

# Multiple Access Channel Resolvability Codes from Source Resolvability Codes

Rumia Sultana and Rémi A. Chou

**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 that relies on 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. Since explicit source resolvability codes are known, our results also yield the first explicit coding schemes that achieve the entire MAC resolvability region for any discrete memoryless multiple-access channel with binary input alphabets.

## I. INTRODUCTION

The concept of multiple access channel (MAC) resolvability has been introduced in [3] as a natural extension of channel resolvability for point-to-point channels [4]. 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 [5], [6], cooperative jamming [5], semantic security for multiple access wiretap channels [7], and strong coordination in networks [8]. These applications are, however, restricted by the fact that no explicit coding scheme is known to optimally implement MAC resolvability. Note indeed that [3], [7] only provide existence results and no explicit code constructions. The objective of this paper is to bridge this gap by providing explicit coding schemes that achieve the MAC resolvability region [7]. While previous works have been successful in providing explicit coding schemes for channel resolvability over point-to-point channels,<sup>1</sup> to the best of our knowledge, the only known explicit constructions for MAC resolvability are those of [13]. However, the explicit constructions in [13], 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.

In this paper, we propose a novel approach to the construction of MAC resolvability codes by showing that such a construction can be reduced to the simpler problem of

Part of this work has been presented at the 2019 Annual Allerton Conference on Communication, Control, and Computing [1], and the 2020 IEEE International Symposium on Information Theory [2]. This work was supported in part by NSF grant CCF-1850227. E-mails: rxsultana@shockers.wichita.edu; remi.chou@wichita.edu.

<sup>1</sup>Explicit constructions based on polar codes for channel resolvability have been proposed for binary *symmetric* point-to-point channels [9] and discrete memoryless point-to-point channels whose input alphabets have prime cardinalities [10]. Another explicit construction based on injective group homomorphisms has been proposed in [11] 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 [12].

code construction for source resolvability [14]. Since explicit constructions of source resolvability codes are known, e.g., [10], 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., [15]. 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 [16] for multiple access channel coding, for the MAC resolvability problem with two transmitters. Note that the main difference with [13], 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 [13] attempts a code construction directly adapted to multiple access channels.

The remainder of the paper is organized as follows. The problem statement is provided in Section II. Our main result is summarized in Section III. Our proposed coding scheme and its analysis are provided in Section IV and Section V, respectively. While our main result focuses on multiple access channels with two transmitters, we discuss an extension of our result to an arbitrary number of transmitters in Section VI. Finally, Section VII provides concluding remarks.

## II. PROBLEM STATEMENT AND REVIEW OF SOURCE RESOLVABILITY

### A. Notation

For  $a, b \in \mathbb{R}$ , define  $\llbracket a, b \rrbracket \triangleq \llbracket \lfloor a \rfloor, \lfloor b \rfloor \rrbracket \cap \mathbb{N}$ . The components of a vector  $X^{1:N}$  of size  $N$  are denoted with superscripts, i.e.,  $X^{1:N} \triangleq (X^1, X^2, \dots, X^N)$ . 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  $\mathbb{V}(p, q) \triangleq \sum_{x \in \mathcal{X}} |p(x) - q(x)|$ .

### B. 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.,

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

**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  $S_1 \triangleq \llbracket 1, 2^{NR_1} \rrbracket$  and  $S_2 \triangleq \llbracket 1, 2^{NR_2} \rrbracket$ , respectively;
- Two encoding functions  $f_{1,N} : S_1 \rightarrow \mathcal{X}^N$  and  $f_{2,N} : S_2 \rightarrow \mathcal{Y}^N$ ;

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

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

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

$$\tilde{p}_{Z^{1:N}}(z^{1:N}) \triangleq \sum_{(s_1, s_2) \in S_1 \times S_2} \frac{q_{Z^{1:N}|X^{1:N}Y^{1:N}}(z^{1:N}|f_{1,N}(s_1), f_{2,N}(s_2))}{|S_1||S_2|}.$$

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** ([7, 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  $\mathcal{T} \triangleq \llbracket 1, |\mathcal{Z}|+3 \rrbracket$  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 [7] 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.

### C. 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  $S \triangleq \llbracket 1, 2^{NR} \rrbracket$ ;
- An encoding function  $e_N : S \rightarrow \mathcal{X}^N$ ;

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

**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

$$\lim_{N \rightarrow +\infty} \mathbb{V}(\tilde{p}_{X^{1:N}}, q_{X^{1:N}}) = 0, \quad (2)$$

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

**Theorem 2** ([4]). 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 A.

## III. MAIN RESULT

Our main result is summarized as follows.

**Theorem 3.** The coding scheme presented in Section IV, which solely relies on source resolvability codes, used as black boxes, and two-universal hash functions [17], achieves the entire multiple access channel resolvability region  $\mathcal{R}_{q_Z}$  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 achieves the entire multiple access channel resolvability region  $\mathcal{R}_{q_Z}$  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., [17], [18], Theorem 3 yields an explicit coding scheme that achieves  $\mathcal{R}_{q_Z}$  for any discrete memoryless multiple access channel with binary input alphabets.

## IV. CODING SCHEME

We explain in Section IV-A 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 IV-B, IV-C.

A. 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  $\text{Conv}$  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  $\mathcal{R}'_{qz}$  are in  $\text{Conv}(\bigcup_{p_X p_Y} \mathcal{R}_{X,Y})$ . For instance, the point  $(I(X;Z|T), I(Y;Z|XT)) \in \mathcal{R}'_{qz}$  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  $\mathcal{R}'_{qz}$  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  $Y$ .

### B. 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 [19], to achieve the 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 C.

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

$$U_{\epsilon=0} = 0 = V_{\epsilon=1}, \quad (3)$$

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

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

The above construction is indeed possible as shown in [16, Example 3]. Then, we have  $I(XY;Z) = R_1 + R_U + R_V$ , where we have defined the functions

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

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

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

Moreover,  $R_1$  is continuous with respect to  $\epsilon$  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  $\epsilon$  by dropping the subscript  $\epsilon$ .

