of our contributions (see Section A.2) is to show the optimality of a two-layer coding scheme design.

   b) *Results on code constructions*: Explicit compound wiretap codes have been proposed for discrete memoryless channels for the asymptotic blocklength regime in [76]. Finite-length code constructions for scalar Gaussian compound channels have been studied in [77]. In contrast, in this work, one of our contributions (see Section A.2) 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) *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., [78, 79, 80, 81, 82, 83, 84, 85], we focus our discussion on works that, similar to our work, consider an information-theoretic security metric.

   a) *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 [86], [87], and the Gaussian wiretap channel in [88]. The above references consider the asymptotic blocklength regime.

   One of our contributions (see Section A.2) is to not only generalize the result in [88] to a compound setting but also to generalize it to vector, rather than scalar, Gaussian channel outputs.

   Note that other coding schemes based on LDPC codes [89, 90, 91], polar codes [92, 93, 94, 95], or random lattice codes [96] have been proposed for degraded or symmetric wiretap channel models, and constructive [97, 98, 99] and random [100] polar coding schemes have been proposed to achieve the secrecy capacity of non-degraded discrete wiretap channels. Coding schemes that combine polar codes and invertible extractors have also been proposed to avoid the need for a pre-shared secret under strong secrecy [101, 102]. However, only [101] considers a compound setting (for discrete memoryless wiretap channels), and none of the references above consider compound Gaussian wiretap channels, as it is needed for the secret sharing model we consider.

   b) *Code construction in the non-asymptotic regime*: Punctured systematic irregular LDPC codes have been proposed for the binary phase-shift-keyed-constrained Gaussian wiretap channel in [103], and LDPC codes for the Gaussian wiretap

channel have also been developed in [104]. Randomized Reed-Muller codes have been proposed for the Gaussian wiretap channel in [105]. Coding scheme designs based on feed-forward neural network autoencoders have also been proposed in [106], where the security and reliability constraints are handled jointly, and in [107], where the security and reliability constraints are handled separately. As discussed in Section A.2, 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.

B 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., $X^n \triangleq (X_1, X_2, \ldots, X_n)$. $\|.\|$ denotes the Euclidean norm and $\|.\|_1$ denotes the L^1 norm.

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

$$Y_j^n \triangleq X^n + N_j^n, \quad \forall j \in \mathcal{J}, \tag{34}$$

where X^n is the signal transmitted by the dealer with the power constraint

$$\frac{1}{n} \sum_{i=1}^{n} X_i^2 \leq P, \tag{35}$$

Y_j^n is the channel observation at Participant $j \in \mathcal{J}$, 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

$$Y_{\mathcal{A}}^n \triangleq \mathbf{1}_t X^n + N_{\mathcal{A}}^n, \quad \mathcal{A} \in \mathbb{A}_t, \tag{36}$$

$$Y_{\mathcal{U}}^n \triangleq \mathbf{1}_z X^n + N_{\mathcal{U}}^n, \quad \mathcal{U} \in \mathbb{U}_z, \tag{37}$$

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 $\Sigma_{\mathcal{A}} \triangleq \mathrm{diag}((\sigma_j^2)_{j\in\mathcal{A}})$ and $\Sigma_{\mathcal{U}} \triangleq \mathrm{diag}((\sigma_j^2)_{j\in\mathcal{U}})$, respectively.

Definition 10. *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 qualified 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 $\hat{S}(\mathcal{A}) \triangleq g_{\mathcal{A}}(Y_{\mathcal{A}}^n)$.*

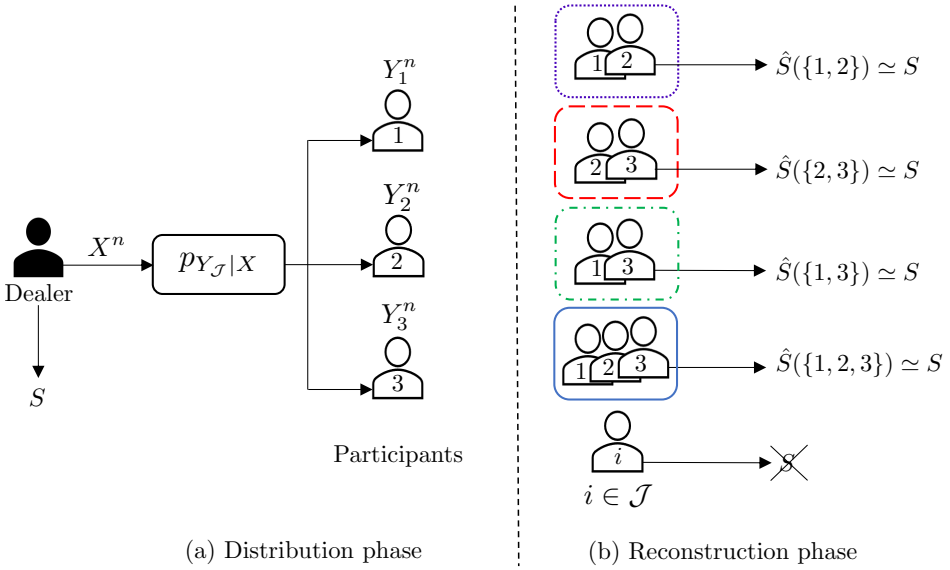
Definition 11. *A secret sharing rate R_s is achievable if there exists a sequence of*

$(2^{nR_s}, t, z, n)$ *secret sharing strategies such that*

$$\lim_{n\to+\infty} \max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = 0, \qquad (\textit{Reliability}) \tag{38}$$

$$\lim_{n\to+\infty} \max_{\mathcal{U}\in\mathbb{U}_z} I(S; Y_{\mathcal{U}}^n) = 0. \qquad (\textit{Security}) \tag{39}$$

(38) *means that any subset of at least* t *participants is able to recover the secret, and* (39) *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.*



(a) Distribution phase (b) Reconstruction phase

Figure 5: The access structure is defined by $\mathbb{A}_{t=2} \triangleq \{\{1,2\},\{2,3\},\{1,3\},\{1,2,3\}\}$ and $\mathbb{U}_{z=1} \triangleq \{\{1\},\{2\},\{3\}\}$, meaning that any two participants can reconstruct the secret, and any individual participant cannot learn any information about the secret.

The setting is illustrated in Figure 5 for the special case $\mathcal{J} = [3]$, $t = 2$, and $z = 1$. 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 11 (Adapted from [5]). *The secret sharing capacity is given by*

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

C Main results

C.1 Optimality of two-layer coding scheme in the asymptotic regime

We first introduce two-layer coding schemes in Definition 12.

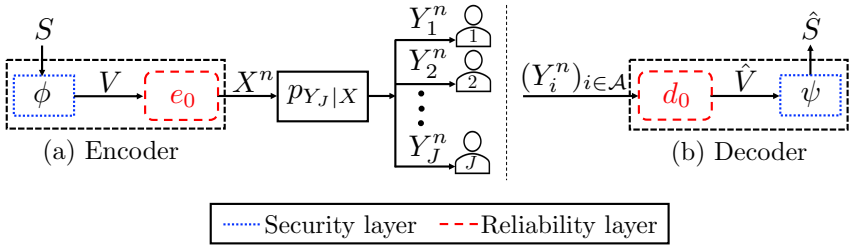


Figure 6: Two-layer code design. The reliability layer is implemented using a channel code (e_0, d_0) without any security constraints, and the security layer is implemented using the functions ψ and ϕ.

Definition 12. *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 (36) such that if $X^n \triangleq e_0(V)$ is the channel input, where V is uniformly distributed over $\{0,1\}^r$ 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

$$e : \mathcal{S} \to \mathbb{R}^n$$
$$s \mapsto e_0\left(\phi(s)\right).$$

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*

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

The architecture of a two-layer coding scheme, as described in Definition 12, is depicted in Figure 6.

Theorem 12. *There exists a two-layer secret sharing scheme, as in Definition 12, that achieves the secret sharing capacity C_s. A two-layer secret sharing scheme that achieves C_s is presented in Section D, and its analysis is provided in Section E.*

C.2 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 12. As detailed in Section F.1, 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 F.2, 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), $\mathrm{SNR} = -16\mathrm{dB}$.

