Explicit Construction of Multiple Access Channel Resolvability Codes from Source Resolvability Codes

Rumia Sultana and Rémi A. Chou
Department of Electrical Engineering and Computer Science
Wichita State University, Wichita, KS 67260
Emails: {rxsultana@shockers.wichita, remi.chou@wichita}.edu

***Abstract*—We show that the problem of code construction for multiple access channel resolvability can be reduced to the simpler problem of code construction for source resolvability. Specifically, we propose a multiple access channel resolvability coding scheme that involves randomness recycling, implemented via distributed hashing, and block-Markov encoding, where each encoding block is obtained as a combination of several source resolvability codes. Our construction is independent of the way the source resolvability codes are implemented and yields explicit coding schemes that achieve the multiple access channel resolvability region for an arbitrary discrete memoryless multiple access channel whose input alphabets are binary.**

I. Introduction

Applications of the concept of channel resolvability [1], [2] 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 explicit constructions of such codes have been proposed in the literature. 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. Moreover, in [15], an explicit construction based on polar codes is shown to achieve the multiple access channel resolvability region for arbitrary channels whose input alphabets have prime cardinalities.

In this paper, we show that the problem of code construction for multiple access channel resolvability can be reduced to the simpler problem of code construction for source resolvability [16]. Specifically, our construction allows to construct codes that achieve the multiple access channel resolvability region for arbitrary channels with binary input alphabets [8] from source resolvability codes used in a black box manner. Note that explicit constructions of source resolvability codes have, for instance, been provided in [11]. The main idea of our construction is randomness recycling, implemented with distributed hashing, across a block-Markov encoding scheme that involves a combination of several source resolvability codes. 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. Note also that our proposed construction is independent of the way source resolvability is implemented and is thus more general than our previous construction in [15], which heavily relies on the structure of polar codes.

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

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 between p and q is defined as $\mathbb{V}(p_X, q_X) \triangleq \sum_{x\in\mathcal{X}} |p(x) - q(x)|$. For $a, b \in \mathbb{R}$, define $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$.

III. 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 $\mathcal{S}_1 \triangleq [\![1, 2^{NR_1}]\!]$ and $\mathcal{S}_2 \triangleq [\![1, 2^{NR_2}]\!]$, respectively;*
- *Two encoding functions $f_{1,N} : \mathcal{S}_1 \to \mathcal{X}^N$ and $f_{2,N} : \mathcal{S}_2 \to \mathcal{Y}^N$;*

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

Definition 2. *(R_1, R_2) is an achievable resolvability rate pair for the memoryless multiple access channel $(\mathcal{X}\times\mathcal{Y}, q_{Z|XY}, \mathcal{Z})$ if there exists a sequence of $(2^{NR_1}, 2^{NR_2}, N)$ codes such that $\lim_{N\to+\infty} \mathbb{V}(\widetilde{p}_{Z^{1:N}}, q_{Z^{1:N}}) = 0$, where $q_{Z^{1:N}} \triangleq \prod_{i=1}^N q_Z$ with q_Z defined in (1) and $\forall z^{1:N} \in \mathcal{Z}^N$,*

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

The multiple access channel resolvability region $\mathcal{R}_{q_Z}$ is defined as the closure of the set of all achievable rate pairs and has been characterized in [8].

Our objective is to show that the construction of multiple access channel resolvability codes that achieve $\mathcal{R}_{q_Z}$ reduces to the simpler problem of constructing source resolvability codes.

IV. Proposed coding Scheme to achieve $\mathcal{R}_{q_Z}$

We first review in Section IV-A the notion of source resolvability codes which are used in a black box manner in our construction of MAC resolvability codes. We explain in Section IV-B that the general construction of MAC resolvability codes can be reduced to two special cases. Finally, we provide a coding scheme for these two special cases in Sections IV-C, IV-D.

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 $e_N : \mathcal{S} \to \mathcal{X}^N$;*

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

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

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

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

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

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

To achieve the multiple access channel resolvability region $\mathcal{R}_{q_Z}$, it is sufficient to achieve

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

by [15]. We consider two cases to achieve $\mathcal{R}_{X,Y}$ for some fixed distribution $p_X p_Y$.

Case 1: $I(XY;Z) > I(X;Z) + I(Y;Z)$. In this case, it is sufficient [15] to achieve the set of rate pairs

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

with rate-splitting using the following lemma.