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

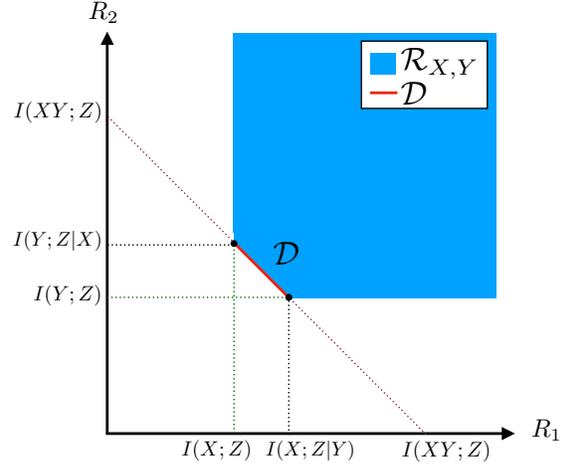


Fig. 1: Region  $\mathcal{R}_{X,Y}$  in Case 1:  $I(XY;Z) > I(X;Z) + I(Y;Z)$ .

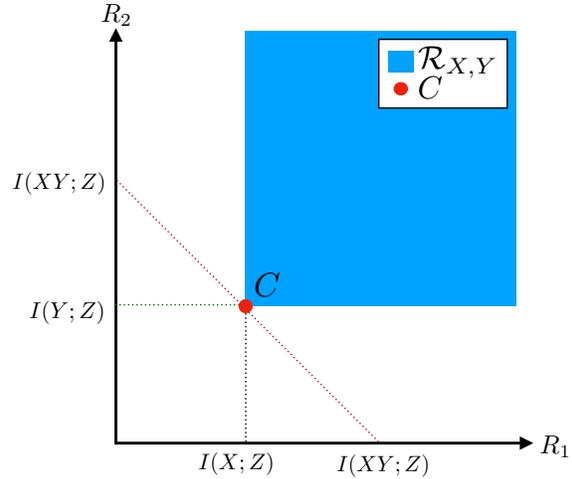


Fig. 2: Region  $\mathcal{R}_{X,Y}$  in Case 2:  $I(XY;Z) = I(X;Z) + I(Y;Z)$ .

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  $H(X|UZ)$ ,  $H(U|Z)$ ,  $H(V|UZ)$  for User 1 and the two virtual users, respectively.

- The encoding at Transmitter 1 is described in Algorithm 1 and uses

- A hash function  $G_X : \{0, 1\}^N \rightarrow \{0, 1\}^{r_X}$  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

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

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

- 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  $\tilde{p}_{X^{1:N}}$  satisfies  $\mathbb{V}(\tilde{p}_{X^{1:N}}, q_{X^{1:N}}) \leq \delta(N)$ , where  $\delta(N)$  is such that  $\lim_{N \rightarrow +\infty} \delta(N) = 0$ .

In Algorithm 1, the hash function output  $\tilde{E}_i$ ,  $i \in \llbracket 2, k \rrbracket$ , 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  $G_U : \{0, 1\}^N \rightarrow \{0, 1\}^{r_U}$  and  $G_V : \{0, 1\}^N \rightarrow \{0, 1\}^{r_V}$  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

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

- 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  $\tilde{p}_{U^{1:N}}$  satisfies  $\mathbb{V}(\tilde{p}_{U^{1:N}}, q_{U^{1:N}}) \leq \delta(N)$ , where  $\delta(N)$  is such that  $\lim_{N \rightarrow +\infty} \delta(N) = 0$ .
- 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  $\tilde{p}_{V^{1:N}}$  satisfies  $\mathbb{V}(\tilde{p}_{V^{1:N}}, q_{V^{1:N}}) \leq \delta(N)$ , where  $\delta(N)$  is such that  $\lim_{N \rightarrow +\infty} \delta(N) = 0$ .

In Algorithm 2, the hash function outputs  $\tilde{D}_i$  and  $\tilde{F}_i$ ,  $i \in \llbracket 2, k \rrbracket$ , 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.

### C. 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  $V \leftarrow Y$ .

## V. CODING SCHEME ANALYSIS

### A. Coding Scheme Analysis for Case 1

First, we show that in each encoding Block  $i \in \llbracket 1, k \rrbracket$ , the random variables  $\tilde{U}_i^{1:N}$ ,  $\tilde{V}_i^{1:N}$ ,  $\tilde{X}_i^{1:N}$ ,  $\tilde{Y}_i^{1:N}$ ,  $\tilde{Z}_i^{1:N}$  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

### 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  $i \in \llbracket 2, k \rrbracket$ , 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  $\tilde{X}_1^{1:N} \triangleq e_N^X(E_1)$
- 4:   **else if**  $i > 1$  **then**
- 5:     Define  $\tilde{E}_i \triangleq G_X(\tilde{X}_{i-1}^{1:N})$
- 6:     Define  $\tilde{X}_i^{1:N} \triangleq e_N^X(\tilde{E}_i \| E_i)$ , where  $\|$  denotes concatenation
- 7:   **end if**
- 8:   Send  $\tilde{X}_i^{1:N}$  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  $i \in \llbracket 2, k \rrbracket$ , 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  $i \in \llbracket 2, k \rrbracket$ , a vector  $F_i$  of  $N(I(V; UZ) + \epsilon_1)$  uniformly distributed bits.

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

all blocks. To do so, we show that the recycled randomness  $\tilde{E}_i, \tilde{D}_i, \tilde{F}_i$  in Block  $i \in \llbracket 2, k \rrbracket$  that appears in Line 5 of Algorithms 1 and 2 is 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 IV-B achieves the desired rate-tuple.

For convenience, define  $\tilde{E}_1 \triangleq \emptyset$ ,  $\tilde{D}_1 \triangleq \emptyset$ , and  $\tilde{F}_1 \triangleq \emptyset$ . Let

$$\tilde{p}_{E_i D_i F_i X_i^{1:N} U_i^{1:N} V_i^{1:N} Y_i^{1:N} Z_i^{1:N}} \quad (8)$$

denote the joint probability distribution of the random variables  $\tilde{E}_i, \tilde{D}_i, \tilde{F}_i, \tilde{X}_i^{1:N}, \tilde{U}_i^{1:N}, \tilde{V}_i^{1:N}, \tilde{Y}_i^{1:N}$ , and  $\tilde{Z}_i^{1:N}$  created in Block  $i \in \llbracket 1, k \rrbracket$  of the coding scheme of Section IV-B.