Figure 7 shows the information leakage $\max_{\mathcal{U} \in \mathbb{U}_z} I(S; Y_{\mathcal{U}}^n)$ 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 7 confirms the intuition that the information leakage increases as the secret rate increases. Figure 8

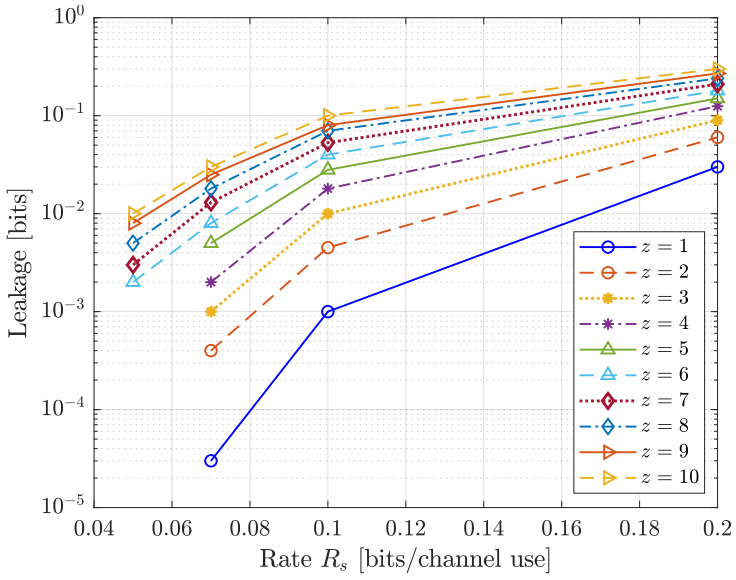


Figure 7: Information leakage $\max_{\mathcal{U}\in\mathbb{U}_z} I(S;Y_{\mathcal{U}}^n)$ versus secret sharing rate $R_s = \frac{k}{n}$ for $z \in [10]$.

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 $n \in \{5, 10, 15, 20\}$. We see the average probability of error decreases as the secret rate increases for fixed k and SNR by our code construction.

D A two-layer coding scheme

In Section D.1, we reduce the Gaussian vector channel outputs to Gaussian scalar channel outputs using sufficient statistics [108]. In Section D.2, we describe a two-layer coding scheme.

D.1 Sufficient statistics

Using Lemma 18 below, we will prove in Section E that there is no loss of generality in considering the following Equations (40) and (41) as channel model instead of (36) and (37).

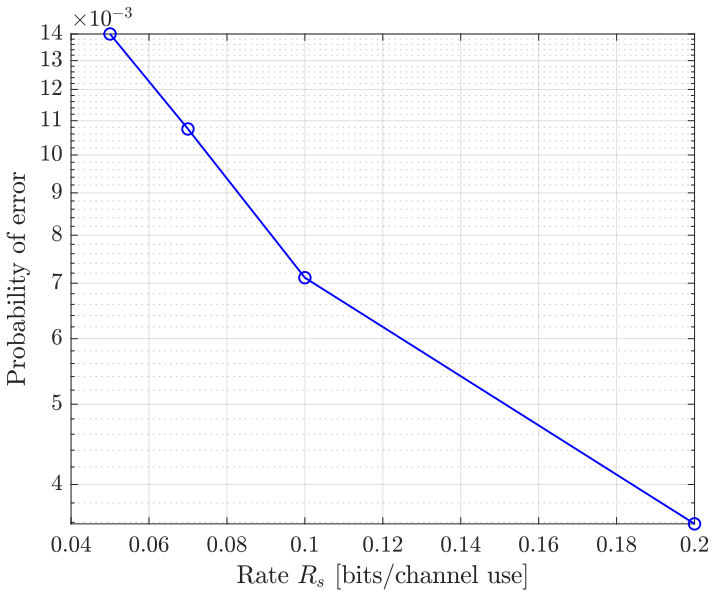


Figure 8: Probability of error $\max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S]$ versus secret sharing rate $R_s = \frac{k}{n}$.

Hence, in this section, we consider the following channel model: For any $i \in [n]$,

$$\tilde{Y}_{\mathcal{A},i} \triangleq \sigma^2_{\tilde{Y}_{\mathcal{A}}} X_i + \tilde{N}_{\mathcal{A},i}, \quad \mathcal{A} \in \mathbb{A}_t, \tag{40}$$

$$\tilde{Y}_{\mathcal{U},i} \triangleq \sigma^2_{\tilde{Y}_{\mathcal{U}}} X_i + \tilde{N}_{\mathcal{U},i}, \quad \mathcal{U} \in \mathbb{U}_z, \tag{41}$$

where

$$\sigma^2_{\tilde{Y}_{\mathcal{A}}} \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}}^{-1} \mathbf{1}_t, \tag{42}$$

$$\sigma^2_{\tilde{Y}_{\mathcal{U}}} \triangleq \mathbf{1}_z^T \Sigma_{\mathcal{U}}^{-1} \mathbf{1}_z, \tag{43}$$

$$\tilde{N}_{\mathcal{A},i} \triangleq \mathbf{1}_t^T \Sigma_{\mathcal{A}}^{-1} N_{\mathcal{A},i} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y}_{\mathcal{A}}}), \tag{44}$$

$$\tilde{N}_{\mathcal{U},i} \triangleq \mathbf{1}_z^T \Sigma_{\mathcal{U}}^{-1} N_{\mathcal{U},i} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y}_{\mathcal{U}}}). \tag{45}$$

Lemma 18 ([109, 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

$$\tilde{Y}_{\mathcal{S}} = \mathbf{1}_{|\mathcal{S}|}^T \Sigma_{\mathcal{S}}^{-1} Y_{\mathcal{S}}, \quad \mathcal{S} \subset \mathcal{J}.$$

D.2 Coding scheme

We first describe the reliability layer and secrecy layer in Sections D.2 and D.2, respectively. Then, in Section D.2, we describe the encoding and decoding of our proposed secret sharing scheme.

a) *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

$$\lim_{n\to\infty} \frac{r}{n} = \frac{1}{2} \min_{\mathcal{A}\in\mathbb{A}_t} \log\left(1 + \sigma^2_{\tilde{Y}_{\mathcal{A}}} P\right), \tag{46}$$

such that if V is uniformly distributed over $\{0,1\}^r$ and $e_0(V)$ is sent over the channel described by (40), then

$$\lim_{n\to+\infty} \max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[d_0(\tilde{Y}^n_{\mathcal{A}})) \neq V] = 0. \tag{47}$$

b) *Secrecy layer*: We first review the definition of two-universal hash functions.

Definition 13 ([21], [51])**.** *A family $\mathcal{F}$ of two-universal hash functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^k\}$ is such that*

$$\forall x, x' \in \{0,1\}^n, x \neq x' \Rightarrow \mathbb{P}[F(x) = F(x')] \leq 2^{-k}, \tag{48}$$

where F is a function uniformly chosen in $\mathcal{F}$.

Define $\mathcal{L} \triangleq \{0,1\}^r \backslash \{\mathbf{0}\}$, and consider the two-universal hash family of functions

$\mathcal{P} \triangleq \{v \mapsto \psi(\lambda, v)\}_{\lambda \in \mathcal{L}}$, where ψ is defined as

$$\begin{aligned} \psi : \mathcal{L} \times \{0,1\}^r &\to \{0,1\}^k \\ (\lambda, v) &\mapsto (\lambda \odot v)_k, \end{aligned} \tag{49}$$

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

$$\begin{aligned} \phi : \mathcal{L} \times \{0,1\}^k \times \{0,1\}^{r-k} &\to \{0,1\}^r \\ (\lambda, s, b) &\mapsto \lambda^{-1} \odot (s \| b), \end{aligned} \tag{50}$$

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

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

E Coding scheme analysis

In Sections E.1, E.2, and E.3, we analyze the security, rate, and reliability, respectively, of the coding scheme of Section D. We also discuss the seed sharing process in Section E.4.