Lemma 1 ([15]). *As in [18, 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

$$\begin{aligned}&R_1 : \epsilon \mapsto I(X;Z|U), \text{ from } [0,1] \text{ to } \mathbb{R}^+,\\ &R_U : \epsilon \mapsto I(U;Z), \text{ from } [0,1] \text{ to } \mathbb{R}^+,\\ &R_V : \epsilon \mapsto I(V;Z|UX), \text{ from } [0,1] \text{ to } \mathbb{R}^+.\end{aligned}$$

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

Case 2: $I(XY;Z) = I(X;Z) + I(Y;Z)$. In this case, it is sufficient [15] to achieve the rate pair $(I(X;Z), I(Y;Z))$.

C. Encoding Scheme for Case 1

Fix a point (R_1, R_2) in $\mathcal{D}$. By Lemma 1, there exists a joint probability distribution q_{UVXYZ} over $\mathcal{U}\times\mathcal{V}\times\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$ 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 below a coding scheme that will be shown to achieve the point (R_1, R_2).

- The encoding at Transmitter 1 is described in Algorithm 1 and uses
  - A hash function $G_X : \{0,1\}^N \longrightarrow \{0,1\}^{r_X}$ chosen uniformly at random in a family of 2-universal hash functions [19], where r_X will be defined later.
  - A source resolvability code for the discrete memoryless source $(\mathcal{X}, q_X)$ with encoder function e_N^X and rate $H(X) + \frac{\epsilon_1}{2}$, where $\epsilon_1 \triangleq 2(\delta_{\mathcal{A}}(N) + \xi)$,

$\delta_{\mathcal{A}}(N) \triangleq \log(|\mathcal{U}||\mathcal{V}||\mathcal{X}|+3)\sqrt{\frac{2}{N}(3+\log N)}$, $\xi > 0$, such that the distribution of the encoder output $\widetilde{p}_{X^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{X^{1:N}}, q_{X^{1:N}}) \leq \delta(N)$ where $\delta(N)$ is such that $\lim_{N\to+\infty} \delta(N) = 0$.

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

- The encoding at Transmitter 2 is described in Algorithm 2 and uses
  - Two hash functions $G_U : \{0,1\}^N \longrightarrow \{0,1\}^{r_U}$, $G_V : \{0,1\}^N \longrightarrow \{0,1\}^{r_V}$ chosen uniformly at random in families of 2-universal hash functions, where r_U and r_V will be defined later.
  - A source resolvability code for the discrete memoryless source $(\mathcal{U}, q_U)$ with encoding function e_N^U and rate $H(U) + \frac{\epsilon_1}{2}$, such that the distribution of the encoder output $\widetilde{p}_{U^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{U^{1:N}}, q_{U^{1:N}}) \leq \delta(N)$.
  - A source resolvability code for the discrete memoryless source $(\mathcal{V}, q_V)$ with encoding function e_N^V and rate $H(V) + \frac{\epsilon_1}{2}$, such that the distribution of the encoder output $\widetilde{p}_{V^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{V^{1:N}}, q_{V^{1:N}}) \leq \delta(N)$.

  In Algorithm 2, the hash function outputs $\widetilde{D}_i$ and $\widetilde{F}_i$, $i \in [\![2,k]\!]$, with length 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 1.

Algorithm 1 Encoding algorithm for resolvability of Transmitter 1 in Case 1

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

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

D. Encoding Scheme for Case 2

Consider a joint probability distribution $q_{XYZ} \triangleq q_{Z|XY} p_X p_Y$ such that $I(XY;Z) = I(X;Z) + I(Y;Z)$. We provide an encoding scheme that will be shown to achieve the point $(R_1, R_2) = (I(X;Z), I(Y;Z))$.

- The encoding at Transmitter 1 is the same as in Algorithm 1 except that E_1 is now a vector of of $N(H(X) + \epsilon_2)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, E_i is a vector of $N(I(X;Z) + \epsilon_2)$ uniformly distributed bits, where $\epsilon_2 \triangleq 2(\delta_{\mathcal{A}}^{(2)}(N) + \xi)$ with $\delta_{\mathcal{A}}^{(2)}(N) \triangleq \log(|\mathcal{X}||\mathcal{Y}|+3)\sqrt{\frac{2}{N}(2+\log N)}$, $\xi > 0$.