We first prove in the following lemma that in Block  $i \in \llbracket 2, k \rrbracket$ , if the inputs  $\tilde{X}_{i-1}^{1:N}, \tilde{U}_{i-1}^{1:N}, \tilde{V}_{i-1}^{1:N}$  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  $p_E^{unif}, p_D^{unif}, p_F^{unif}$  denote the uniform distri-

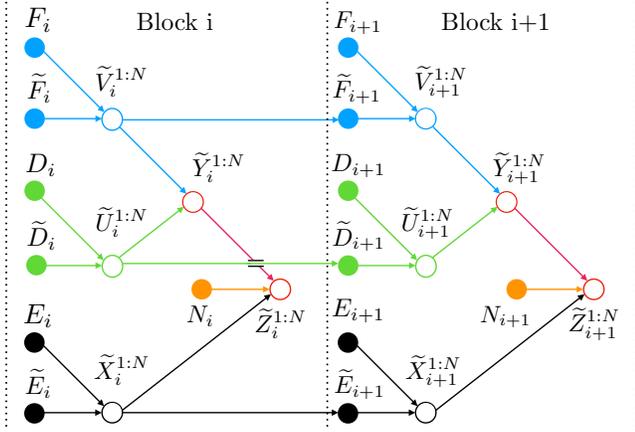


Fig. 3: Dependence graph for the random variables involved in the encoding for Case 1.  $N_i, i \in \llbracket 1, k \rrbracket$ , is the channel noise corresponding to the transmission over Block  $i$ . For Block  $i \in \llbracket 2, k \rrbracket$ ,  $(D_i, \tilde{D}_i), (F_i, \tilde{F}_i), (E_i, \tilde{E}_i)$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

butions over  $\{0, 1\}^{r_X}, \{0, 1\}^{r_U}, \{0, 1\}^{r_V}$ , respectively. Then,

$$\mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})Z^{1:N}}, p_E^{unif} p_D^{unif} p_F^{unif} q_{Z^{1:N}}) \leq \delta^{(0)}(N),$$

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 B, 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  $\mathcal{S} \subseteq \mathcal{A}$ ,

$$\mathbb{V}(w_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}, q_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}) \leq 1/N, \quad (9)$$

$$H_{\infty}(w_{T_{\mathcal{S}}^{1:N} Z^{1:N}} | q_{Z^{1:N}}) \geq NH(T_{\mathcal{S}} | Z) - N\delta_{\mathcal{S}}(N), \quad (10)$$

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 B, 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

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

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

$$\begin{aligned} & \mathbb{V}(q_{EDFZ^{1:N}}, p_E^{unif} p_D^{unif} p_F^{unif} q_{Z^{1:N}}) \\ & \stackrel{(a)}{\leq} \mathbb{V}(q_{EDFZ^{1:N}}, w_{EDFZ^{1:N}}) \\ & \quad + \mathbb{V}(w_{EDFZ^{1:N}}, p_E^{unif} p_D^{unif} p_F^{unif} q_{Z^{1:N}}) \\ & \stackrel{(b)}{=} \mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})Z^{1:N}}, \\ & \quad w_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})Z^{1:N}}) \\ & \quad + \mathbb{V}(w_{EDFZ^{1:N}}, p_E^{unif} p_D^{unif} p_F^{unif} q_{Z^{1:N}}) \end{aligned}$$

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

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 B 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

$$\begin{aligned} & \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{A}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - NH(T_{\mathcal{S}} | Z) + N\delta_{\mathcal{A}}(N)}} \\ & \stackrel{(a)}{=} \left( 2^{N(H(X|UZ) - \frac{\epsilon_1}{2}) - NH(X|Z)} \right. \\ & \quad + 2^{N(H(U|Z) - \frac{\epsilon_1}{2}) - NH(U|Z)} \\ & \quad + 2^{N(H(V|ZX) - \frac{\epsilon_1}{2}) - NH(V|Z)} \\ & \quad + 2^{N(H(X|UZ) - \frac{\epsilon_1}{2}) + N(H(U|Z) - \frac{\epsilon_1}{2}) - NH(XU|Z)} \\ & \quad + 2^{N(H(U|Z) - \frac{\epsilon_1}{2}) + N(H(V|ZX) - \frac{\epsilon_1}{2}) - NH(UV|Z)} \\ & \quad + 2^{N(H(V|ZX) - \frac{\epsilon_1}{2}) + N(H(X|UZ) - \frac{\epsilon_1}{2}) - NH(VX|Z)} \\ & \quad \left. + 2^{N(H(X|UZ) - \frac{\epsilon_1}{2}) + N(H(U|Z) - \frac{\epsilon_1}{2}) + N(H(V|ZX) - \frac{\epsilon_1}{2})} \right. \\ & \quad \left. \times 2^{-NH(XUV|Z)} \right)^{\frac{1}{2}} \times 2^{\frac{1}{2}N\delta_{\mathcal{A}}(N)} \\ & \stackrel{(b)}{=} \left( 2^{-NI(X;U|Z) - N\frac{\epsilon_1}{2}} + 2^{-N\frac{\epsilon_1}{2}} + 2^{-NI(V;UX|Z) - N\frac{\epsilon_1}{2}} \right. \\ & \quad + 2^{-N\epsilon_1} + 2^{-N\epsilon_1 - NI(V;X|UZ)} + 2^{-N\frac{3\epsilon_1}{2}} \\ & \quad \left. + 2^{-NI(V;U|ZX) - NI(X;U|Z) - N\epsilon_1} \right)^{\frac{1}{2}} \times 2^{\frac{1}{2}N\delta_{\mathcal{A}}(N)} \\ & \stackrel{(c)}{\leq} \delta^{(0)}(N) - 2/N \xrightarrow{N \rightarrow +\infty} 0, \end{aligned}$$

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  $\epsilon_1 = 2(\delta_{\mathcal{A}}(N) + \xi)$ .  $\square$

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  $i \in \llbracket 1, k \rrbracket$ , we have

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

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

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

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

$$\begin{aligned} &\mathbb{V}(\tilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}Z_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}) \\ &\stackrel{(a)}{=} \mathbb{V}(\tilde{p}_{Z^{1:N}|X^{1:N}Y^{1:N}}\tilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}}, \\ &\quad q_{Z^{1:N}|X^{1:N}Y^{1:N}}q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}}) \\ &\stackrel{(b)}{=} \mathbb{V}(\tilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}Y_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}}) \\ &\stackrel{(c)}{=} \mathbb{V}(\tilde{p}_{U_1^{1:N}V_1^{1:N}X_1^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}}) \\ &\stackrel{(d)}{=} \mathbb{V}(\tilde{p}_{X_1^{1:N}}\tilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}q_{U^{1:N}V^{1:N}}) \\ &\stackrel{(e)}{\leq} \mathbb{V}(\tilde{p}_{X_1^{1:N}}\tilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}\tilde{p}_{U_1^{1:N}V_1^{1:N}}) \\ &\quad + \mathbb{V}(q_{X^{1:N}}\tilde{p}_{U_1^{1:N}V_1^{1:N}}, q_{X^{1:N}}q_{U^{1:N}V^{1:N}}) \\ &\stackrel{(f)}{=} \mathbb{V}(\tilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\tilde{p}_{U_1^{1:N}}\tilde{p}_{V_1^{1:N}}, q_{U^{1:N}}q_{V^{1:N}}) \\ &\stackrel{(g)}{\leq} \mathbb{V}(\tilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\tilde{p}_{U_1^{1:N}}\tilde{p}_{V_1^{1:N}}, q_{U^{1:N}}\tilde{p}_{V_1^{1:N}}) \\ &\quad + \mathbb{V}(q_{U^{1:N}}\tilde{p}_{V_1^{1:N}}, q_{U^{1:N}}q_{V^{1:N}}) \\ &= \mathbb{V}(\tilde{p}_{X_1^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\tilde{p}_{U_1^{1:N}}, q_{U^{1:N}}) + \mathbb{V}(\tilde{p}_{V_1^{1:N}}, q_{V^{1:N}}) \\ &\stackrel{(h)}{\leq} 3\delta(N), \end{aligned} \quad (13)$$

