2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)
Allerton Park and Retreat Center
Monticello, IL, USA, September 24-27, 2019

Explicit Low-complexity Codes for Multiple Access Channel Resolvability

Rumia Sultana and Rémi A. Chou

***Abstract*—We design an explicit low-complexity coding scheme that achieves the multiple access channel resolvability region for an arbitrary discrete memoryless multiple access channel whose input alphabets have prime cardinalities. Unlike previous works, we do not assume channel symmetry and rely on rate-splitting to avoid time sharing when it is known to be unnecessary. The idea of our construction is to reduce the problem of multiple access channel resolvability to a combination of several source resolvability problems. Our coding scheme relies on polar codes for source coding to implement source resolvability, and a block Markov coding scheme that performs randomness recycling in the different encoding blocks.**

I. Introduction

Channel resolvability has been introduced for point-to-point channels and multiple access channels in [1] and [2], respectively. Applications of these notions include strong secrecy for the point-to-point [3], [4] and multiple access [5], [6] wiretap channels, cooperative jamming [5], semantic security for the point-to-point [7] and the multiple access wiretap channel [8], and strong coordination in networks [9].

Beyond existence results of channel resolvability codes provided in the above references, several works have investigated the constructions of such codes. Explicit and low-complexity constructions based on polar codes for channel resolvability have been proposed for binary *symmetric* channels [10] and discrete memoryless channels whose input alphabets have prime cardinalities [11]. Another explicit construction based on injective group homomorphisms has been proposed in [12] for channel resolvability over binary *symmetric* channels. Low-complexity, but non-explicit, linear coding schemes for channel resolvability over arbitrary memoryless channels have also been proposed in [13]. As for multiple access channel resolvability, two explicit constructions have been proposed in [14] for *symmetric* multiple access channels, one based on invertible extractors and a second one based on injective group homomorphisms.

In this paper, we focus on code constructions for multiple access channel resolvability. Our contribution is to provide an explicit and low-complexity coding scheme that achieves the multiple access channel resolvability region [8] of an *abritrary* discrete memoryless multiple access channel whose input alphabets have prime cardinalities. We also highlight that our proposed coding scheme does not require time-sharing when it is known to be unnecessary. The main idea of our coding scheme is to reduce the problem of multiple access channel resolvability to a combination of several source resolvability problems. Our coding scheme involves block-Markov encoding that takes advantage of randomness recycling in consecutive encoding blocks, and polar codes for source coding [15] to implement source resolvability. To avoid, as much as possible, time-sharing, we also implement the idea of rate splitting developed in [16] for multiple access channels. 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., [17]. Finally, note that our proposed construction does not use the same tools as the one used in [14] for multiple access channel resolvability over symmetric multiple access channels, and that it remains unclear whether the coding schemes in [14] could be extended to achieve the multiple access channel resolvability region of an arbitrary multiple access channel.

The remainder of the paper is organized as follows. The problem statement is provided in Section III. Our proposed coding scheme and its analysis are provided in Section IV and Section V, respectively. Finally, Section VI provides concluding remarks.

II. Notation

Let $[\![a,b]\!]$ be the set of integers between $\lfloor a \rfloor$ and $\lceil b \rceil$. For $n \in \mathbb{N}$, let $G_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes n}$ be the source polarization matrix defined in [15]. 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 any set $\mathcal{A} \subset [\![1, N]\!]$, 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 Kullback-Leibler divergence between p_X and q_X as

$$\mathbb{D}(p_X||q_X) \triangleq \sum_{x\in\mathcal{X}} p_X(x) \log \frac{p_X(x)}{q_X(x)}.$$

For joint probability distributions p_{XY} and q_{XY} defined over $\mathcal{X} \times \mathcal{Y}$, the conditional Kullback-Leibler divergence is written as

$$\mathbb{E}_{p_X}[\mathbb{D}(p_{Y|X}\|q_{Y|X})] \triangleq \sum_{x\in\mathcal{X}} p_X(x)\mathbb{D}(p_{Y|X=x}\|q_{Y|X=x}).$$

Rumia Sultana and Rémi A. Chou are with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS.
This work was supported in part by NSF grant CCF-1850227.
E-mails: rxsultana@shockers.wichita.edu; remi.chou@wichita.edu.

III. Problem Statement

Consider a discrete memoryless multiple access channel $(\mathcal{X}\times\mathcal{Y}, q_{Z|XY}, \mathcal{Z})$, where $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are finite alphabets. 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 $\mathcal{S}_1 \triangleq [\![1, 2^{NR_1}]\!]$ 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: the transmitters form $f_{1,N}(S_1)$ and $f_{2,N}(S_2)$, 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 $\lim_{N\to+\infty}\mathbb{D}(\widetilde{p}_{Z^{1:N}}||q_{Z^{1:N}}) = 0$, where $q_{Z^{1:N}} \triangleq \prod_{i=1}^N q_Z$ with q_Z defined in (1) and $\forall z^{1:N}\in\mathcal{Z}^N$,*

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

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

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

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 [8] 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 an explicit low-complexity coding scheme that achieves $\mathcal{R}_{q_Z}$.

IV. Coding Scheme

A. 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 $f_N : \mathcal{S} \to \mathcal{X}^N$;*

and operates as follows. The encoder forms $\widetilde{X}^{1:N} \triangleq f_N(S)$ 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*

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

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

Theorem 2 ([1]). *The source resolvability of a discrete memoryless source $(\mathcal{X}, q_X)$ is $H(q_X)$.*

B. High-level description of our coding scheme

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

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

for some product distribution p_Xp_Y on $\mathcal{X}\times\mathcal{Y}$.

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

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

Similarly, the other corner points of $\mathcal{R}'_{q_Z}$ also belong to $\mathrm{Conv}(\bigcup_{p_Xp_Y}\mathcal{R}_{X,Y})$. Next, we consider two cases to achieve the region $\mathcal{R}_{X,Y}$ for some fixed distribution p_Xp_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 $\mathcal{D}$.
- 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.

C. Encoding Scheme for Case 1

By inspecting Figure 1, we have the following proposition.