E.1 Analysis of secrecy

We first present two supporting lemmas needed for the secrecy analysis in Section E.1. We then perform the leakage analysis in Section E.1.

a) *Supporting lemmas*: For any $v \in \mathcal{V} \triangleq \{0,1\}^r$, $\delta > 0$, $\mathcal{U} \in \mathbb{U}_z$, define

$$t(v) \triangleq \sigma^2_{\tilde{Y}_{\mathcal{U}}} e_0(v), \tag{51}$$

$$r_{t(v)} \triangleq \sqrt{(n\sigma^2_{\tilde{Y}_{\mathcal{U}}} + \|t(v)\|^2)(1+\delta)}. \tag{52}$$

Denote the ball of radius $r_{t(v)}$ in $\mathbb{R}^n$ as

$$\beta_n(r_{t(v)}) \triangleq \left\{ y^n \in \mathbb{R}^n : \|y^n\| \leq r_{t(v)} \right\}, \tag{53}$$

and the spherical shell

$$\mathbb{T}(v) \triangleq \left\{ y^n \in \mathbb{R}^n : n\sigma^2_{\tilde{Y}_{\mathcal{U}}}(1-\delta) \leq \|y^n - t(v)\|^2 \leq n\sigma^2_{\tilde{Y}_{\mathcal{U}}}(1+\delta) \right\}. \tag{54}$$

In the following, for any $\mathcal{U} \in \mathbb{U}_z$, let also $p_{SV\tilde{Y}^n_{\mathcal{U}}\Lambda}$ denote the probability distribution induced by the coding scheme of Section D. Note that

$$p_{SV\tilde{Y}^n_{\mathcal{U}}\Lambda} = p_{\tilde{Y}^n_{\mathcal{U}}|V} p_V p_{S\Lambda|\tilde{Y}^n_{\mathcal{U}}V},$$

where p_V is the uniform distributions over $\{0,1\}^r$.

Lemma 19. *For any $\mathcal{U} \in \mathbb{U}_z$, define $q_{SV\tilde{Y}^n_{\mathcal{U}}\Lambda} \triangleq q_{\tilde{Y}^n_{\mathcal{U}}|V} q_{S|V\Lambda} q_V q_\Lambda$, where q_V and q_Λ are the uniform distributions over $\{0,1\}^r$ and $\{0,1\}^r \backslash \{\mathbf{0}\}$, respectively, and for any $y^n \in \mathbb{R}^n$, $v \in \{0,1\}^r$, $s \in \mathcal{S}$, $\lambda \in \{0,1\}^r \backslash \{\mathbf{0}\}$,*

$$q_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v) \triangleq \mathbb{1}\left\{ y^n \in \mathbb{T}(v) \cap \beta_n(r_{t(v)}) \right\} \times p_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v), \tag{55}$$

$$q_{S|V\Lambda}(s|v,\lambda) \triangleq \mathbb{1}\left\{ s = (\lambda \odot v)_k \right\}. \tag{56}$$

Then, for any $\delta \in]0, 1/2[$, we have

$$\left\| p_{SV\tilde{Y}^n_{\mathcal{U}}\Lambda} - q_{SV\tilde{Y}^n_{\mathcal{U}}\Lambda} \right\|_1 \leq \delta^{(0)}(n),$$

where $\delta^{(0)}(n) \triangleq 4e^{\frac{-n\delta^2}{6}} + e^{-\frac{n}{4}\left(\sqrt{\delta+1}-1\right)^2}$.

Proof. We have

$$
\begin{aligned}
&\left\|p_{SV\tilde{Y}_{\mathcal{U}}^n\Lambda} - q_{SV\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \\
&\overset{(a)}{=} \left\|p_{\tilde{Y}_{\mathcal{U}}^n|V}p_V p_{S\Lambda|\tilde{Y}_{\mathcal{U}}^n V} - q_{\tilde{Y}_{\mathcal{U}}^n|V}q_{S|V\Lambda}q_V q_\Lambda\right\|_1 \\
&\overset{(b)}{\leq} \left\|p_{\tilde{Y}_{\mathcal{U}}^n|V}p_V p_{S\Lambda|\tilde{Y}_{\mathcal{U}}^n V} - q_{\tilde{Y}_{\mathcal{U}}^n|V}p_V p_{S\Lambda|\tilde{Y}_{\mathcal{U}}^n V}\right\|_1 + \left\|q_{\tilde{Y}_{\mathcal{U}}^n|V}p_V p_{S\Lambda|\tilde{Y}_{\mathcal{U}}^n V} - q_{\tilde{Y}_{\mathcal{U}}^n|V}q_{S|V\Lambda}q_V q_\Lambda\right\|_1 \\
&\overset{(c)}{=} \left\|p_{\tilde{Y}_{\mathcal{U}}^n|V}p_V - q_{\tilde{Y}_{\mathcal{U}}^n|V}p_V\right\|_1 + \left\|p_V p_{S\Lambda|V} - q_{S|V\Lambda}q_V q_\Lambda\right\|_1 \\
&\overset{(d)}{=} \left\|p_{\tilde{Y}_{\mathcal{U}}^n|V}p_V - q_{\tilde{Y}_{\mathcal{U}}^n|V}p_V\right\|_1 + \left\|p_{V|S\Lambda}p_S p_\Lambda - q_V q_\Lambda q_{S|V\Lambda}\right\|_1, \qquad (57)
\end{aligned}
$$

where (a) holds by the definition of $q_{SV\tilde{Y}_{\mathcal{U}}^n\Lambda}$, (b) holds by triangle inequality, (c) holds by the Markov chain $(\Lambda, S) - V - \tilde{Y}_{\mathcal{U}}^n$, (d) holds by the independence between S and Λ. The first term in the right-hand side of (57) is upper-bounded as follows

$$
\begin{aligned}
&\left\|p_{\tilde{Y}_{\mathcal{U}}^n|V}p_V - q_{\tilde{Y}_{\mathcal{U}}^n|V}p_V\right\|_1 \\
&= \int_{y^n}\sum_v \left|p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)p_V(v) - q_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)p_V(v))\right| dy^n \\
&\overset{(a)}{=} \int_{y^n}\sum_v \left|p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)2^{-r} - \mathbb{1}\left\{y^n \in \mathbb{T}(v)\cap\beta_n(r_{t(v)})\right\} \times p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)2^{-r}\right| dy^n \\
&= \sum_v \int_{y^n\notin\mathbb{T}(v)\cap\beta_n(r_{t(v)})} \left|p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)2^{-r}\right| dy^n \\
&\overset{(b)}{\leq} 2^{-r}\left[\sum_v \int_{y^n\notin\mathbb{T}(v)} p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)dy^n + \sum_v \int_{y^n\notin\beta_n(r_{t(v)})} p_{\tilde{Y}_{\mathcal{U}}^n|V}(y^n|v)dy^n\right] \\
&\overset{(c)}{=} \sum_v 2^{-r}\mathbb{P}\left[\|\tilde{Y}_{\mathcal{U}}^n - t(v)\|^2 > n\sigma^2_{\tilde{Y}_{\mathcal{U}}}(1+\delta)|V=v\right] \\
&\quad + \sum_v 2^{-r}\mathbb{P}\left[\|\tilde{Y}_{\mathcal{U}}^n - t(v)\|^2 < n\sigma^2_{\tilde{Y}_{\mathcal{U}}}(1-\delta)|V=v\right] \\
&\quad + \sum_v 2^{-r}\mathbb{P}\left[\|\tilde{Y}_{\mathcal{U}}^n\|^2 \geq (n\sigma^2_{\tilde{Y}_{\mathcal{U}}} + \|t(v)\|^2)(1+\delta)|V=v\right] \\
&\overset{(d)}{\leq} \sum_v 2^{-r}\left[2\exp\left(-\frac{n}{2}(\delta - \ln(1+\delta))\right) + 2\exp\left(-\frac{n}{2}(-\delta - \ln(1-\delta))\right)\right. \\
&\quad \left. + \exp\left(-\frac{1}{4}(n + 2\|t(v)\|^2\sigma^{-2}_{\tilde{Y}_{\mathcal{U}}})\left(\sqrt{\delta+1} - 1\right)^2\right)\right]
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(e)}{\leq} 2\exp\left(-\frac{n\delta^2}{6}\right) + 2\exp\left(-\frac{n\delta^2}{4}\right) + 2^{-r}\sum_{v}\exp\left(-\frac{n}{4}\left(1+\frac{2\|t(v)\|^2}{n\sigma^2_{\tilde{Y}_{\mathcal{U}}}}\right)\left(\sqrt{\delta+1}-1\right)^2\right)\\
&\leq 4e^{\frac{-n\delta^2}{6}} + 2^{-r}\sum_{v}\exp\left(-\frac{n}{4}\left(\sqrt{\delta+1}-1\right)^2\right)\\
&= 4e^{\frac{-n\delta^2}{6}} + e^{-\frac{n}{4}\left(\sqrt{\delta+1}-1\right)^2}, \qquad (58)
\end{aligned}
$$