where (a) holds by the two Markov chains  $(U^{1:N}, V^{1:N}) - (X^{1:N}, Y^{1:N}) - Z^{1:N}$  and  $(\tilde{U}_1^{1:N}, \tilde{V}_1^{1:N}) - (\tilde{X}_1^{1:N}, \tilde{Y}_1^{1:N}) - \tilde{Z}_1^{1:N}$ , (b) holds because  $q_{Z^{1:N}|X^{1:N}Y^{1:N}} = \tilde{p}_{Z_1^{1:N}|X_1^{1:N}Y_1^{1:N}}$ , (c) holds by (12), (d) holds because  $X^{1:N}$  is independent from  $(U^{1:N}, V^{1:N})$  and  $\tilde{X}_1^{1:N}$  is independent from  $(\tilde{U}_1^{1:N}, \tilde{V}_1^{1:N})$ , (e) holds by the triangle inequality, (f) holds because  $U^{1:N}$  is independent from  $V^{1:N}$  and  $\tilde{U}_1^{1:N}$  is independent from  $\tilde{V}_1^{1:N}$ , (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  $i \in \llbracket 2, k-1 \rrbracket$ , the lemma holds. For  $i \in \llbracket 2, k \rrbracket$ , consider  $\bar{E}_i, \bar{D}_i, \bar{F}_i$  distributed according to  $p_E^{unif}, p_D^{unif}, p_F^{unif}$ , 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  $i \in \llbracket 1, k-1 \rrbracket$ , we have

$$\begin{aligned} &\mathbb{V}(\tilde{p}_{U_{i+1}^{1:N}V_{i+1}^{1:N}X_{i+1}^{1:N}Y_{i+1}^{1:N}Z_{i+1}^{1:N}}, q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}}) \\ &\stackrel{(a)}{\leq} \mathbb{V}(\tilde{p}_{X_{i+1}^{1:N}}, q_{X^{1:N}}) + \mathbb{V}(\tilde{p}_{U_{i+1}^{1:N}}, q_{U^{1:N}}) + \mathbb{V}(\tilde{p}_{V_{i+1}^{1:N}}, q_{V^{1:N}}) \\ &\stackrel{(b)}{\leq} \mathbb{V}(\tilde{p}_{X_{i+1}^{1:N}}, p_{\bar{X}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{X}_{i+1}^{1:N}}, q_{X^{1:N}}) \\ &\quad + \mathbb{V}(\tilde{p}_{U_{i+1}^{1:N}}, p_{\bar{U}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{U}_{i+1}^{1:N}}, q_{U^{1:N}}) \end{aligned}$$

$$\begin{aligned} &+ \mathbb{V}(\tilde{p}_{V_{i+1}^{1:N}}, p_{\bar{V}_{i+1}^{1:N}}) + \mathbb{V}(p_{\bar{V}_{i+1}^{1:N}}, q_{V^{1:N}}) \\ &\stackrel{(c)}{\leq} 3\delta(N) + \mathbb{V}(\tilde{p}_{X_{i+1}^{1:N}}, p_{\bar{X}_{i+1}^{1:N}}) + \mathbb{V}(\tilde{p}_{U_{i+1}^{1:N}}, p_{\bar{U}_{i+1}^{1:N}}) \\ &\quad + \mathbb{V}(\tilde{p}_{V_{i+1}^{1:N}}, p_{\bar{V}_{i+1}^{1:N}}) \\ &\stackrel{(d)}{\leq} 3\delta(N) + \mathbb{V}(\tilde{p}_{E_{i+1}}, p_E^{unif}) + \mathbb{V}(\tilde{p}_{D_{i+1}}, p_D^{unif}) \\ &\quad + \mathbb{V}(\tilde{p}_{F_{i+1}}, p_F^{unif}), \end{aligned} \quad (14)$$

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

$$\begin{aligned} &\max\left(\mathbb{V}(\tilde{p}_{E_{i+1}}, p_E^{unif}), \mathbb{V}(\tilde{p}_{D_{i+1}}, p_D^{unif}), \mathbb{V}(\tilde{p}_{F_{i+1}}, p_F^{unif})\right) \\ &\leq \mathbb{V}(\tilde{p}_{E_{i+1}D_{i+1}F_{i+1}}, p_E^{unif}p_D^{unif}p_F^{unif}) \\ &\stackrel{(a)}{\leq} \mathbb{V}(\tilde{p}_{E_{i+1}D_{i+1}F_{i+1}}, q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}) \\ &\quad + \mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}, p_E^{unif}p_D^{unif}p_F^{unif}) \\ &\stackrel{(b)}{=} \mathbb{V}(\tilde{p}_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}, \\ &\quad q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}) \\ &\quad + \mathbb{V}(q_{G_X(X^{1:N})G_U(U^{1:N})G_V(V^{1:N})}, p_E^{unif}p_D^{unif}p_F^{unif}) \\ &\stackrel{(c)}{\leq} \mathbb{V}(\tilde{p}_{X_i^{1:N}U_i^{1:N}V_i^{1:N}}, q_{X^{1:N}U^{1:N}V^{1:N}}) + \delta^{(0)}(N) \\ &\stackrel{(d)}{\leq} \delta_i(N) + \delta^{(0)}(N), \end{aligned} \quad (15)$$

where (a) holds by the triangle inequality, (b) holds because  $\bar{E}_{i+1} \triangleq G_X(\bar{X}_{i+1}^{1:N})$ ,  $\bar{D}_{i+1} \triangleq G_U(\bar{U}_{i+1}^{1:N})$ ,  $\bar{F}_{i+1} \triangleq G_V(\bar{V}_{i+1}^{1:N})$  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