Algorithm 2 Encoding algorithm for resolvability of Transmitter 2 in Case 1

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

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

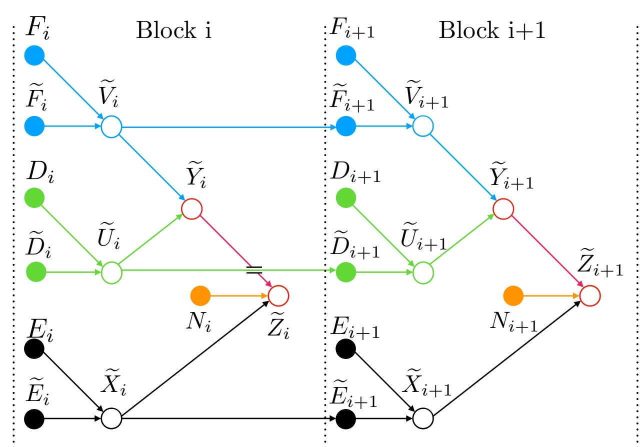

Fig. 1. Dependence graph for the random variables involved in the encoding for Case 1. N_i, $i \in [\![1,k]\!]$, is the channel noise corresponding to the transmission over Block i. For Block $i \in [\![2,k]\!]$, $(D_i, \widetilde{D}_i)$, $(F_i, \widetilde{F}_i)$, $(E_i, \widetilde{E}_i)$ are the random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

- The encoding at Transmitter 2 is described in Algorithm 3 and uses
  - A hash function $G_Y : \{0,1\}^N \longrightarrow \{0,1\}^{r_Y}$ chosen uniformly at random in a family of two-universal hash functions, where r_Y will be defined later.
  - A source resolvability code for the discrete memoryless source $(\mathcal{Y}, q_Y)$ with encoding function e_N^Y and rate $H(Y) + \frac{\epsilon_2}{2}$, such that the distribution of the encoder output $\widetilde{p}_{Y^{1:N}}$ satisfies $\mathbb{V}(\widetilde{p}_{Y^{1:N}}, q_{Y^{1:N}}) \leq \delta(N)$.

The dependencies between the random variables involved in

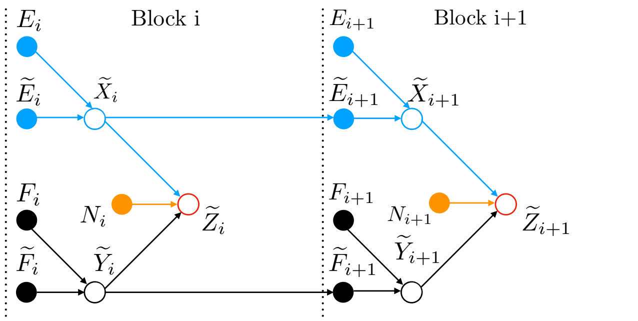

Fig. 2. Dependence graph for the random variables involved in the encoding for Case 2. N_i, $i \in [\![1,k]\!]$, is the channel noise corresponding to the transmission over Block i. For Block $i \in [\![2,k]\!]$, $(E_i, \widetilde{E}_i)$, $(F_i, \widetilde{F}_i)$ are the random sequences used at the encoder to form $\widetilde{X}_i$, $\widetilde{Y}_i$, respectively.

the encoding for Case 2 are represented in Figure 2.

Algorithm 3 Encoding algorithm for resolvability of Transmitter 2 in Case 2

Require: A vector F_1 of $N(H(Y)+\epsilon_2)$ uniformly distributed bits, and for $i \in [\![2,k]\!]$, a vector F_i of $N(I(Y;Z)+\epsilon_2)$ uniformly distributed bits.

```
for Block i = 1 to k do
    if i = 1 then
        Define Ỹ_1^{1:N} ≜ e_N^Y(F_1)
    else if i > 1 then
        Define F̃_i ≜ G_Y(Ỹ_{i-1}^{1:N})
        Define Ỹ_i^{1:N} ≜ e_N^Y(F̃_i || F_i)
    end if
    Send Ỹ_i^{1:N} over the channel
end for
```

V. Coding Scheme Analysis

We only focus on Case 1 and omit Case 2 due to space constraints.