where (a) holds by (55) and because V is uniformly distributed, (b) holds by the union bound, (c) holds by (52), (53), and (54), (d) holds for the by Lemmas 21 and 22 in Appendix G, (e) holds because $\forall x \in]0, \frac{1}{2}[, x - \ln(1+x) > \frac{x^2}{3}$ and $\forall x \in]0, \frac{1}{2}[, -x - \ln(1-x) > \frac{x^2}{2}$.

We now upper-bound the second term in the right-hand side of (57). For any $s \in \{0,1\}^k, \lambda \in \{0,1\}^r \backslash \{\mathbf{0}\}, v \in \{0,1\}^r$, we have

$$
\begin{aligned}
p_{V|S\Lambda}(v|s,\lambda) &\overset{(a)}{=} \sum_{b} p_{V|BS\Lambda}(v|b,s,\lambda)p_B(b)\\
&\overset{(b)}{=} \frac{1}{2^{r-k}}\sum_{b} p_{V|BS\Lambda}(v|b,s,\lambda)\\
&\overset{(c)}{=} 2^{k-r}\sum_{b}\mathbb{1}\left\{\phi(\lambda,s,b)=v\right\}\\
&\overset{(d)}{=} 2^{k-r}\sum_{b}\mathbb{1}\left\{\lambda^{-1}\odot(s\|b)=v\right\}\\
&= 2^{k-r}\sum_{b}\mathbb{1}\left\{(s\|b)=\lambda\odot v\right\}, \qquad (59)
\end{aligned}
$$

where (a) holds by marginalization over $b \in \{0,1\}^{r-k}$ and independence between B and (S,Λ), (b) holds because p_B is the uniform distribution over $\{0,1\}^{r-k}$, (c) holds by definition of v in Section D.2, (d) holds by the definition of ϕ in Section D.2. Then, we have

$$
\begin{aligned}
&\left\|p_{V|S\Lambda}p_S p_\Lambda - q_V q_\Lambda q_{S|V\Lambda}\right\|_1\\
&= \sum_{v,s,\lambda}\left|p_{V|S\Lambda}(v|s,\lambda)p_S(s)p_\Lambda(\lambda) - q_{S|V\Lambda}(s|v,\lambda)q_V(v)q_\Lambda(\lambda)\right|
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(a)}{=} \sum_{v,s,\lambda} \left| 2^{k-r} \sum_{b} \mathbb{1}\left\{(s\|b) = \lambda \odot v\right\} 2^{-k} |\mathcal{L}|^{-1} - \mathbb{1}\left\{s = (\lambda \odot v)_k\right\} 2^{-r} |\mathcal{L}|^{-1} \right| \\
&\overset{(b)}{=} \sum_{v,s,\lambda} \left| \mathbb{1}\left\{s = (\lambda \odot v)_k\right\} 2^{-r} |\mathcal{L}|^{-1} - \mathbb{1}\left\{s = (\lambda \odot v)_k\right\} 2^{-r} |\mathcal{L}|^{-1} \right| \\
&= 0,
\end{aligned}
$$

where (a) holds by Equations (56) and (59), (b) holds because $\mathbb{1}\left\{s = (\lambda \odot v)_k\right\} = \sum_b \mathbb{1}\left\{(s\|b) = \lambda \odot v\right\}$ since if $s = (\lambda \odot v)_k$, then there exists a unique $b^* \in \mathcal{B}$ such that $(s\|b^*) = \lambda \odot v$, which means $\sum_b \mathbb{1}\left\{(s\|b) = \lambda \odot v\right\} = 1$, and if $s \neq (\lambda \odot v)_k$, then there is no $b^* \in \mathcal{B}$ such that $(s\|b^*) = \lambda \odot v$. □

For any $\mathcal{U} \in \mathbb{U}_z$, the conditional min-entropy $H_\infty(q_{V\tilde{Y}^n_{\mathcal{U}}}|q_{\tilde{Y}^n_{\mathcal{U}}})$ of V given $\tilde{Y}^n_{\mathcal{U}}$ is defined as [88]

$$
H_\infty(q_{V\tilde{Y}^n_{\mathcal{U}}}|q_{\tilde{Y}^n_{\mathcal{U}}}) \triangleq -\log \int_{\mathbb{R}^n} \max_v q_V(v) q_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v) dy^n.
$$

Lemma 20. *For any $\mathcal{U} \in \mathbb{U}_z$, we have*

$$
H_\infty(q_{V\tilde{Y}^n_{\mathcal{U}}}|q_{\tilde{Y}^n_{\mathcal{U}}}) \geq r - \frac{n}{2}\left[\log(1 + \sigma^2_{\tilde{Y}_{\mathcal{U}}} P) + \delta^{(1)}(n)\right],
$$

where $\delta^{(1)}(n) \triangleq \delta \log e + \log(1+\delta) + O(n^{-2})$.

Proof. We have

$$
\begin{aligned}
&H_\infty(q_{V\tilde{Y}^n_{\mathcal{U}}}|q_{\tilde{Y}^n_{\mathcal{U}}}) \\
&\overset{(a)}{=} r - \log \int_{\mathbb{R}^n} \max_v q_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v) dy^n \\
&\overset{(b)}{=} r - \log \int_{\mathbb{R}^n} \max_v \mathbb{1}\left\{y^n \in \mathbb{T}(v) \cap \beta_n(r_{t(v)})\right\} \times p_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v) dy^n \\
&\overset{(c)}{=} r - \log \int_{\mathbb{R}^n} \max_v \mathbb{1}\left\{y^n \in \mathbb{T}(v) \cap \beta_n(r_{t(v)})\right\} \times g\left(y^n - t(v)\right) dy^n
\end{aligned}
$$

$$
\begin{aligned}
&= r - \log \int\limits_{\mathbb{R}^n} \max_v \mathbb{1}\left\{y^n \in \mathbb{T}(v) \cap \beta_n(r_{t(v)})\right\} \times \frac{1}{(\sigma^2_{\tilde{Y}_{\mathcal{U}}} 2\pi)^{\frac{n}{2}}} e^{\frac{-\|y^n - t(v)\|^2}{2\sigma^2_{\tilde{Y}_{\mathcal{U}}}}} dy^n \\
&\overset{(d)}{\geq} r - \log \frac{e^{-\frac{n\sigma^2_{\tilde{Y}_{\mathcal{U}}}(1-\delta)}{2\sigma^2_{\tilde{Y}_{\mathcal{U}}}}}}{(\sigma^2_{\tilde{Y}_{\mathcal{U}}} 2\pi)^{\frac{n}{2}}} \int\limits_{\mathbb{R}^n} \max_v \mathbb{1}\left\{y^n \in \mathbb{T}(v) \cap \beta_n(r_{t(v)})\right\} dy^n \\
&\overset{(e)}{\geq} r - \log \frac{e^{-\frac{n(1-\delta)}{2}}}{(\sigma^2_{\tilde{Y}_{\mathcal{U}}} 2\pi)^{\frac{n}{2}}} \int\limits_{\mathbb{R}^n} \max_v \mathbb{1}\left\{y^n \in \beta_n(\rho_n)\right\} dy^n \\
&= r - \log \frac{e^{-\frac{n(1-\delta)}{2}}}{(\sigma^2_{\tilde{Y}_{\mathcal{U}}} 2\pi)^{\frac{n}{2}}} \mathrm{vol}(\beta_n(\rho_n)) \\
&\overset{(f)}{=} r - \log \left[\frac{e^{-\frac{n(1-\delta)}{2}}}{(\sigma^2_{\tilde{Y}_{\mathcal{U}}} 2\pi)^{\frac{n}{2}}} \frac{1}{\sqrt{n\pi}} \left(\frac{2\pi e}{n}\right)^{\frac{n}{2}} \left(\sqrt{(n\sigma^2_{\tilde{Y}_{\mathcal{U}}} + \sigma^4_{\tilde{Y}_{\mathcal{U}}} nP)(1+\delta)}\right)^n \left(1 + O(n^{-1})\right)\right] \\
&\geq r - \frac{n}{2}\left[\log(1 + \sigma^2_{\tilde{Y}_{\mathcal{U}}} P) + \delta \log e + \log(1+\delta) + \frac{2\log\left(1 + O(n^{-1})\right)}{n}\right],
\end{aligned}
$$