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

□

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

**Lemma 4.** For  $i \in \llbracket 2, k \rrbracket$ , we have

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

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

*Proof.* We have

$$\begin{aligned} &\mathbb{V}(\tilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \tilde{p}_{Z_{i-1}^{1:N}}\tilde{p}_{E_iD_iF_i}) \\ &\stackrel{(a)}{\leq} \mathbb{V}(\tilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \tilde{p}_{Z_{i-1}^{1:N}}p_E^{unif}p_D^{unif}p_F^{unif}) \\ &\quad + \mathbb{V}(\tilde{p}_{Z_{i-1}^{1:N}}p_E^{unif}p_D^{unif}p_F^{unif}, \tilde{p}_{Z_{i-1}^{1:N}}\tilde{p}_{E_iD_iF_i}) \\ &\leq 2\mathbb{V}(\tilde{p}_{Z_{i-1}^{1:N}E_iD_iF_i}, \tilde{p}_{Z_{i-1}^{1:N}}p_E^{unif}p_D^{unif}p_F^{unif}) \end{aligned}$$

$$\begin{aligned}
&\stackrel{(b)}{\leq} 2 \left( \mathbb{V}(\tilde{p}_{E_i D_i F_i Z_{1:i-1}^{1:N}}, q_{EDFZ^{1:N}}) \right. \\
&\quad + \mathbb{V}(q_{EDFZ^{1:N}}, p_{\tilde{E}}^{unif} p_{\tilde{D}}^{unif} p_{\tilde{F}}^{unif} q_{Z^{1:N}}) \\
&\quad \left. + \mathbb{V}(p_{\tilde{E}}^{unif} p_{\tilde{D}}^{unif} p_{\tilde{F}}^{unif} q_{Z^{1:N}}, p_{\tilde{E}}^{unif} p_{\tilde{D}}^{unif} p_{\tilde{F}}^{unif} \tilde{p}_{Z_{1:i-1}^{1:N}}) \right) \\
&\stackrel{(c)}{\leq} 2 \left( \mathbb{V}(\tilde{p}_{X_{i-1}^{1:N} U_{i-1}^{1:N} V_{i-1}^{1:N} Z_{i-1}^{1:N}}, q_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}) \right. \\
&\quad + \mathbb{V}(q_{EDFZ^{1:N}}, p_{\tilde{E}}^{unif} p_{\tilde{D}}^{unif} p_{\tilde{F}}^{unif} q_{Z^{1:N}}) \\
&\quad \left. + \mathbb{V}(q_{Z^{1:N}}, \tilde{p}_{Z_{1:i-1}^{1:N}}) \right) \\
&\stackrel{(d)}{\leq} 2(2\mathbb{V}(\tilde{p}_{X_{i-1}^{1:N} U_{i-1}^{1:N} V_{i-1}^{1:N} Z_{i-1}^{1:N}}, q_{X^{1:N} U^{1:N} V^{1:N} Z^{1:N}}) + \delta^{(0)}(N)) \\
&\stackrel{(e)}{\leq} 4\delta_{i-1}(N) + 2\delta^{(0)}(N),
\end{aligned}$$

where (a) and (b) hold by the triangle inequality, (c) holds by the data processing inequality using (11) and  $\tilde{E}_i \triangleq G_X(\tilde{X}_{i-1}^{1:N})$ ,  $\tilde{D}_i \triangleq G_U(\tilde{U}_{i-1}^{1:N})$ ,  $\tilde{F}_i \triangleq G_V(\tilde{V}_{i-1}^{1:N})$  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  $i \in \llbracket 2, k \rrbracket$  is almost independent of the channel outputs in Blocks 1 to  $i-1$  considered jointly.

**Lemma 5.** For  $i \in \llbracket 2, k \rrbracket$ , we have

$$\mathbb{V} \left( \tilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i}, \tilde{p}_{Z_{1:i-1}^{1:N}} \tilde{p}_{D_i E_i F_i} \right) \leq \delta_i^{(2)}(N),$$

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  $i \in \llbracket 2, k-1 \rrbracket$ . Then, for  $i \in \llbracket 3, k \rrbracket$ , we have

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

We have

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

$$\begin{aligned}
&\left. \tilde{p}_{Z_{1:i-2}^{1:N}} \tilde{p}_{Z_{i-1}^{1:N} D_{i-1} E_{i-1} F_{i-1}} \right) + \delta_i^{(1)}(N) \\
&= 2\mathbb{V} \left( \tilde{p}_{Z_{1:i-2}^{1:N} D_{i-1} E_{i-1} F_{i-1}}, \tilde{p}_{Z_{1:i-2}^{1:N}} \tilde{p}_{D_{i-1} E_{i-1} F_{i-1}} \right) \\
&\quad + \delta_i^{(1)}(N) \\
&\stackrel{(e)}{\leq} \delta_i^{(1)}(N) + 2\delta_{i-1}^{(2)}(N) \\
&\leq \delta_i^{(2)}(N),
\end{aligned}$$

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  $(\tilde{D}_i, \tilde{E}_i, \tilde{F}_i, \tilde{Z}_{i-1}^{1:N}) - (\tilde{D}_{i-1}, \tilde{E}_{i-1}, \tilde{F}_{i-1}) - \tilde{Z}_{1:i-2}^{1:N}$ , (e) holds by the induction hypothesis.  $\square$

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

**Lemma 6.** We have

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

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

*Proof.* We have

$$\begin{aligned}
&\mathbb{V} \left( \tilde{p}_{Z_{1:k}^{1:N}}, \prod_{i=1}^k \tilde{p}_{Z_i^{1:N}} \right) \\
&\stackrel{(a)}{\leq} \sum_{i=2}^k \mathbb{V} \left( \tilde{p}_{Z_{1:i}^{1:N}} \prod_{j=i+1}^k \tilde{p}_{Z_j^{1:N}}, \tilde{p}_{Z_{1:i-1}^{1:N}} \prod_{j=i}^k \tilde{p}_{Z_j^{1:N}} \right) \\
&= \sum_{i=2}^k \mathbb{V} \left( \tilde{p}_{Z_{1:i}^{1:N}}, \tilde{p}_{Z_{1:i-1}^{1:N}} \tilde{p}_{Z_i^{1:N}} \right) \\
&\leq \sum_{i=2}^k \mathbb{V} \left( \tilde{p}_{Z_{1:i}^{1:N} D_i E_i F_i}, \tilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i} \tilde{p}_{Z_{1:i-1}^{1:N}} \right) \\
&\stackrel{(b)}{=} \sum_{i=2}^k \mathbb{V} \left( \tilde{p}_{Z_{1:i-1}^{1:N} | D_i E_i F_i} \tilde{p}_{Z_i^{1:N} D_i E_i F_i}, \tilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i} \tilde{p}_{Z_{1:i-1}^{1:N}} \right) \\
&= \sum_{i=2}^k \mathbb{V} \left( \tilde{p}_{Z_{1:i-1}^{1:N} D_i E_i F_i}, \tilde{p}_{Z_{1:i-1}^{1:N}} \tilde{p}_{D_i E_i F_i} \right) \\
&\stackrel{(c)}{\leq} \sum_{i=2}^k \delta_i^{(2)}(N) \\
&\leq (k-1) \max_{j \in \llbracket 2, k \rrbracket} \delta_j^{(2)}(N),
\end{aligned}$$