Proposition 1. *To achieve the region $\mathcal{R}_{X,Y}$ when $I(XY;Z) > I(X;Z) + I(Y;Z)$, it is sufficient to achieve any rate pair (R_1, R_2) in $\mathcal{D}$, where*

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

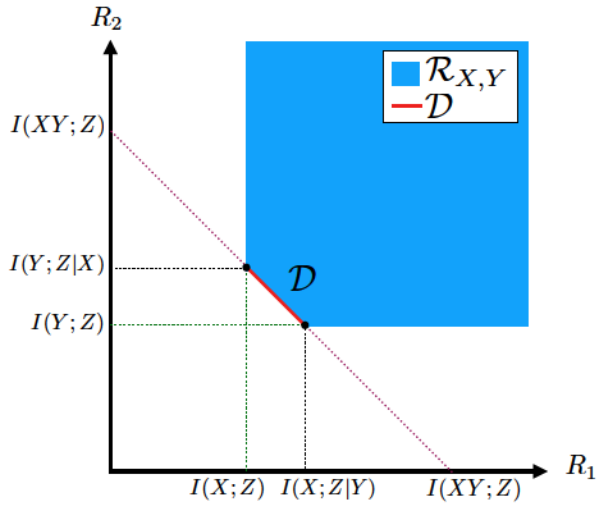

Fig. 1. Region $\mathcal{R}_{X,Y}$ in Case 1: $I(XY;Z) > I(X;Z) + I(Y;Z)$.

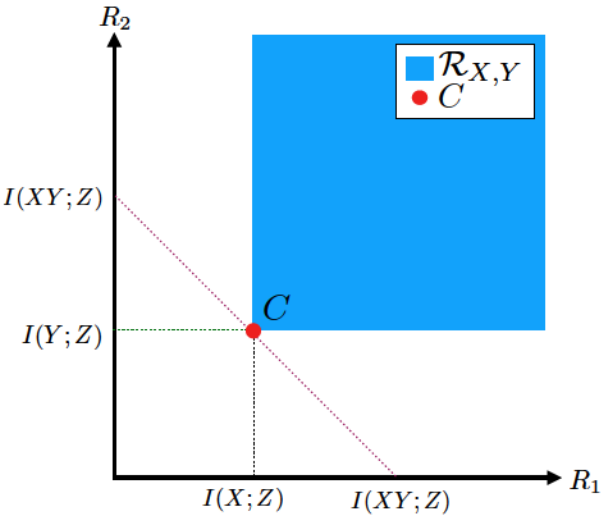

Fig. 2. Region $\mathcal{R}_{X,Y}$ in Case 2: $I(XY;Z) = I(X;Z) + I(Y;Z)$.

We will need the following results to show the achievability of $\mathcal{D}$ with rate-splitting.

Lemma 1. *As in [16, Example 3], we choose $f : \mathcal{Y} \times \mathcal{Y} \to \mathcal{Y}$, $(u,v) \mapsto \max(u,v)$, and split $(\mathcal{Y}, p_Y)$ to form $(\mathcal{Y} \times \mathcal{Y}, p_{U_\epsilon} p_{V_\epsilon}), \epsilon \in [0,1]$, such that for any $\epsilon > 0$, $p_{f(U_\epsilon,V_\epsilon)} = p_Y$, for fixed (y,u), $p_{f(U_\epsilon,V_\epsilon)|U_\epsilon}(y|u)$ is a continuous function of ϵ, and*

$$U_{\epsilon=0} = 0 = V_{\epsilon=1}, \tag{2}$$
$$U_{\epsilon=1} = f(U_{\epsilon=1}, V_{\epsilon=1}), \tag{3}$$
$$V_{\epsilon=0} = f(U_{\epsilon=0}, V_{\epsilon=0}). \tag{4}$$

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. Then, we have $I(XY;Z) = R_1 + R_U + R_V$, where we have defined the functions

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

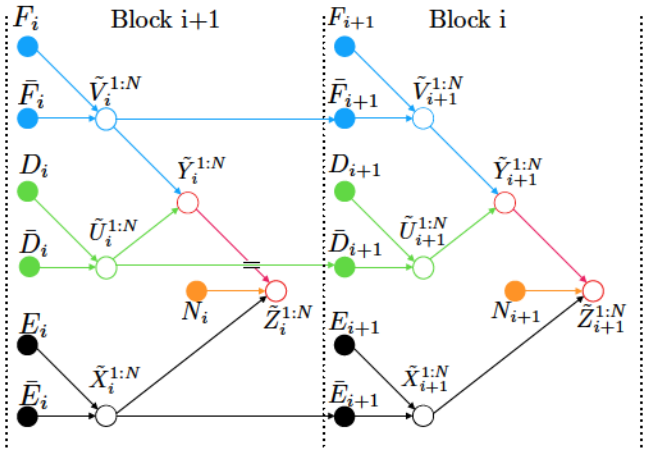

Fig. 3. Functional dependence graph of the block encoding scheme for multiple access channel resolvability. N_i, $i \in [\![1,k]\!]$, is the channel noise corresponding to the transmission over Block i. For Block i, $(E_i, \bar{E}_{i-1})$, $(D_i, \bar{D}_{i-1})$, $(F_i, \bar{F}_{i-1})$ are the randomness used at the encoder to form $\tilde{X}_i, \tilde{U}_i, \tilde{V}_i$, where $\forall i \in [\![2,k]\!]$, $\bar{E}_i = \bar{E}_{i-1}$, $\bar{D}_i = \bar{D}_{i-1}$, $\bar{F}_i = \bar{F}_{i-1}$ and E_i, D_i, F_i are only used in Block i.

$$R_V : \epsilon \mapsto I(V;Z|UX), \text{ from } [0,1] \text{ to } \mathbb{R}^+.$$

Moreover, $\epsilon \mapsto R_1(\epsilon)$ is continuous and $[I(X;Z), I(X;Z|Y)]$ is contained in its image.

Proof. The proof is similar to [16], [18]. 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 [16, 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 $(2)-(4)$, 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. □

Fix q_{UV} and consider the corresponding distribution q_{UVXYZ}. Let $N \triangleq 2^n$, $n \in \mathbb{N}$, and assume that $|\mathcal{X}|$ and $|\mathcal{Y}|$ are prime numbers. Define $X^{1:N} \triangleq C^{1:N} G_n$, $U^{1:N} \triangleq A^{1:N} G_n$, $V^{1:N} \triangleq B^{1:N} G_n$, where G_n is defined in Section II, and define for $\beta < 1/2$, $\delta_N \triangleq 2^{-N^\beta}$ and the sets

$$\begin{aligned} \mathcal{V}_U &\triangleq \left\{ i \in [\![1,N]\!] : H(A^i|A^{1:i-1}) > \log|\mathcal{Y}| - \delta_N \right\}, \\ \mathcal{V}_V &\triangleq \left\{ i \in [\![1,N]\!] : H(B^i|B^{1:i-1}) > \log|\mathcal{Y}| - \delta_N \right\}, \\ \mathcal{V}_X &\triangleq \left\{ i \in [\![1,N]\!] : H(C^i|C^{1:i-1}) > \log|\mathcal{X}| - \delta_N \right\}, \\ \mathcal{V}_{U|Z} &\triangleq \left\{ i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Z^{1:N}) \right. \\ &\qquad \left. > \log|\mathcal{Y}| - \delta_N \right\}, \end{aligned}$$

$$\mathcal{V}_{X|UZ} \triangleq \{i \in [\![1,N]\!] : H(C^i|C^{1:i-1}U^{1:N}Z^{1:N}) > \log|\mathcal{X}| - \delta_N\},$$

$$\mathcal{V}_{V|UZX} \triangleq \{i \in [\![1,N]\!] : H(B^i|B^{1:i-1}U^{1:N}Z^{1:N}X^{1:N}) > \log|\mathcal{Y}| - \delta_N\}.$$