where (a) holds because q_V is the uniform distribution over $\{0,1\}^r$, (b) holds by (55), (c) holds by denoting g as the zero-mean normal density on $\mathbb{R}^n$ with covariance matrix $\mathrm{diag}((\sigma^2_{\tilde{Y}_{\mathcal{U}}})_{i\in[n]})$ such that for any $y^n \in \mathbb{R}^n$, $v \in \{0,1\}^r, p_{\tilde{Y}^n_{\mathcal{U}}|V}(y^n|v) = g\left(y^n - t(v)\right)$, (d) holds by (54), (e) holds by (53) and by denoting $\beta_n(\rho_n)$ as the ball of radius ρ_n in $\mathbb{R}^n$, i.e.,

$$
\beta_n(\rho_n) \triangleq \left\{y^n \in \mathbb{R}^n : \|y^n\| \leq \rho_n\right\},
$$

with

$$
\rho_n \triangleq \sqrt{(n\sigma^2_{\tilde{Y}_{\mathcal{U}}} + \sigma^4_{\tilde{Y}_{\mathcal{U}}} nP)(1+\delta)}, \tag{60}
$$

as $\|t(v)\|^2 \leq \sigma^4_{\tilde{Y}_{\mathcal{U}}} nP$ from the power constraint and (51), which implies $\beta_n(r_{t(v)}) \subset \beta_n(\rho_n)$, (g) holds by (60) and approximating the volume of the ball $\beta_n(\rho_n)$ as [110]

$$
\mathrm{vol}(\beta_n(\rho_n)) = \frac{1}{\sqrt{n\pi}} \left(\frac{2\pi e}{n}\right)^{\frac{n}{2}} \rho_n^n (1 + O(n^{-1})).
$$

□

b) *Leakage analysis*: Define p_{unif} as the uniform distribution over $\{0,1\}^k$. Then, we have

$$\begin{aligned}
&\left\|p_{S\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}p_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \\
&\leq \left\|p_{SY_{\mathcal{U}}^n\Lambda} - q_{S\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 + \left\|q_{S\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}q_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 + \left\|p_{\text{unif}}q_{\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}p_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \\
&\overset{(a)}{\leq} 2\delta^{(0)}(n) + \left\|q_{S\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}q_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \\
&\overset{(b)}{=} 2\delta^{(0)}(n) + \left\|q_{\psi(\Lambda,V)\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}q_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \\
&\overset{(c)}{\leq} 2\delta^{(0)}(n) + \frac{1}{2}\sqrt{2^{k-H_\infty(q_{V\tilde{Y}_{\mathcal{U}}^n}|q_{\tilde{Y}_{\mathcal{U}}^n})}} \\
&\overset{(d)}{\leq} 2\delta^{(0)}(n) + \frac{1}{2}\sqrt{2^{k-r+\frac{n}{2}\left[\log(1+\sigma^2_{\tilde{Y}_{\mathcal{U}}}P)+\delta^{(1)}(n)\right]}},
\end{aligned} \tag{61}$$

where (a) holds by Lemma 19, (b) holds by the definition of ψ in Section D.2 and (56), (c) holds by Lemma 23 in Appendix G, (d) holds by Lemma 20. Then, for $\delta > 0$, define the output length of the hash function as

$$k \triangleq r - \frac{n}{2}\left[\max_{\mathcal{U}\in\mathbb{U}_z}\log(1+\sigma^2_{\tilde{Y}_{\mathcal{U}}}P) + \delta^{(1)}(n)\right] - n\delta, \tag{62}$$

such that (61) becomes

$$\left\|p_{S\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}p_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1 \leq 2\delta^{(0)}(n) + \tfrac{1}{2}\sqrt{2^{-n\delta}}. \tag{63}$$

Then, we have

$$\begin{aligned}
I(S;\tilde{Y}_{\mathcal{U}}^n\Lambda) &\overset{(a)}{\leq} f(\left\|p_{S\tilde{Y}_{\mathcal{U}}^n\Lambda} - p_{\text{unif}}p_{\tilde{Y}_{\mathcal{U}}^n\Lambda}\right\|_1) \\
&\overset{(b)}{\leq} f(2\delta^{(0)}(n) + \tfrac{1}{2}\sqrt{2^{-n\delta}}).
\end{aligned} \tag{64}$$

where (a) holds by [111] with $f : x \mapsto x\log(2^k/x)$, (b) holds by (63) for n large

enough. Since (64) is true for any $\mathcal{U} \in \mathbb{U}_z$, we have for n large enough

$$\max_{\mathcal{U}\in\mathbb{U}_z} I(S;\tilde{Y}_{\mathcal{U}}^n\Lambda) \leq f(2\delta^{(0)}(n) + \tfrac{1}{2}\sqrt{2^{-n\delta}}). \tag{65}$$

Then, for any $\mathcal{U} \in \mathbb{U}_z$, we have

$$\begin{aligned}
\max_{\mathcal{U}\in\mathbb{U}_z} I(S;\Lambda\tilde{Y}_{\mathcal{U}}^n) &\geq I(S;\Lambda\tilde{Y}_{\mathcal{U}}^n) \\
&= I(S;\Lambda\tilde{Y}_{\mathcal{U}}^n Y_{\mathcal{U}}^n) - I(S;Y_{\mathcal{U}}^n|\Lambda\tilde{Y}_{\mathcal{U}}^n) \\
&\overset{(a)}{\geq} I(S;\Lambda Y_{\mathcal{U}}^n) - I(X^nS;Y_{\mathcal{U}}^n|\Lambda\tilde{Y}_{\mathcal{U}}^n) \\
&\overset{(b)}{\geq} I(S;\Lambda Y_{\mathcal{U}}^n) - I(X^nS\Lambda;Y_{\mathcal{U}}^n|\tilde{Y}_{\mathcal{U}}^n) \\
&= I(S;\Lambda Y_{\mathcal{U}}^n) - I(X^n;Y_{\mathcal{U}}^n|\tilde{Y}_{\mathcal{U}}^n) - I(S\Lambda;Y_{\mathcal{U}}^n|\tilde{Y}_{\mathcal{U}}^nX^n) \\
&\overset{(c)}{=} I(S;\Lambda Y_{\mathcal{U}}^n) - I(S\Lambda;Y_{\mathcal{U}}^n|\tilde{Y}_{\mathcal{U}}^nX^n) \\
&\overset{(d)}{\geq} I(S;\Lambda Y_{\mathcal{U}}^n) - I(S\Lambda;Y_{\mathcal{U}}^n\tilde{Y}_{\mathcal{U}}^n|X^n) \\
&= I(S;\Lambda Y_{\mathcal{U}}^n) - I(S\Lambda;Y_{\mathcal{U}}^n|X^n) - I(S\Lambda;\tilde{Y}_{\mathcal{U}}^n|X^nY_{\mathcal{U}}^n) \\
&\overset{(e)}{\geq} I(S;\Lambda Y_{\mathcal{U}}^n) - I(S\Lambda;Y_{\mathcal{U}}^n|X^n) - I(S\Lambda X^n;\tilde{Y}_{\mathcal{U}}^n|Y_{\mathcal{U}}^n) \\
&\overset{(f)}{=} I(S;\Lambda Y_{\mathcal{U}}^n),
\end{aligned} \tag{66}$$