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

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

**Lemma 7.** For Block  $i \in \llbracket 1, k \rrbracket$ , we have

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

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

*Proof.* We have

$$\begin{aligned}
& \mathbb{V}(\tilde{p}_{Z^{1:k}}^{1:N}, q_{Z^{1:kN}}) \\
& \stackrel{(a)}{\leq} (k-1)\delta_k^{(2)}(N) + \mathbb{V}\left(\prod_{i=1}^k \tilde{p}_{Z_i^{1:N}}, q_{Z^{1:kN}}\right) \\
& \stackrel{(b)}{\leq} (k-1)\delta_k^{(2)}(N) + \mathbb{V}(\tilde{p}_{Z_1^{1:N}} \prod_{i=2}^k \tilde{p}_{Z_i^{1:N}}, q_{Z^{1:N}} \prod_{i=2}^k \tilde{p}_{Z_i^{1:N}}) \\
& \quad + \mathbb{V}(q_{Z^{1:N}} \prod_{i=2}^k \tilde{p}_{Z_i^{1:N}}, q_{Z^{1:kN}}) \\
& \stackrel{(c)}{\leq} (k-1)\delta_k^{(2)}(N) + \delta_1(N) + \mathbb{V}\left(\prod_{i=2}^k \tilde{p}_{Z_i^{1:N}}, q_{Z^{1:(k-1)N}}\right) \\
& \stackrel{(d)}{\leq} (k-1)\delta_k^{(2)}(N) + \sum_{i=1}^k \delta_i(N) \\
& \leq (k-1)\delta_k^{(2)}(N) + k \max_{j \in \llbracket 1, k \rrbracket} \delta_j(N),
\end{aligned}$$

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.  $\square$

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

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

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

*Proof.* Let  $k$  be such that  $\frac{1}{k} \max(H(X), H(U), H(V)) < \epsilon_0$ . Then, by the definition of  $\epsilon_1$ , we have

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

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

$$R_V = \frac{\sum_{i=1}^k |F_i|}{kN}$$

$$\begin{aligned}
&= \frac{N(H(V) + \epsilon_1) + (k-1)N(I(V; ZUX) + \epsilon_1)}{kN} \\
&\leq \frac{H(V)}{k} + I(V; ZUX) + \epsilon_1 \\
&\leq \epsilon_0 + I(V; ZUX) + \epsilon_1 \\
&\xrightarrow{N \rightarrow +\infty} I(V; ZUX) + \epsilon_0 + 2\xi.
\end{aligned}$$

$\square$

## B. 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

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

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.

## VI. 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  $\mathcal{X}_l = \{0, 1\}$ ,  $l \in \mathcal{L} \triangleq \llbracket 1, L \rrbracket$ ,  $\mathcal{Z}$  is a finite alphabet, and  $X_{\mathcal{L}} \triangleq (X_l)_{l \in \mathcal{L}}$ . The definitions in Section II-B 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*

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

where  $p_{\mathcal{T}}$  is defined over  $\mathcal{T} \triangleq \llbracket 1, |\mathcal{Z}| + 2^L - 1 \rrbracket$  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 [7]. The achievability follows from Theorem 5.  $\square$

**Theorem 5.** *The coding scheme presented in Section VI-A, 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.*

### A. Achievability Scheme

In the following, we use the notation  $X_S \triangleq (X_l)_{l \in S}$  for  $S \subseteq \mathcal{L}$ , and  $X_{1:l} \triangleq X_{\llbracket 1, l \rrbracket}$  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

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

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., [20], and the region  $\mathcal{R}(p_{X_{\mathcal{L}}})$  thus forms a contrapolymatroid [19] 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  $G_{X_l} : \{0, 1\}^N \rightarrow \{0, 1\}^{r_{X_l}}$  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

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

- 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  $\tilde{p}_{X_l^{1:N}}$  satisfies  $\mathbb{V}(\tilde{p}_{X_l^{1:N}}, q_{X_l^{1:N}}) \leq \delta(N)$ , where  $\delta(N)$  is such that  $\lim_{N \rightarrow +\infty} \delta(N) = 0$ .

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

---

### 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.

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

### B. Achievability Scheme Analysis

For convenience, define, for any  $l \in \mathcal{L}$ ,  $\tilde{E}_{l,1} \triangleq \emptyset$ . Let  $\tilde{p}_{E_{1:L}, i, X_{1:L}, Z^{1:N}}$  denote the joint probability distribution of the random variables  $\tilde{E}_{l,i}$ ,  $\tilde{X}_{l,i}^{1:N}$ , and  $\tilde{Z}_i^{1:N}$ ,  $l \in \mathcal{L}$ , created in Block  $i \in [1, k]$  of the coding scheme of Section VI-A.

We prove in the following lemma that in Block  $i \in [2, k]$ , if the inputs  $\tilde{X}_{1:L, i-1}^{1:N}$  of the hash functions  $(G_{X_l})_{l \in \mathcal{L}}$  are re-

placed by  $X_{1:L}^{1:N}$  distributed according to  $q_{X_{1:L}^{1:N}} \triangleq \prod_{l=1}^N q_{X_{1:L}}$ , then the outputs of these hash functions are almost jointly uniformly distributed. Define

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

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

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

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

*Proof.* Using Lemma 16 in Appendix B, 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  $\mathcal{S} \subseteq \mathcal{L}$

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

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

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 B, 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

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

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

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

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 B, (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  $\epsilon_2 = 2(\delta_{\mathcal{L}}^*(N) + \xi)$ .  $\square$

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  $i \in \llbracket 1, k \rrbracket$ ,