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. We perform rate splitting for the second transmitter to get two virtual users, and then source resolvability for the discrete memoryless sources $(\mathcal{Y}, q_U)$ and $(\mathcal{Y}, q_V)$ using randomness with rates $H(U)$ and $H(V)$, respectively in Block 1. As it will be shown later the amount of randomness used in Block 1 is non-optimal. 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.

Algorithm 1 Encoding algorithm at Transmitter 1

Require: A vector $\bar{E}_1$ of $|\mathcal{V}_{X|UZ}|$ uniformly distributed symbols, and k vectors $E_{1:k}$ of $|\mathcal{V}_X \backslash \mathcal{V}_{X|UZ}|$ uniformly distributed symbols.

1: **for** Block $i = 1$ to k **do**
2: $\quad \bar{E}_i \leftarrow \bar{E}_1$
3: $\quad \widetilde{C}_i^{1:N}[\mathcal{V}_{X|UZ}] \leftarrow \bar{E}_i$
4: $\quad \widetilde{C}_i^{1:N}[\mathcal{V}_X \backslash \mathcal{V}_{X|UZ}] \leftarrow E_i$
5: $\quad$ Successively draw the remaining components of $\widetilde{C}_i^{1:N}[\mathcal{V}_X^c]$ according to

$$\widetilde{p}_{C_i^j|C_i^{1:j-1}}(c_i^j|\widetilde{C}_i^{1:j-1}) \triangleq q_{C^j|C^{1:j-1}}(c_i^j|\widetilde{C}_i^{1:j-1}) \quad \text{if } j \in \mathcal{V}_X^c \qquad (5)$$

6: $\quad$ Construct $\widetilde{X}_i^{1:N} \triangleq \widetilde{C}_i^{1:N}G_n$ and send the codeword over the channel.
7: **end for**

Remark 1. *An interpretation of the set $\mathcal{V}_{X|UZ}$ is that the sequence $C_i^{1:N}[\mathcal{V}_{X|UZ}]$ (used to form $\widetilde{X}_i^{1:N}$) is asymptotically independent of $(U^{1:N}, Z^{1:N})$ [19]–[21]. We thus choose to recycle $C_i^{1:N}[\mathcal{V}_{X|UZ}]$ in the next block to form $\widetilde{X}_{i+1}^{1:N}$. We have a similar interpretation for the sets $\mathcal{V}_{U|Z}$ and $\mathcal{V}_{V|UZX}$.*

Remark 2. *The randomizations described in (5) − (7) could be replaced by deterministic decisions for the indices $\mathcal{H}_X^c, \mathcal{H}_U^c, \mathcal{H}_V^c$, where*

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

Algorithm 2 Encoding algorithm at Transmitter 2

Require: A vector $\bar{D}_1$ of $|\mathcal{V}_{U|Z}|$ uniformly distributed symbols, and k vectors $D_{1:k}$ of $|\mathcal{V}_U \backslash \mathcal{V}_{U|Z}|$ uniformly distributed symbols. A vector $\bar{F}_1$ of $|\mathcal{V}_{V|UZX}|$ uniformly distributed symbols, and k vectors $F_{1:k}$ of $|\mathcal{V}_V \backslash \mathcal{V}_{V|UZX}|$ uniformly distributed symbols.

1: **for** Block $i = 1$ to k **do**
2: $\quad \bar{D}_i \leftarrow \bar{D}_1$
3: $\quad \bar{F}_i \leftarrow \bar{F}_1$
4: $\quad \widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}] \leftarrow \bar{D}_i$
5: $\quad \widetilde{A}_i^{1:N}[\mathcal{V}_U \backslash \mathcal{V}_{U|Z}] \leftarrow D_i$
6: $\quad \widetilde{B}_i^{1:N}[\mathcal{V}_{V|UZX}] \leftarrow \bar{F}_i$
7: $\quad \widetilde{B}_i^{1:N}[\mathcal{V}_V \backslash \mathcal{V}_{V|UZX}] \leftarrow F_i$
8: $\quad$ Successively draw the remaining components of $\widetilde{A}_i^{1:N}[\mathcal{V}_U^c]$ according to

$$\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \triangleq q_{A^j|A^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \quad \text{if } j \in \mathcal{V}_U^c \qquad (6)$$

9: $\quad$ Successively draw the remaining components of $\widetilde{B}_i^{1:N}[\mathcal{V}_V^c]$ according to

$$\widetilde{p}_{B_i^j|B_i^{1:j-1}}(b_i^j|\widetilde{B}_i^{1:j-1}) \triangleq q_{B^j|B^{1:j-1}}(b_i^j|\widetilde{B}_i^{1:j-1}) \quad \text{if } j \in \mathcal{V}_V^c \qquad (7)$$

10: $\quad$ Construct $\widetilde{U}_i^{1:N} \triangleq \widetilde{A}_i^{1:N}G_n$ and $\widetilde{V}_i^{1:N} \triangleq \widetilde{B}_i^{1:N}G_n$.
11: $\quad$ Form $\widetilde{Y}_i^{1:N} \triangleq f(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$ (as described in Lemma 1) and send the codeword over the channel.
12: **end for**

$$\mathcal{H}_V \triangleq \{i \in [\![1,N]\!] : H(B^i|B^{1:i-1}) > \delta_N\},$$

i.e., randomized decisions are only needed for the indices in $\mathcal{V}_X^c \backslash \mathcal{H}_X^c, \mathcal{V}_U^c \backslash \mathcal{H}_U^c, \mathcal{V}_V^c \backslash \mathcal{H}_V^c$, respectively, as shown in [22].