where (a), (b), (d) and (e) hold by the chain rule and nonnegativity of the mutual information, (c) holds by Lemma 18 and [108, Section 2.9], (f) holds by the Markov chain $(S,\Lambda) - X^n - Y_{\mathcal{U}}^n$ and the Markov chain $(S,\Lambda,X^n) - Y_{\mathcal{U}}^n - \tilde{Y}_{\mathcal{U}}^n$ Finally, we have

$$\max_{\mathcal{U}\in\mathbb{U}_z} I(S;\Lambda Y_{\mathcal{U}}^n) \leq \max_{\mathcal{U}\in\mathbb{U}_z} I(S;\Lambda\tilde{Y}_{\mathcal{U}}^n) \xrightarrow{n\to+\infty} 0, \tag{67}$$

where the inequality holds by (66) since (66) is valid for any $\mathcal{U} \in \mathbb{U}_z$, and the limit holds by (65).

E.2 Secret sharing rate

The secret sharing rate is

$$\begin{aligned} R_s &= \frac{k}{n} \\ &\overset{(a)}{=} \frac{r - \frac{n}{2}\left[\max_{\mathcal{U}\in\mathbb{U}_z} \log(1+\sigma^2_{\tilde{Y}_\mathcal{U}} P) + \delta^{(1)}(n)\right] - n\delta}{n} \\ &\xrightarrow{n\to+\infty} \frac{1}{2} \min_{\mathcal{A}\in\mathbb{A}_t, \mathcal{U}\in\mathbb{U}_z} \log\left(\frac{1+\sigma^2_{\tilde{Y}_\mathcal{A}} P}{1+\sigma^2_{\tilde{Y}_\mathcal{U}} P}\right) - \epsilon(\delta) \\ &\overset{(b)}{=} \frac{1}{2} \min_{\mathcal{A}\in\mathbb{A}_t, \mathcal{U}\in\mathbb{U}_z} \log\left(\frac{1+\sum_{l\in\mathcal{A}} \frac{P}{\sigma_l^2}}{1+\sum_{l\in\mathcal{U}} \frac{P}{\sigma_l^2}}\right) - \epsilon(\delta), \end{aligned}$$

where (a) holds by (62), the limits holds by (46) with $\epsilon(\delta)$ such that $\lim_{\delta\to 0} \epsilon(\delta) = 0$, (b) holds by (42) and (43).

E.3 Analysis of reliability

For any $\mathcal{A} \in \mathbb{A}_t$, we have

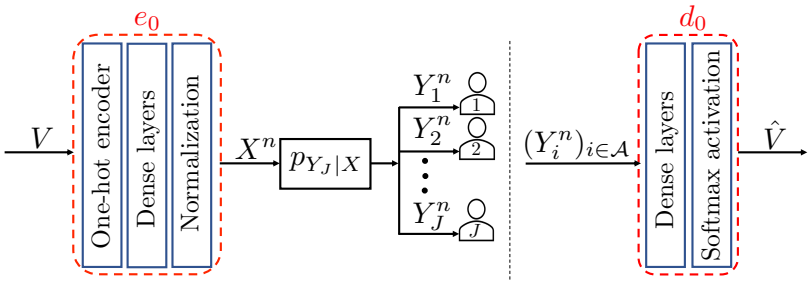
$$\begin{aligned} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] &\leq \mathbb{P}[d_0(\tilde{Y}^n_\mathcal{A})) \neq V] \\ &\leq \max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[d_0(\tilde{Y}^n_\mathcal{A})) \neq V]. \end{aligned} \tag{68}$$

Since (68) is valid for any $\mathcal{A} \in \mathbb{A}_t$, by (47), we have

$$\lim_{n\to+\infty} \max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = 0. \tag{69}$$

E.4 Seed sharing

Note that the seed Λ in the coding scheme of Section D needs to be shared between all the parties. This can be done with negligible impact on the overall communication rate similar to [87] using an hybrid argument by repeating the coding scheme of Section E with the same seed Λ.



(a) Encoder (b) Decoder

Figure 9: Architecture of the autoencoder (e_0, d_0) via feed-forward neural networks.

F Secret sharing scheme at finite blocklength

We design a secret sharing scheme at finite blocklength in Section F.1 and evaluate its performance through simulations in Section F.2.

F.1 Secret sharing scheme design

a) *Reliability layer design*: The design of the reliability layer consists in designing an encoder/decoder pair (e_0, d_0) as described in Definition 12. Let $\mathcal{V} \triangleq [2^r]$ be the message set. (e_0, d_0) is implemented with an autoencoder as in [112]. The goal of the autoencoder is here to learn a representation of the encoded message that is robust to the channel noise so that the authorized participants can reconstruct the message from their noisy channel observations with a small probability of error. As depicted in Figure 9, 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 9, 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 $p_v \triangleq \exp(\mu_v) \left(\sum_{i=1}^{|\mathcal{V}|} \exp(\mu_i)\right)^{-1}$. 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 possible messages $v \in \mathcal{V}$ using a stochastic gradient descent (SGD) as in [113] and the categorical cross-entropy loss function.

b) *Secrecy layer design*: We implement the secrecy layer with the functions ψ and ϕ defined in Equations (49) and (50), respectively. Note that, unlike the asymptotic regime, we will choose a fixed seed $\lambda \in \mathcal{L}$ rather than a random seed.

c) *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 D.2. 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 $M_{1:\gamma} \triangleq (M_i)_{i \in [\gamma]}$.

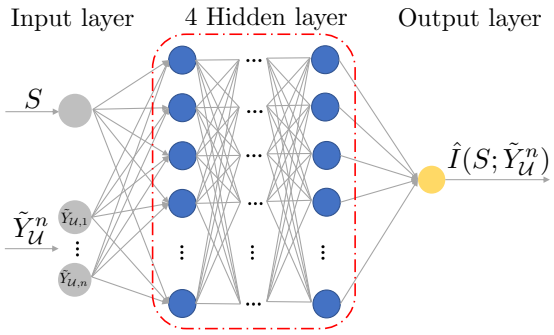


Figure 10: The security performance is evaluated in terms of the leakage $I(S;\tilde{Y}_{\mathcal{U}}^n)$, $\mathcal{U} \in \mathbb{U}_z$, via the mutual information estimator where $\tilde{Y}_{\mathcal{U}}^n \triangleq (\tilde{Y}_{\mathcal{U},i})_{i\in[n]}$.

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 $\hat{S}(\mathcal{A}) \triangleq \psi(\alpha, \hat{M}_{1:\gamma})$.