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

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

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

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

where (a) holds because  $q_{Z_1^{1:N} | X_{1:L,1}^{1:N}} = \tilde{p}_{Z_1^{1:N} | X_{1:L,1}^{1:N}}$ , (b) holds by the triangle inequality and because  $(\tilde{X}_{l,1}^{1:N})_{l \in \mathcal{L}}$  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  $i \in \llbracket 2, k-1 \rrbracket$ , (20) holds. For any  $l \in \mathcal{L}$  and  $i \in \llbracket 2, k \rrbracket$ , consider  $\tilde{E}_{l,i}$  distributed according to  $p_{\tilde{E}_{l,i}}^{unif}$ , the uniform distribution over  $\{0, 1\}^{r_{X_l}}$ , and let  $p_{\tilde{X}_{l,i}^{1:N}}$  denote the distribution of  $\tilde{X}_{l,i}^{1:N} \triangleq e_N^{X_l}(\tilde{E}_{l,i}, E_{l,i})$ . For  $i \in \llbracket 1, k-1 \rrbracket$ , we have

$$\begin{aligned} & \mathbb{V}(\tilde{p}_{X_{1:L,i+1}^{1:N}, Z_{i+1}^{1:N}}, q_{X_{1:L,i+1}^{1:N}, Z_{i+1}^{1:N}}) \\ &\stackrel{(a)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\tilde{p}_{X_{l,i+1}^{1:N}}, q_{X_{l,i+1}^{1:N}}) \\ &\stackrel{(b)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\tilde{p}_{X_{l,i+1}^{1:N}}, p_{\tilde{X}_{l,i+1}^{1:N}}) + \mathbb{V}(p_{\tilde{X}_{l,i+1}^{1:N}}, q_{X_{l,i+1}^{1:N}}) \\ &\stackrel{(c)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\tilde{p}_{X_{l,i+1}^{1:N}}, p_{\tilde{X}_{l,i+1}^{1:N}}) + \delta(N) \\ &\stackrel{(d)}{\leq} \sum_{l \in \mathcal{L}} \mathbb{V}(\tilde{p}_{E_{l,i+1}}, p_{\tilde{E}_{l,i+1}}^{unif}) + \delta(N) \\ &\stackrel{(e)}{\leq} \sum_{l \in \mathcal{L}} \left( \delta(N) + \mathbb{V}(\tilde{p}_{E_{l,i+1}}, q_{G_{X_l}(X_l^{1:N})}) \right. \\ &\quad \left. + \mathbb{V}(q_{G_{X_l}(X_l^{1:N})}, p_{\tilde{E}_{l,i+1}}^{unif}) \right) \\ &\stackrel{(f)}{=} \sum_{l \in \mathcal{L}} \left( \delta(N) + \mathbb{V}(\tilde{p}_{G_{X_l}(X_l^{1:N})}, q_{G_{X_l}(X_l^{1:N})}) \right. \\ &\quad \left. + \mathbb{V}(q_{G_{X_l}(X_l^{1:N})}, p_{\tilde{E}_{l,i+1}}^{unif}) \right) \\ &\stackrel{(g)}{\leq} \sum_{l \in \mathcal{L}} \delta(N) + \mathbb{V}(\tilde{p}_{X_{l,i}^{1:N}}, q_{X_{l,i}^{1:N}}) + \delta^{*(0)}(N) \end{aligned}$$

$$\begin{aligned} & \stackrel{(h)}{\leq} \sum_{l \in \mathcal{L}} \delta(N) + \delta_i^*(N) + \delta^{*(0)}(N) \\ &= L \left( \delta(N) + \delta_i^*(N) + \delta^{*(0)}(N) \right), \end{aligned}$$

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

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

**Lemma 11.** For  $i \in \llbracket 2, k \rrbracket$ , we have

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

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

*Proof.* We have

$$\begin{aligned} & \mathbb{V}(\tilde{p}_{E_{1:L,i}, Z_{i-1}^{1:N}}, \tilde{p}_{E_{1:L,i}}, \tilde{p}_{Z_{i-1}^{1:N}}) \\ &\stackrel{(a)}{\leq} \mathbb{V}(\tilde{p}_{E_{1:L,i}, Z_{i-1}^{1:N}}, p_{E_{1:L,i}}^{unif} \tilde{p}_{Z_{i-1}^{1:N}}) \\ &\quad + \mathbb{V}(p_{E_{1:L,i}}^{unif} \tilde{p}_{Z_{i-1}^{1:N}}, \tilde{p}_{E_{1:L,i}}, \tilde{p}_{Z_{i-1}^{1:N}}) \\ &\leq 2\mathbb{V}(\tilde{p}_{E_{1:L,i}, Z_{i-1}^{1:N}}, p_{E_{1:L,i}}^{unif} \tilde{p}_{Z_{i-1}^{1:N}}) \\ &\stackrel{(b)}{\leq} 2 \left( \mathbb{V}(\tilde{p}_{E_{1:L,i}, Z_{i-1}^{1:N}}, q_{G_{X_{1:L}}(X_{1:L}^{1:N}) Z_{i-1}^{1:N}}) \right. \\ &\quad \left. + \mathbb{V}(q_{G_{X_{1:L}}(X_{1:L}^{1:N}) Z_{i-1}^{1:N}}, p_{E_{1:L,i}}^{unif} q_{Z_{i-1}^{1:N}}) \right. \\ &\quad \left. + \mathbb{V}(p_{E_{1:L,i}}^{unif} q_{Z_{i-1}^{1:N}}, p_{E_{1:L,i}}^{unif} \tilde{p}_{Z_{i-1}^{1:N}}) \right) \\ &\stackrel{(c)}{\leq} 2(\mathbb{V}(\tilde{p}_{X_{1:L,i-1}^{1:N}, Z_{i-1}^{1:N}}, q_{X_{1:L,i-1}^{1:N}, Z_{i-1}^{1:N}}) + \delta^{*(0)}(N) \\ &\quad + \mathbb{V}(q_{Z_{i-1}^{1:N}}, \tilde{p}_{Z_{i-1}^{1:N}})) \\ &\stackrel{(d)}{\leq} 4\delta_{i-1}^*(N) + 2\delta^{*(0)}(N), \end{aligned}$$

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

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

**Lemma 12.** For  $i \in \llbracket 2, k \rrbracket$ , we have

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

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  $i \in \llbracket 2, k-1 \rrbracket$ . Then, for  $i \in \llbracket 3, k \rrbracket$ , we have

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

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

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*

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

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

**Lemma 14.** *For block  $i \in \llbracket 1, k \rrbracket$ , we have*

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

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 VI-A achieves the desired rate-tuple.