Theorem 3. *The coding scheme of Section IV-C, which operates over k blocks of length N, achieves the region $\mathcal{R}_{X,Y}$ for the discrete memoryless channel $(\mathcal{X} \times \mathcal{Y}, q_{XY|Z}, \mathcal{Z})$, where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are prime numbers. The coding scheme is explicit with complexity $\mathcal{O}(kN \log N)$.*

D. Encoding Scheme for Case 2

Fix a joint probability distribution q_{XYZ} over $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are prime numbers. Define $X^{1:N} \triangleq C^{1:N}G_n$, $Y^{1:N} \triangleq B^{1:N}G_n$, and the sets

$$\mathcal{V}_X \triangleq \{i \in [\![1,N]\!] : H(C^i|C^{1:i-1}) > \log|\mathcal{X}| - \delta_N\},$$
$$\mathcal{V}_Y \triangleq \{i \in [\![1,N]\!] : H(B^i|B^{1:i-1}) > \log|\mathcal{Y}| - \delta_N\},$$
$$\mathcal{V}_{X|Z} \triangleq \{i \in [\![1,N]\!] : H(C^i|C^{1:i-1}Z^{1:N}) > \log|\mathcal{X}| - \delta_N\},$$
$$\mathcal{V}_{Y|ZX} \triangleq \{i \in [\![1,N]\!] : H(B^i|B^{1:i-1}Z^{1:N}X^{1:N}) > \log|\mathcal{Y}| - \delta_N\}.$$

The encoding scheme operates over $k \in \mathbb{N}$ blocks of length $N \triangleq 2^n, n \in \mathbb{N}$. The encoding for the first transmitter is the same as Algorithm 1 with the substitution $U \leftarrow \emptyset$,

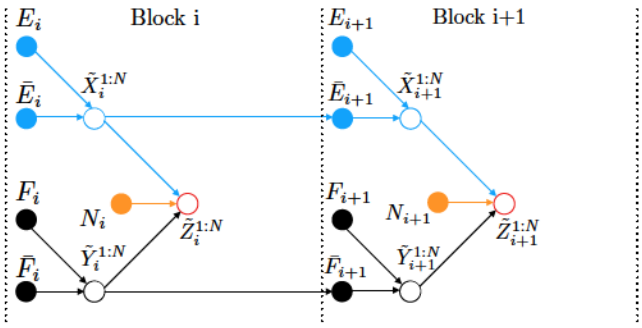

Fig. 4. Functional dependence graph of the block encoding scheme for multiple access channel resolvability. N_i, $i \in [\![1,k]\!]$, is the channel noise corresponding to the transmission over Block i. For Block i, $(E_i, \bar{E}_{i-1})$, $(F_i, \bar{F}_{i-1})$ are the randomness used at the encoder to form $\widetilde{X}_i$, $\widetilde{Y}_i$, where $\forall i \in [\![2,k]\!]$, $\bar{E}_i = \bar{E}_{i-1}$, $\bar{F}_i = \bar{F}_{i-1}$ and E_i, F_i are only used in Block i.

and for the second transmitter, the encoding is described in Algorithm 3. A high level description of the encoding scheme is as follows. For the first and second transmitters, we perform source resolvability for the discrete memoryless sources $(\mathcal{X}, q_X)$ and $(\mathcal{Y}, q_Y)$ using randomness with rates $H(X)$ and $H(Y)$, respectively. As it will be shown later the amount of randomness used is non-optimal. For the next encoding blocks, we proceed as in the Block 1 except that part of the randomness is now recycled from the previous block. Specifically, 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 can be shown to approach $H(X|Z)$ and $H(Y|ZX)$ for User 1 and User 2, respectively.

Algorithm 3 Encoding algorithm at Transmitter 2

Require: A vector $\bar{F}_1$ of $|\mathcal{V}_{Y|ZX}|$ uniformly distributed symbols, and k vectors $F_{1:k}$ of $|\mathcal{V}_Y \backslash \mathcal{V}_{Y|ZX}|$ uniformly distributed symbols.

1: **for** Block $i = 1$ to k **do**
2: $\quad \bar{F}_i \leftarrow \bar{F}_1$
3: $\quad \widetilde{B}_i^{1:N}[\mathcal{V}_{Y|ZX}] \leftarrow \bar{F}_i$
4: $\quad \widetilde{B}_i^{1:N}[\mathcal{V}_Y \backslash \mathcal{V}_{Y|ZX}] \leftarrow F_i$
5: $\quad$ Successively draw the remaining components of $\widetilde{B}_i^{1:N}[\mathcal{V}_Y^c]$ according to

$$\begin{aligned} &\widetilde{p}_{B_i^j|B_i^{1:j-1}}(b_i^j|\widetilde{B}_i^{1:j-1}) \\ &\triangleq q_{B^j|B^{1:j-1}}(b_i^j|\tilde{B}_i^{1:j-1}) \qquad \text{if } j \in \mathcal{V}_Y^c \end{aligned} \tag{8}$$

6: $\quad$ Construct $\widetilde{Y}_i^{1:N} \triangleq \widetilde{B}_i^{1:N} G_n$ and send the codeword over the channel.
7: **end for**

Remark 3. *The randomizations described in* (8) *could be replaced by deterministic decisions for $j \in \mathcal{H}_Y^c$, where $\mathcal{H}_Y \triangleq \{i \in [\![1,N]\!] : H(B^i|B^{1:i-1}) > \delta_N\}$, i.e., randomized decisions are only needed for $j \in \mathcal{V}_Y^c \backslash \mathcal{H}_Y^c$, as shown in [22].*

Theorem 4. *The coding scheme of Section IV-D, which operates over k blocks of length N, achieves the region $\mathcal{R}_{X,Y}$ over the discrete memoryless channel $(\mathcal{X} \times \mathcal{Y}, q_{Z|XY}, \mathcal{Z})$, where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are prime numbers. The coding scheme is explicit with complexity $\mathcal{O}(kN \log N)$.*

V. Coding Scheme Analysis

We focus on Case 1 and omit Case 2 due to space constraint. We start by proving with the first two lemmas that the target distribution is well approximated in each Block $i \in [\![1,k]\!]$.

Lemma 2. *For Block $i \in [\![1,k]\!]$,*

$$\mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}}) \leq \delta_N^{(1)},$$

where $\delta_N^{(1)} \triangleq 3N\delta_N$.