F.2 Performance evaluation

a) *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 SNR $= -16$dB. We also consider a secret of length $k = 1$ and a power $P = 1$. Note that since the SNR is the same for all the participants, we have for $\mathcal{A}^* \triangleq [t]$ and $\mathcal{U}^* \triangleq [z]$

$$\max_{\mathcal{A}\in\mathbb{A}_t} \mathbb{P}[\hat{S}(\mathcal{A}) \neq S] = \mathbb{P}[\hat{S}(\mathcal{A}^*) \neq S],$$
$$\max_{\mathcal{U}\in\mathbb{U}_z} I(S; Y_{\mathcal{U}}^n) = I(S; Y_{\mathcal{U}^*}^n).$$

For the autoencoder training and neural network implementation, we use Python 3.7 and Tensorflow 2.3.

b) *Performance evaluation of the reliability layer*:

For the parameters defined in Section F.2, we train the autoencoder for $(n, r) = (5, 2)$ using SGD with the Adam optimizer [113] 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 $Y^n_{\mathcal{A}^*}$. By Lemma 18, without loss of generality, we consider $\tilde{Y}^n_{\mathcal{A}^*} \triangleq \mathbf{1}_t^T \Sigma^{-1}_{\mathcal{A}^*} Y^n_{\mathcal{A}^*}$, where $\Sigma_{\mathcal{A}^*} \triangleq \mathrm{diag}((\sigma_j^2)_{j\in\mathcal{A}^*})$. Finally, the trained decoder d_0 forms an estimate of V, $\hat{V}(\mathcal{A}^*) \triangleq d_0(\tilde{Y}^n_{\mathcal{A}^*})$. Figure 11 shows the average probability of error $\mathbb{P}[\hat{V}(\mathcal{A}^*)\neq V]$.

c) *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

$$X_i^n \triangleq e_0(\phi(\lambda, M_i, B_i)), \tag{70}$$

such that the channel observations of the participants in $\mathcal{U}^*$ are $Y^n_{\mathcal{U}^*,i} \triangleq X_i^n + N^n_{\mathcal{U}^*,i}$. Similar to (66), using Lemma 18, there is no loss of generality in considering $\tilde{Y}^n_{\mathcal{U}^*,i} \triangleq \mathbf{1}_z^T \Sigma^{-1}_{\mathcal{U}^*} Y^n_{\mathcal{U}^*,i}$ instead of $Y^n_{\mathcal{U}^*,i}$. Finally, generate the secret as

$$S \triangleq \psi(\alpha, M_{1:\gamma}). \tag{71}$$

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 $\gamma = 4$. Next, we concatenate all the observations $\tilde{Y}^n_{\mathcal{U}^*,i}$, $i \in [\gamma]$, as $\tilde{Y}^n_{\mathcal{U}^*,1:\gamma}$ and to evaluate the leakage $I(S; \tilde{Y}^n_{\mathcal{U}^*,1:\gamma})$, we use the MINE from [73] based on neural networks, whose architecture is depicted in Figure 10. 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 $p_{S\tilde{Y}^n_{\mathcal{U}^*,1:\gamma}}$ are produced as described above. The samples of the marginal distributions are generated by dropping either s or $y^n_{\mathcal{U}^*,1:\gamma}$, from the joint samples $(s, y^n_{\mathcal{U}^*,1:\gamma})$. We trained the neural network over 40000 epochs of $20,000$ messages with a batch size of 2500. Figure 7 shows the information leakage $I(S; \tilde{Y}^n_{\mathcal{U}^*,1:\gamma})$ with respect to the secret sharing rate $R_s = \frac{k}{n}$ when z varies

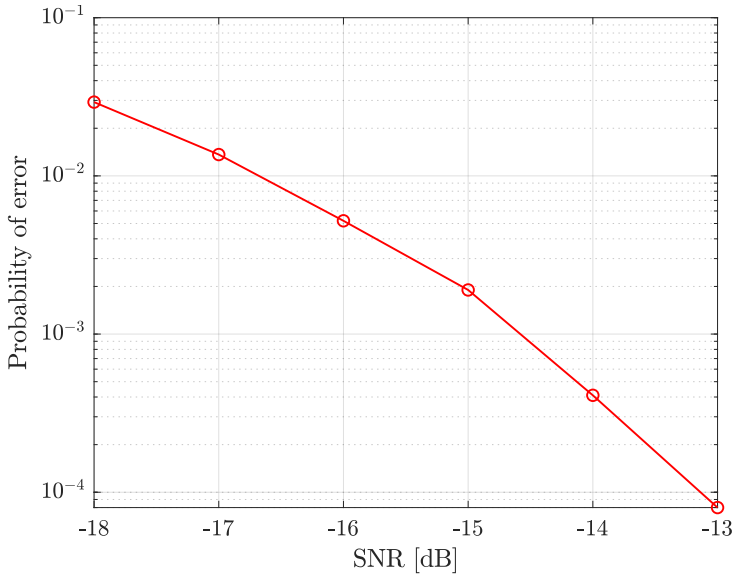


Figure 11: Probability of error (e_0, d_0) at SNR $= -16$dB.

in [10].

d) *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 (70) 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 18, 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 (71).

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 8 shows the average probability of error $\mathbb{P}[\hat{S}(\mathcal{A}^*) \neq S]$ with respect to the secret sharing rate $R_s = \frac{k}{n}$.

G 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.

APPENDIX

APPENDIX D

Supporting Lemmas

Lemma 21 ([114, Lemma 2]). *Let Y^n be a length-n vector with independent and identically distributed zero-mean Gaussian entries with variance σ_Y^2. Then, for any $0 < \delta < 1$,*

$$\mathbb{P}\left[\|Y^n\|^2 \geq n\sigma_Y^2(1+\delta)\right] \leq 2\exp\left(-\frac{n}{2}(\delta - \ln(1+\delta))\right),$$
$$\mathbb{P}\left[\|Y^n\|^2 \leq n\sigma_Y^2(1-\delta)\right] \leq 2\exp\left(-\frac{n}{2}(-\delta - \ln(1-\delta))\right).$$

Lemma 22 ([115, Lemma 8.1]). *Let X be a noncentral χ^2 variable with D degrees of freedom and noncentrality parameter $B^{\frac{1}{2}} \geq 0$, then for all $x > 0$,*

$$\mathbb{P}\left[X \geq (D+B) + 2\sqrt{(D+2B)x} + 2x\right] \leq \exp(-x). \tag{72}$$

Moreover, if we set $\delta = \frac{2\sqrt{(D+2B)x}+2x}{D+B}$, then (72) becomes

$$\begin{aligned}\mathbb{P}\left[X \geq (D+B)(1+\delta)\right] &\leq \exp\left(-\frac{1}{4}(D+2B)\left(\sqrt{\frac{2\delta(D+B)}{D+2B}+1}-1\right)^2\right)\\ &\leq \exp\left(-\frac{1}{4}(D+2B)\left(\sqrt{\delta+1}-1\right)^2\right).\end{aligned}$$

Lemma 23 ([31]). *Let V and Y be distributed according to p_{VY} over $\mathcal{V} \times \mathcal{Y}$. Consider $F : \mathcal{L} \times \{0,1\}^r \to \{0,1\}^k$, where the first input, denoted by Λ, is uniformly distributed over $\mathcal{L}$ to indicate that F is chosen uniformly at random in a family of two-universal hash functions. Then,*

$$\|p_{F(\Lambda,V),\Lambda,Y} - p_{U_\mathcal{S}} p_{U_\mathcal{L}} p_Y\|_1 \leq \frac{1}{2}\sqrt{2^{k - H_\infty(p_{VY}|p_Y)}}, \tag{73}$$

where $p_{U_\mathcal{S}}$ and $p_{U_\mathcal{L}}$ are the uniform distribution over $\{0,1\}^k$ and $\mathcal{L}$, respectively.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 472–487, 1998.

[2] T. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, 1993.

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

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

[5] 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.

[6] R. Sultana and R. Chou, "Explicit low-complexity codes for multiple access channel resolvability," in *Proc. of the Annual Allerton Conf. on Communication, Control, and Computing*, pp. 116–123, 2019.

[7] R. Sultana and R. Chou, "Explicit construction of multiple access channel resolvability codes from source resolvability codes," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2020.

[8] R. Sultana and R. A. Chou, "Multiple access channel resolvability codes from source resolvability codes," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3608–3619, 2022.

[9] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inform. Forensics Sec*, vol. 6, no. 3, pp. 595–605, 2011.

[10] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. of IEEE Inf. Theory Workshop 2010*, pp. 1–5.

[11] M. Frey, I. Bjelakovic, and S. Stanczak, "The MAC Resolvability Region, Semantic Security and Its Operational Implications," *arXiv preprint arXiv:1710.02342*, 2017.

[12] M. Bloch and J. Kliewer, "Strong coordination over a line network," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2319–2323, 2013.

[13] M. Bloch, L. Luzzi, and J. Kliewer, "Strong coordination with polar codes," in *Proc. of the Annual Allerton Conf. on Communication, Control, and Compputing*, pp. 565–571, 2012.