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

*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  $\epsilon_2$ , for any  $l \in \mathcal{L}$ , we have

$$\begin{aligned}
R_l &= \frac{\sum_{i=1}^k |E_{l,i}|}{kN} \\
&= \frac{N(H(X_l) + \epsilon_2) + (k-1)N(I(X_l; Z | X_{1:l-1}) + \epsilon_2)}{kN}
\end{aligned}$$

$$\begin{aligned}
& \leq \frac{H(X_l)}{k} + I(X_l; Z | X_{1:l-1}) + \epsilon_2 \\
& \leq \epsilon_0 + I(X_l; Z | X_{1:l-1}) + \epsilon_2 \\
& \xrightarrow{N \rightarrow +\infty} I(X_l; Z | X_{1:l-1}) + \epsilon_0 + 2\xi.
\end{aligned}$$

$\square$

## VII. 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.

## APPENDIX A

### AN EXPLICIT CODING SCHEME FOR SOURCE RESOLVABILITY

Let  $n \in \mathbb{N}$  and  $N \triangleq 2^n$ . Let  $G_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes n}$  be the source polarization matrix defined in [21]. For any set  $\mathcal{A} \subseteq \llbracket 1, N \rrbracket$  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

$$\begin{aligned}
\mathcal{V}_X &\triangleq \{i \in \llbracket 1, N \rrbracket : H(A^i | A^{1:i-1}) > 1 - \delta_N\}, \\
\mathcal{H}_X &\triangleq \{i \in \llbracket 1, N \rrbracket : H(A^i | A^{1:i-1}) > \delta_N\}.
\end{aligned}$$

### Algorithm 4 Encoding algorithm for source resolvability

**Require:** A vector  $R$  of  $|\mathcal{V}_X|$  uniformly distributed bits

- 1: Define  $\tilde{A}^{1:N}[\mathcal{V}_X] \triangleq R$
- 2: Define  $\tilde{A}^j$  according to  $q_{A^j | A^{1:j-1}}$  for  $j \in \mathcal{V}_X^c \setminus \mathcal{H}_X^c$  and as  $\tilde{A}^j \triangleq \operatorname{argmax}_{a \in \{0,1\}} q_{A^j | A^{1:j-1}}(a | a^{1:j-1})$  for  $j \in \mathcal{H}_X^c$
- 3: Define  $\tilde{X}^{1:N} \triangleq \tilde{A}^{1:N} G_n$

In Algorithm 4, the distribution of  $\tilde{X}^{1:N}$  is such that  $\lim_{N \rightarrow \infty} \mathbb{V}(\tilde{p}_{\tilde{X}^{1:N}}, q_{\tilde{X}^{1:N}}) = 0$  by [22], [23]. Moreover, the rate of  $R$  is  $\frac{|\mathcal{V}_X|}{N} \xrightarrow{N \rightarrow +\infty} H(X)$  by [24, Lemma 1], and the rate of randomness used in Line 2 is 0 by [10, 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 sub-normalized 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 sub-normalized 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** ([25], [26, Lemma 2]). Define  $\mathcal{A} \triangleq \llbracket 1, A \rrbracket$ . Let  $(\mathcal{T}_a)_{a \in \mathcal{A}}$  be  $A$  finite alphabets and define for  $\mathcal{S} \subseteq \mathcal{A}$ ,  $\mathcal{T}_{\mathcal{S}} \triangleq \times_{a \in \mathcal{S}} \mathcal{T}_a$ . 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

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

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 [27], [28], i.e.,

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

**Lemma 17** ([25], [26, Lemma 1]). Consider a subnormalized non-negative function  $p_{X_{\mathcal{L}} Z}$  defined over  $\times_{l \in \mathcal{L}} \mathcal{X}_l \times \mathcal{Z}$ , 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  $F_l : \{0, 1\}^{r_l} \rightarrow \{0, 1\}^{r_l}$ , 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  $\text{supp}(q_Z) \subseteq \text{supp}(p_Z)$ , 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  $\llbracket 1, 2^{r_{\mathcal{L}}} \rrbracket$  and  $\llbracket 1, s_{\mathcal{L}} \rrbracket$ , respectively.

## APPENDIX C PROOF OF LEMMA 1

The proof is similar to [16]. We have

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

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 [16, Lemma 6] that  $I(X; ZU)$  is a continuous function of  $\epsilon$ , 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.

## REFERENCES

- [1] 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*, 2019, pp. 116–123.
- [2] —, "Explicit construction of multiple access channel resolvability codes from source resolvability codes," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2020.
- [3] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 472–487, 1998.
- [4] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 752–772, 1993.
- [5] 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.
- [6] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. of IEEE Inf. Theory Workshop 2010*, pp. 1–5.
- [7] M. Frey, I. Bjelakovic, and S. Stanczak, "The MAC resolvability region, semantic security and its operational implications," *arXiv preprint arXiv:1710.02342*, 2017.
- [8] M. Bloch and J. Kliewer, "Strong coordination over a line network," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2013, pp. 2319–2323.
- [9] M. Bloch, L. Luzzi, and J. Kliewer, "Strong coordination with polar codes," in *Proc. of the Annual Allerton Conf. on Communication, Control, and Computing*, 2012, pp. 565–571.
- [10] 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.
- [11] 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.
- [12] R. Amjad and G. Kramer, "Channel resolvability codes based on concatenation and sparse linear encoding," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2015, pp. 2111–2115.
- [13] 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*, 2014, pp. 466–470.
- [14] T. Han, "Information-spectrum methods in information theory volume 50 of," *Applications of Mathematics*, 2003.
- [15] S. Vadhan, "Pseudorandomness," *Foundations and Trends® in Theoretical Computer Science*, vol. 7, no. 1–3, pp. 1–336, 2012.
- [16] 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.
- [17] 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.
- [18] R. Chou, M. R. Bloch, and J. Kliewer, "Polar coding for empirical and strong coordination via distribution approximation," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2015, pp. 1512–1516.
- [19] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," in *Combinatorial Optimization*. Springer, 2003, pp. 11–26.
- [20] 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.
- [21] E. Arıkan, "Source polarization," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2010, pp. 899–903.
- [22] 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.
- [23] —, "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 Computing*, 2015, pp. 1380–1385.
- [24] 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.
- [25] R. Chou, "Secret sharing over a public channel from correlated random variables," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2018, pp. 991–995.
- [26] —, "Distributed secret sharing over a public channel from correlated random variables," *arXiv preprint arXiv:2110.10307*, 2021.
- [27] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.
- [28] 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*, 2013, pp. 2715–2719.