Proof. We have

$$\begin{aligned}
&\mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}}) \\
&\overset{(a)}{=} \mathbb{E}[\mathbb{D}(q_{X^{1:N}|U^{1:N}V^{1:N}} \| \widetilde{p}_{X_i^{1:N}|U_i^{1:N}V_i^{1:N}})] \\
&\quad + \mathbb{D}(q_{U^{1:N}V^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}}) \\
&\overset{(b)}{=} \mathbb{E}[\mathbb{D}(q_{X^{1:N}} \| \widetilde{p}_{X_i^{1:N}})] + \mathbb{D}(q_{U^{1:N}V^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}}) \\
&\overset{(c)}{=} \mathbb{D}(q_{X^{1:N}} \| \widetilde{p}_{X_i^{1:N}}) + \mathbb{E}[\mathbb{D}(q_{U^{1:N}|V^{1:N}} \| \widetilde{p}_{U_i^{1:N}|V_i^{1:N}})] \\
&\quad + \mathbb{D}(q_{V^{1:N}} \| \widetilde{p}_{V_i^{1:N}}) \\
&= \mathbb{D}(q_{X^{1:N}} \| \widetilde{p}_{X_i^{1:N}}) + \mathbb{D}(q_{U^{1:N}} \| \widetilde{p}_{U_i^{1:N}}) + \mathbb{D}(q_{V^{1:N}} \| \widetilde{p}_{V_i^{1:N}}) \\
&\overset{(d)}{=} \mathbb{D}(q_{C^{1:N}} \| \widetilde{p}_{C_i^{1:N}}) + \mathbb{D}(q_{A^{1:N}} \| \widetilde{p}_{A_i^{1:N}}) + \mathbb{D}(q_{B^{1:N}} \| \widetilde{p}_{B_i^{1:N}}) \\
&\overset{(e)}{=} \sum_{j=1}^{N} \mathbb{E}_{q_{C^{1:j-1}}} \mathbb{D}(q_{C^j|C^{1:j-1}} \| \widetilde{p}_{C_i^j|C_i^{1:j-1}}) \\
&\quad + \sum_{j=1}^{N} \mathbb{E}_{q_{A^{1:j-1}}} \mathbb{D}(q_{A^j|A^{1:j-1}} \| \widetilde{p}_{A_i^j|A_i^{1:j-1}}) \\
&\quad + \sum_{j=1}^{N} \mathbb{E}_{q_{B^{1:j-1}}} \mathbb{D}(q_{B^j|B^{1:j-1}} \| \widetilde{p}_{B_i^j|B_i^{1:j-1}}) \\
&\overset{(f)}{=} \sum_{j \in \mathcal{V}_X} \mathbb{E}_{q_{C^{1:j-1}}} \mathbb{D}(q_{C^j|C^{1:j-1}} \| \widetilde{p}_{C_i^j|C_i^{1:j-1}}) \\
&\quad + \sum_{j \in \mathcal{V}_U} \mathbb{E}_{q_{A^{1:j-1}}} \mathbb{D}(q_{A^j|A^{1:j-1}} \| \widetilde{p}_{A_i^j|A_i^{1:j-1}}) \\
&\quad + \sum_{j \in \mathcal{V}_V} \mathbb{E}_{q_{B^{1:j-1}}} \mathbb{D}(q_{B^j|B^{1:j-1}} \| \widetilde{p}_{B_i^j|B_i^{1:j-1}}) \\
&\overset{(g)}{=} \sum_{j \in \mathcal{V}_X} (\log|\mathcal{X}| - H(C^j|C^{1:j-1})) \\
&\quad + \sum_{j \in \mathcal{V}_U} (\log|\mathcal{Y}| - H(A^j|A^{1:j-1})) \\
&\quad + \sum_{j \in \mathcal{V}_V} (\log|\mathcal{Y}| - H(B^j|B^{1:j-1})) \\
&\overset{(h)}{\leq} |\mathcal{V}_X|\delta_N + |\mathcal{V}_U|\delta_N + |\mathcal{V}_V|\delta_N \\
&\leq 3N\delta_N,
\end{aligned}$$

where (a) holds by the chain rule for divergence [23], and the expectation is over $q_{U^{1:N}V^{1:N}}$, (b) holds because $X^{1:N}$

is independent from $(U^{1:N}, V^{1:N})$, and $\widetilde{X}_i^{1:N}$ is independent from $(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$, in (c) the expectation is over $q_{V^{1:N}}$, (d) holds by invertibility of G_n, (e) holds by the chain rule for divergence, (f) holds by $(5)-(7)$, (g) holds by the uniformity of the symbols in positions $\mathcal{V}_X$, $\mathcal{V}_U$ and $\mathcal{V}_V$, (h) holds by the definition of $\mathcal{V}_X$, $\mathcal{V}_U$ and $\mathcal{V}_V$. □

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

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

Proof. First, we have

$$\begin{aligned}\tilde{p}_{Y_i^{1:N}|U_i^{1:N}V_i^{1:N}X_i^{1:N}} &\overset{(a)}{=} \tilde{p}_{Y_i^{1:N}|U_i^{1:N}V_i^{1:N}} \\ &\overset{(b)}{=} q_{Y^{1:N}|U^{1:N}V^{1:N}} \\ &\overset{(c)}{=} q_{Y^{1:N}|U^{1:N}V^{1:N}X^{1:N}} \end{aligned} \tag{9}$$

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

$$\begin{aligned}&\mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}Z_i^{1:N}}) \\ &\overset{(a)}{=} \mathbb{E}[\mathbb{D}(q_{Z^{1:N}|U^{1:N}V^{1:N}X^{1:N}Y^{1:N}} \| \widetilde{p}_{Z_i^{1:N}|U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}})] \\ &\quad + \mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}}) \\ &\overset{(b)}{=} \mathbb{E}[\mathbb{D}(q_{Z^{1:N}|X^{1:N}Y^{1:N}} \| \widetilde{p}_{Z_i^{1:N}|X_i^{1:N}Y_i^{1:N}})] \\ &\quad + \mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}}) \\ &\overset{(c)}{=} \mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}}) \\ &\overset{(d)}{=} \mathbb{E}[\mathbb{D}(q_{Y^{1:N}|U^{1:N}V^{1:N}X^{1:N}} \| \widetilde{p}_{Y_i^{1:N}|U_i^{1:N}V_i^{1:N}X_i^{1:N}})] \\ &\quad + \mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}}) \\ &\overset{(e)}{=} \mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}}) \\ &\overset{(f)}{\leq} \delta_N^{(1)},\end{aligned}$$

where (a) holds by chain rule for divergence [23] and the expectation is over $q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}}$, (b) holds by the two Markov chains $(U^{1:N}, V^{1:N}) - (X^{1:N}, Y^{1:N}) - Z^{1:N}$ and $(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}) - (\widetilde{X}_i^{1:N}, \widetilde{Y}_i^{1:N}) - \widetilde{Z}_i^{1:N}$, (c) holds because $q_{Z^{1:N}|X^{1:N}Y^{1:N}} = \widetilde{p}_{Z_i^{1:N}|X_i^{1:N}Y_i^{1:N}}$, in (d) the expectation is over $q_{U^{1:N}V^{1:N}X^{1:N}}$, (e) holds by (9), (f) holds by Lemma 2. □

We now show that the channel outputs of two consecutive blocks are asymptotically independent.