[14] R. Chou, M. Bloch, and J. Kliewer, "Empirical and strong coordination via soft covering with polar codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5087–5100, 2018.

[15] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2355–2409, 2016.

[16] R. Amjad and G. Kramer, "Channel resolvability codes based on concatenation and sparse linear encoding," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2111–2115, 2015.

[17] R. Chou, M. Bloch, and J. Kliewer, "Low-complexity channel resolvability codes for the symmetric multiple-access channel," in *Proc. of IEEE Inf. Theory Workshop*, pp. 466–470, 2014.

[18] T. Han, "Information-spectrum methods in information theory volume 50 of," *Applications of Mathematics*, 2003.

[19] S. Vadhan, "Pseudorandomness," *Foundations and Trends® in Theoretical Computer Science*, vol. 7, no. 1–3, pp. 1–336, 2012.

[20] A. Grant, B. Rimoldi, R. Urbanke, and P. Whiting, "Rate-splitting multiple access for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 873–890, 2001.

[21] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of computer and system sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[22] R. Chou, M. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[23] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," in *Combinatorial Optimization—Eureka, You Shrink!*, pp. 11–26, Springer, 2003.

[24] R. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, 2018.

[25] E. Arikan, "Source polarization," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 899–903, 2010.

[26] R. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.

[27] R. Chou and M. Bloch, "Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes," in *Proc. of the Annual Allerton Conf. on Communication, Control, and Compputing*, pp. 1380–1385, 2015.

[28] R. Chou, M. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

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

[30] R. A. Chou, "Distributed secret sharing over a public channel from correlated random variables," *arXiv preprint arXiv:2110.10307*, 2021.

[31] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[32] S. Watanabe and M. Hayashi, "Non-Asymptotic Analysis of Privacy Amplification via Rényi Entropy and Inf-Spectral Entropy," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2715–2719, 2013.

[33] 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*, pp. 970–975, 2021.

[34] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics and Secur.*, vol. 2, no. 3, pp. 364–375, 2007.

[35] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics and Secur.*, vol. 5, no. 3, pp. 381–392, 2010.

[36] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics and Secur.*, vol. 5, no. 2, pp. 240–254, 2010.

[37] A. Pierrot, R. Chou, and M. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications*, pp. 669–673, 2013.

[38] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of eavesdropper's statistics in experimental wireless secret-key generation," *arXiv preprint arXiv:1312.3304*, 2013.

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

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

[41] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, 2010.

[42] M. Ye and A. Barg, "Universal source polarization and an application to a multi-user problem," in *Proc. of the Annual Allerton Conf. on Communication, Control, and Computing*, pp. 805–812, 2014.

[43] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, 2000.

[44] R. A. Chou, "Biometric systems with multiuser access structures," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 807–811, 2019.

[45] V. Rana, R. A. Chou, and H. M. Kwon, "Information-theoretic secret sharing from correlated Gaussian random variables and public communication," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 549–559, 2021.

[46] Y. Liang, G. Kramer, and H. V. Poor, "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–12, 2009.

[47] N. Tavangaran, H. Boche, and R. F. Schaefer, "Secret-key generation using compound sources and one-way public communication," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 227–241, 2016.

[48] M. Bloch, "Channel intrinsic randomness," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2607–2611, 2010.

[49] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[50] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[51] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[52] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, 1997.

[53] 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*, pp. 351–368, Springer, 2000.

[54] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret-key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, 2014.

[55] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, 2012.

[56] J. M. Renes, R. Renner, and D. Sutter, "Efficient one-way secret-key agreement and private channel coding via polarization," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 194–213, Springer, 2013.

[57] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, 2010.

[58] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and steiner tree packing," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6490–6500, 2010.

[59] R. Chou and A. Yener, "Secret-key generation in many-to-one networks: An integrated game-theoretic and information-theoretic approach," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5144–5159, 2019.

[60] R. A. Chou, "Unified framework for polynomial-time wiretap channel codes," *arXiv preprint arXiv:2002.01924*, 2020.

[61] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Conference on the Theory and Application of Cryptography*, pp. 27–35, Springer, 1988.

[62] R. A. Chou and M. R. Bloch, "Data compression with nearly uniform output," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 1979–1983, 2013.

[63] R. Chou, B. Vellambi, M. Bloch, and J. Kliewer, "Coding schemes for achieving strong secrecy at negligible cost," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1858–1873, 2016.

[64] R. A. Chou, M. R. Bloch, and A. Yener, "Universal covertness for discrete memoryless sources," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5432–5442, 2021.

[65] R. Sultana, V. Rana, and R. A. Chou, "Secret sharing over a gaussian broadcast channel: Optimal coding scheme design and deep learning approach at short blocklength," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2023.

[66] A. Beimel, "Secret-sharing schemes: A survey," in *International Conference on Coding and Cryptology*, (Berlin, Heidelberg), pp. 11–46, 2011.

[67] V. Rana, R. A. Chou, and H. Kwon, "Secret sharing from correlated Gaussian random variables and public communication," in *IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2021.

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

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

[70] G. A. Darbellay and I. Vajda, "Estimation of the information by an adaptive partitioning of the observation space," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1315–1321, 1999.

[71] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical review E*, vol. 69, no. 6, pp. 066138 (1–16), 2004.

[72] T. Suzuki, M. Sugiyama, J. Sese, and T. Kanamori, "Approximating mutual information by maximum likelihood density ratio estimation," in *Workshop on New challenges for feature selection in data mining and knowledge discovery*, pp. 5–20, 2008.

[73] 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.

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

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

[76] 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*, vol. 18, pp. 117–132, 2022.

[77] 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.

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

[79] A. Nooraiepour and T. M. Duman, "Randomized turbo codes for the wiretap channel," in *IEEE Global Commun. Conf.*, pp. 1–6, 2017.

[80] 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.

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

[82] 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.

[83] 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.

[84] 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.*, pp. 1–5, 2019.

[85] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning based wiretap coding via mutual information estimation," in *Proc. of ACM Workshop on Wireless Security and Machine Learning*, pp. 74–79, 2020.

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

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

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

[89] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[90] A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 585–594, 2011.

[91] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2393–2397, 2011.

[92] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[93] E. Şaşoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 1117–1121, 2013.

[94] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Selected Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, 2013.

[95] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Letters*, vol. 14, no. 8, pp. 752–754, 2010.

[96] C. Ling, L. Luzzi, J. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.

[97] Y. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE J. Selected Areas Commun.*, vol. 34, no. 2, pp. 278–291, 2016.

[98] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages," in *2015 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2015.

[99] J. Renes, R. Renner, and D. Sutter, "Efficient one-way secret-key agreement and private channel coding via polarization," in *Advances in Cryptology. Springer*, pp. 194–213, 2013.

[100] T. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1311–1324, 2017.

[101] R. A. Chou, "Explicit wiretap channel codes via source coding, universal hashing, and distribution approximation, when the channels' statistics are uncertain," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 117–132, 2022.

[102] R. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 476–480, 2018.

[103] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained Gaussian wiretap channel," in *IEEE Globecom Workshops*, pp. 898–902, 2011.

[104] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *IEEE Int. Conf. Commun. Workshop*, pp. 435–440, 2015.

[105] A. Nooraiepour, S. R. Aghdam, and T. M. Duman, "On secure communications over Gaussian wiretap channels via finite-length codes," *IEEE Commun. Letters*, vol. 24, no. 9, pp. 1904–1908, 2020.

[106] 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.

[107] 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*, pp. 1–6, 2021.

[108] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley, 1991.

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

[110] X. Wang, "Volumes of generalized unit balls," *Mathematics Magazine*, vol. 78, no. 5, pp. 390–395, 2005.

[111] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[112] 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.

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

[114] B. Nazer, Y. Shkel, and S. C. Draper, "The AWGN Red Alert Problem," *IEEE Trans. Inf. Theory*, 2012.

[115] L. Birgé, "An alternative point of view on lepski's method," *Lecture Notes-Monograph Series*, pp. 113–133, 2001.