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

$$\mathbb{D}\left(\widetilde{p}_{Z_{i-1:i}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1} \| \widetilde{p}_{Z_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1}\widetilde{p}_{Z_i^{1:N}}\right) \leq \delta_N^{(2)},$$

where $\delta_N^{(2)} \triangleq \delta_N^{(1)} + 2N\sqrt{2\ln 2}\sqrt{\delta_N^{(1)}} \times \log\left(|\mathcal{X}||\mathcal{Y}|^3|\mathcal{Z}|/\left[\sqrt{2\ln 2}\sqrt{\delta_N^{(1)}}\right]\right)$.

Proof. Let $i \in [\![1,k]\!]$. We have

$$\begin{aligned}&H(A^{1:N}[\mathcal{V}_{U|Z}]|Z^{1:N}) - H(\widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}]|\widetilde{Z}_i^{1:N}) \\ &= H(A^{1:N}[\mathcal{V}_{U|Z}]Z^{1:N}) - H(\widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}]\widetilde{Z}_i^{1:N}) \\ &\quad + H(\widetilde{Z}_i^{1:N}) - H(Z^{1:N}) \\ &\overset{(a)}{\leq} NL_1\log(|\mathcal{Y}||\mathcal{Z}|/L_1) + NL_2\log(|\mathcal{Z}|/L_2) \\ &\overset{(b)}{\leq} 2NL_3\log(|\mathcal{X}||\mathcal{Y}|^3|\mathcal{Z}|/L_3) \\ &\overset{(c)}{\leq} 2N\sqrt{2\ln 2}\sqrt{\delta_N^{(1)}}\log\left(|\mathcal{X}||\mathcal{Y}|^3|\mathcal{Z}|/\left[\sqrt{2\ln 2}\sqrt{\delta_N^{(1)}}\right]\right) \\ &\triangleq \delta_N^{(ABCZ)},\end{aligned} \tag{10}$$

where (a) holds for N large enough by [11, Lemma 18] with $L_1 \triangleq \sqrt{2\ln 2}\sqrt{\mathbb{D}(q_{A^{1:N}[\mathcal{V}_{U|Z}]Z^{1:N}} \| \widetilde{p}_{A_i^{1:N}[\mathcal{V}_{U|Z}]Z_i^{1:N}})}$, $L_2 \triangleq \sqrt{2\ln 2}\sqrt{\mathbb{D}(q_{Z^{1:N}} \| \widetilde{p}_{Z_i^{1:N}})}$, (b) holds for N large enough because $\max(L_1, L_2) \leq L_3$ by the chain rule for relative Kullback-Leibler divergence and invertibility of G_n with $L_3 \triangleq \sqrt{2\ln 2} \times \sqrt{\mathbb{D}(q_{U^{1:N}V^{1:N}X^{1:N}Y^{1:N}Z^{1:N}} \| \widetilde{p}_{U_i^{1:N}V_i^{1:N}X_i^{1:N}Y_i^{1:N}Z_i^{1:N}})}$, (c) holds for N large enough by Lemma 3.

One can obtain the same upper bound for $H(B^{1:N}[\mathcal{V}_{V|UZX}]|U^{1:N}Z^{1:N}X^{1:N}) - H(\widetilde{B}_i^{1:N}[\mathcal{V}_{V|UZX}]|\widetilde{U}_i^{1:N}\widetilde{Z}_i^{1:N}\widetilde{X}_i^{1:N})$ and $H(C^{1:N}[\mathcal{V}_{X|UZ}]|U^{1:N}Z^{1:N}) - H(\widetilde{C}_i^{1:N}[\mathcal{V}_{X|UZ}]|\widetilde{U}_i^{1:N}\widetilde{Z}_i^{1:N})$. Then, for $i \in [\![2,k]\!]$,

$$\begin{aligned}&\mathbb{D}\left(\widetilde{p}_{Z_{i-1:i}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1} \| \widetilde{p}_{Z_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1}\widetilde{p}_{Z_i^{1:N}}\right) \\ &= I(\widetilde{Z}_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1; \widetilde{Z}_i^{1:N}) \\ &= I(\widetilde{Z}_i^{1:N}; \bar{D}_1\bar{E}_1\bar{F}_1) + I(\widetilde{Z}_{i-1}^{1:N}; \widetilde{Z}_i^{1:N}|\bar{D}_1\bar{E}_1\bar{F}_1) \\ &\overset{(d)}{=} I(\widetilde{Z}_i^{1:N}; \bar{D}_1\bar{E}_1\bar{F}_1) \\ &= I(\bar{D}_1; \widetilde{Z}_i^{1:N}) + I(\bar{E}_1; \widetilde{Z}_i^{1:N}|\bar{D}_1) + I(\bar{F}_1; \widetilde{Z}_i^{1:N}|\bar{E}_1\bar{D}_1) \\ &\leq I(\bar{D}_1; \widetilde{Z}_i^{1:N}) + I(\bar{E}_1; \bar{D}_1\widetilde{Z}_i^{1:N}) + I(\bar{F}_1; \bar{D}_1\bar{E}_1\widetilde{Z}_i^{1:N}) \\ &\leq I(\bar{D}_1; \widetilde{Z}_i^{1:N}) + I(\bar{E}_1; \widetilde{U}_i^{1,N}\widetilde{Z}_i^{1:N}) + I(\bar{F}_1; \widetilde{U}_i^{1,N}\widetilde{X}_i^{1,N}\widetilde{Z}_i^{1:N}) \\ &\overset{(e)}{=} I(\widetilde{Z}_i^{1:N}; \widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}]) + I(\widetilde{U}_i^{1:N}\widetilde{Z}_i^{1:N}; \widetilde{C}_i^{1:N}[V_{X|UZ}]) \\ &\quad + I(\widetilde{U}_i^{1:N}\widetilde{X}_i^{1:N}\widetilde{Z}_i^{1:N}; \widetilde{B}_i^{1:N}[\mathcal{V}_{V|UZX}]) \\ &\overset{(f)}{=} |\mathcal{V}_{U|Z}|\log|\mathcal{Y}| - H(\widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}]|\widetilde{Z}_i^{1:N}) + |\mathcal{V}_{X|UZ}||\log\mathcal{X}| \\ &\quad - H(\widetilde{C}_i^{1:N}[\mathcal{V}_{X|UZ}]|\widetilde{U}_i^{1:N}\widetilde{Z}_i^{1:N}) + |\mathcal{V}_{V|UZX}|\log|\mathcal{Y}| \\ &\quad - H(\widetilde{B}_i^{1:N}[\mathcal{V}_{V|UZX}]|\widetilde{U}_i^{1:N}\widetilde{Z}_i^{1:N}\widetilde{X}_i^{1:N}) \\ &\overset{(g)}{\leq} |\mathcal{V}_{U|Z}|\log|\mathcal{Y}| - H(A^{1:N}[\mathcal{V}_{U|Z}]|Z^{1:N}) + |\mathcal{V}_{X|UZ}|\log|\mathcal{X}| \\ &\quad - H(C^{1:N}[\mathcal{V}_{X|UZ}]|U^{1:N}Z^{1:N}) + |\mathcal{V}_{V|UZX}|\log|\mathcal{Y}| \\ &\quad - H(B^{1:N}[\mathcal{V}_{V|UZX}]|U^{1:N}Z^{1:N}X^{1:N}) + \delta_N^{(ABCZ)} \\ &\overset{(h)}{\leq} |\mathcal{V}_{U|Z}|\log|\mathcal{Y}| - \sum_{j\in\mathcal{V}_{U|Z}} H(A^j|A^{1:j-1}Z^{1:N}) \\ &\quad + |\mathcal{V}_{X|UZ}|\log|\mathcal{X}| - \sum_{j\in\mathcal{V}_{X|UZ}} H(C^j|C^{1:j-1}U^{1:N}Z^{1:N}) \\ &\quad + |\mathcal{V}_{V|UZX}|\log|\mathcal{Y}| - \sum_{j\in\mathcal{V}_{V|UZX}} H(B^j|B^{1:j-1}U^{1:N}Z^{1:N}X^{1:N})\end{aligned}$$

$$
\begin{aligned}
&+\delta_N^{(ABCZ)}\\
&\overset{(i)}{\leq} |\mathcal{V}_{U|Z}|\log|\mathcal{Y}| - |\mathcal{V}_{U|Z}|(\log|\mathcal{Y}|-\delta_N) + |\mathcal{V}_{X|UZ}|\log|\mathcal{X}|\\
&\quad - |\mathcal{V}_{X|UZ}|(\log|\mathcal{X}|-\delta_N) + |\mathcal{V}_{V|UZX}|\log|\mathcal{Y}|\\
&\quad - |\mathcal{V}_{V|UZX}|(\log|\mathcal{Y}|-\delta_N) + \delta_N^{(ABCZ)}\\
&\leq 3N\delta_N + \delta_N^{(ABCZ)}\\
&= \delta_N^{(1)} + \delta_N^{(ABCZ)},
\end{aligned}
$$

where (d) holds by the Markov chain $\widetilde{Z}_{i-1} - (\bar{D}_1, \bar{E}_1, \bar{F}_1) - \widetilde{Z}_i^{1:N}$, (e) holds by Algorithms 1 and 2, (f) holds by the uniformity of $\widetilde{A}_i^{1:N}[\mathcal{V}_{U|Z}], \widetilde{C}_i^{1:N}[\mathcal{V}_{X|UZ}]$ and $\widetilde{B}_i^{1:N}[\mathcal{V}_{V|UZX}]$, (g) holds by (10), (h) holds because conditioning reduces entropy, (i) holds by the definition of $\mathcal{V}_{U|Z}, \mathcal{V}_{X|UZ}$, and $\mathcal{V}_{V|UZX}$. □

We next show that the outputs of all the blocks are asymptotically independent.

Lemma 5. *We have*

$$
\mathbb{D}\left(\widetilde{p}_{Z_{1:k}^{1:N}} \middle\| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right) \leq (k-1)\delta_N^{(2)}.
$$

Proof. We have

$$
\begin{aligned}
&\mathbb{D}\left(\widetilde{p}_{Z_{1:k}^{1:N}} \| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right)\\
&\overset{(a)}{=} \sum_{i=2}^{k} I(\widetilde{Z}_i^{1:N}; \widetilde{Z}_{1:i-1}^{1:N})\\
&\leq \sum_{i=2}^{k} I(\widetilde{Z}_i^{1:N}; \widetilde{Z}_{1:i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1)\\
&= \sum_{i=2}^{k} I(\widetilde{Z}_i^{1:N}; \widetilde{Z}_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1)\\
&\quad + \sum_{i=2}^{k} I(\widetilde{Z}_i^{1:N}; \widetilde{Z}_{1:i-2}^{1:N}|\bar{D}_1\bar{E}_1\bar{F}_1\widetilde{Z}_{i-1}^{1:N})\\
&\overset{(b)}{=} \sum_{i=2}^{k} I(\widetilde{Z}_i^{1:N}; \widetilde{Z}_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1)\\
&= \sum_{i=2}^{k} \mathbb{D}\left(\widetilde{p}_{Z_{i-1:i}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1} \| \widetilde{p}_{Z_{i-1}^{1:N}\bar{D}_1\bar{E}_1\bar{F}_1}\widetilde{p}_{Z_i^{1:N}}\right)\\
&\overset{(c)}{\leq} (k-1)\delta_N^{(2)},
\end{aligned}
$$

where (a) holds by [11, Lemma 16], (b) holds as for any $i \in [\![3,k]\!]$, the Markov chain $\widetilde{Z}_{1:i-2}^{1:N} - \bar{D}_1\bar{E}_1\bar{F}_1\widetilde{Z}_{i-1}^{1:N} - \widetilde{Z}_i^{1:N}$ holds, (c) holds by Lemma 4. □

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

Lemma 6. *We have*

$$
\mathbb{D}\left(\widetilde{p}_{Z_{1:k}^{1:N}} \| q_{Z^{1:kN}}\right) \leq \delta_N^{(3)},
$$

where

$$
\begin{aligned}
\delta_N^{(3)} &\triangleq k^{\frac{3}{2}} N \log\left(\frac{1}{\mu_{q_Z}}\right)\sqrt{2\ln 2}\left[\sqrt{\delta_N^{(1)}} + \sqrt{\delta_N^{(2)}}\right],\\
\mu_{q_Z} &\triangleq \min_{z\in\mathcal{Z}} q(z).
\end{aligned}
$$

Proof. First, we observe that

$$
\begin{aligned}
\mathbb{D}\left(q_{Z^{1:kN}} \| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right) &= \mathbb{D}\left(\prod_{i=1}^{k} q_{Z^{1:N}} \middle\| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right)\\
&= \sum_{i=1}^{k} \mathbb{D}\left(q_{Z^{1:N}} \middle\| \widetilde{p}_{Z_i^{1:N}}\right)\\
&\leq k\delta_N^{(1)}, \qquad (11)
\end{aligned}
$$

where the inequality holds by Lemma 3. Then, we have, for N large enough,

$$
\begin{aligned}
&\mathbb{D}\left(\widetilde{p}_{Z_{1:k}^{1:N}} \| q_{Z^{1:kN}}\right)\\
&\overset{(a)}{\leq} \log\left(\frac{1}{\mu_{qZ}^{kN}}\right)\sqrt{2\ln 2}\left[\sqrt{\mathbb{D}\left(\widetilde{p}_{Z_{1:k}^{1:N}} \middle\| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right)}\right.\\
&\qquad \left. + \sqrt{\mathbb{D}\left(q_{Z^{1:kN}} \| \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right)}\right]\\
&\overset{(b)}{\leq} kN \log\left(\frac{1}{\mu_{qZ}}\right)\sqrt{2\ln 2}\left[\sqrt{k\delta_N^{(1)}} + \sqrt{(k-1)\delta_N^{(2)}}\right],
\end{aligned}
$$

where (a) holds by [11, Lemma 17] and because $\mu_{q_{Z^{1:kN}}} = \mu_{qZ}^{kN}$, (b) holds by Lemma 5 and (11). □

Our encoding scheme exploits randomness to draw symbols according to (5)-(7), whose rate is for any $i \in [\![1,k]\!]$,

$$
\begin{aligned}
\lim_{N\to+\infty} \frac{1}{N}\left(\sum_{j\in\mathcal{V}_U^c} H(\widetilde{A}_i^j|\widetilde{A}_i^{1:j-1}) + \sum_{j\in\mathcal{V}_V^c} H(\widetilde{B}_i^j|\widetilde{B}_i^{1:j-1})\right.\\
\left. + \sum_{j\in\mathcal{V}_X^c} H(\widetilde{C}_i^j|\widetilde{C}_i^{1:j-1})\right).
\end{aligned}
$$

We quantify this rate in the following lemma, whose proof is similar to [11, Lemma 20] and is thus omitted.

Lemma 7. *We have for any* $i \in [\![1,k]\!]$

$$
\begin{aligned}
\lim_{N\to+\infty} \frac{1}{N}\left(\sum_{j\in\mathcal{V}_U^c} H(\widetilde{A}_i^j|\widetilde{A}_i^{1:j-1}) + \sum_{j\in\mathcal{V}_V^c} H(\widetilde{B}_i^j|\widetilde{B}_i^{1:j-1})\right.\\
\left. + \sum_{j\in\mathcal{V}_X^c} H(\widetilde{C}_i^j|\widetilde{C}_i^{1:j-1})\right) = 0.
\end{aligned}
$$

Finally, we determine the rate pair achieved by our coding scheme.

Lemma 8. *The rate pair* $(R_1, R_U + R_V)$ *is achievable and*

$$
\lim_{N\to+\infty} R_1 = I(X;Z|U) + \frac{H(X|UZ)}{k},
$$

$$\lim_{N\to+\infty} R_U = I(U;Z) + \frac{H(U|Z)}{k},$$
$$\lim_{N\to+\infty} R_V = I(V;Z|UX) + \frac{H(V;Z|UX)}{k}.$$

Proof. By Lemma 7, the overall rate of uniform symbols required are the following:

$$\begin{aligned}
R_1 &= \frac{|\bar{E}_1|+|E_{1:k}|}{kN} \\
&= \frac{|\mathcal{V}_{X|UZ}|+k|\mathcal{V}_X\backslash\mathcal{V}_{X|UZ}|}{kN} \\
&= \frac{|\mathcal{V}_{X|UZ}|}{kN} + \frac{|\mathcal{V}_X|-|\mathcal{V}_{X|UZ}|}{N} \\
&\xrightarrow{N\to+\infty} I(X;Z|U) + \frac{H(X|UZ)}{k} \\
&\xrightarrow{k\to+\infty} I(X;Z|U), \\
R_U &= \frac{|\bar{D}_1|+|D_{1:k}|}{kN} \\
&= \frac{|\mathcal{V}_{U|Z}|+k|\mathcal{V}_U\backslash\mathcal{V}_{U|Z}|}{kN} \\
&= \frac{|\mathcal{V}_{U|Z}|}{kN} + \frac{|\mathcal{V}_U|-|\mathcal{V}_{U|Z}|}{N} \\
&\xrightarrow{N\to+\infty} I(U;Z) + \frac{H(U|Z)}{k} \\
&\xrightarrow{k\to+\infty} I(U;Z), \\
R_V &= \frac{|\bar{F}_1|+|F_{1:k}|}{kN} \\
&= \frac{|\mathcal{V}_{V|UZX}|+k|\mathcal{V}_V\backslash\mathcal{V}_{V|UZX}|}{kN} \\
&= \frac{|\mathcal{V}_{V|UZX}|}{kN} + \frac{|\mathcal{V}_V|-|\mathcal{V}_{V|UZX}|}{N} \\
&\xrightarrow{N\to+\infty} I(V;Z|UX) + \frac{H(V|UZX)}{k} \\
&\xrightarrow{k\to+\infty} I(V;Z|UX),
\end{aligned}$$

where we have used [21, Lemma 7] in the limits. Finally, we conclude that the rates $R_1 = I(X;Z|U)$, $R_U = I(U;Z)$, $R_V = I(V;Z|UX)$ are achieved with Lemma 6. □

VI. Concluding Remarks

We proposed an explicit and low-complexity coding scheme that achieves the multiple access channel resolvability region of an arbitrary discrete memoryless multiple access channel whose input alphabets have prime cardinalities. Our results improve earlier constructions that were limited to symmetric multiple access channels. The main idea of the coding scheme is to reduce the problem of multiple access channel resolvability in a combination of source resolvability problems. Our construction involves block-Markov coding that takes advantage of randomness recycling in different encoding blocks, and uses polar codes for source coding to implement source resolvability. Rate splitting is also employed to avoid, as much as possible, time-sharing.

We remark that the way source resolvability and randomness recycling is implemented in our coding scheme, heavily relies on the intrinsic structure of polar codes. Consequently, it remains open to determine whether polar codes can be substituted by other source resolvability codes in our coding scheme. Providing a positive answer to this question would make our construction more general.

References

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

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

[3] M. Bloch and J. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, 2013.

[4] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, 2006.

[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] Z. Goldfeld, P. Cuff, and H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, 2016.

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

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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] ——, "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*, 2015, pp. 1380–1385.

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