For convenience define $\widetilde{E}_1 \triangleq \emptyset$, $\widetilde{D}_1 \triangleq \emptyset$, and $\widetilde{F}_1 \triangleq \emptyset$. Let $\widetilde{p}_{E_i D_i F_i X_i^{1:N} U_i^{1:N} V_i^{1:N} Y_i^{1:N} Z_i^{1:N}}$ denote the joint probability distribution of the random variables $\widetilde{E}_i, \widetilde{D}_i, \widetilde{F}_i, \widetilde{X}_i^{1:N}, \widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, \widetilde{Y}_i^{1:N}$, and $\widetilde{Z}_i^{1:N}$ created in Block $i \in [\![1,k]\!]$ of the coding scheme of Section IV. We also define the output lengths of the hash functions G_X, G_U, G_V as follows

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

To prove that randomness recycling is done as expected, we need the following two supporting lemmas.

Lemma 2 ([20]). *Define $\mathcal{A} \triangleq [\![1,A]\!]$. Let $(\mathcal{T}_a)_{a\in\mathcal{A}}$ be A finite alphabets and define for $\mathcal{S} \subseteq \mathcal{A}$, $\mathcal{T}_{\mathcal{S}} \triangleq \bigtimes_{a\in\mathcal{S}} \mathcal{T}_a$. Consider the random variables $T_{\mathcal{A}}^{1:N} \triangleq (T_a^{1:N})_{a\in\mathcal{A}}$ and $Z^{1:N}$ defined over $\mathcal{T}_{\mathcal{A}}^N \times \mathcal{Z}^N$ with probability distribution $q_{T_{\mathcal{A}}^{1:N} Z^{1:N}} \triangleq \prod_{i=1}^N q_{T_{\mathcal{A}} Z}$. For any $\epsilon > 0$, there exists a subnormalized non-negative function $w_{T_{\mathcal{A}}^{1:N} Z^{1:N}}$ defined over $\mathcal{T}_{\mathcal{A}}^N \times \mathcal{Z}^N$ such that $\mathbb{V}(q_{T_{\mathcal{A}}^{1:N} Z^{1:N}}, w_{T_{\mathcal{A}}^{1:N} Z^{1:N}}) \leq \epsilon$ and*

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

where $\delta_{\mathcal{S}}(N) \triangleq (\log(|\mathcal{T}_{\mathcal{S}}|+3))\sqrt{\frac{2}{N}(A + \log(\frac{1}{\epsilon}))}$, and we have defined the conditional min-entropy as [21],

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

Lemma 3 (Adapted from [22, Lemma 5]). *Let $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$ and Z be random variables distributed according to $p_{X_{\mathcal{L}} Z}$ over $\mathcal{X}_{\mathcal{L}} \times \mathcal{Z}$. For $l \in \mathcal{L}$, let $F_l : \{0,1\}^{n_l} \longrightarrow \{0,1\}^{r_l}$, be uniformly chosen in a family $\mathcal{F}_l$ of two-universal hash functions. Define $s_{\mathcal{L}} \triangleq \prod_{l\in\mathcal{L}} s_l$, where $s_l \triangleq |\mathcal{F}_l|$, $l \in \mathcal{L}$, and for any $\mathcal{S} \subseteq \mathcal{L}$, define $r_{\mathcal{S}} \triangleq \sum_{i\in\mathcal{S}} r_i$. Define also $\mathcal{F}_{\mathcal{L}} \triangleq (F_l)_{l\in\mathcal{L}}$ and*

$$
F_{\mathcal{L}}(X_{\mathcal{L}}) \triangleq (F_1(X_1) || F_2(X_2) || \ldots || F_L(X_L)),
$$

where $||$ denotes concatenation. Then, for any q_Z defined over $\mathcal{Z}$ such that $supp(q_Z) \subseteq supp(p_Z)$, we have

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

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

Using Lemmas 2 and 3, one can prove the following result, which shows that in Block $i \in [\![2,k]\!]$, if the inputs $\widetilde{X}_{i-1}^{1:N}$, $\widetilde{U}_{i-1}^{1:N}$, $\widetilde{V}_{i-1}^{1:N}$ of the hash functions G_X, G_U, G_V, respectively, are replaced by $X^{1:N}$, $U^{1:N}$, $V^{1:N}$ distributed according to $q_{X^{1:N} U^{1:N} V^{1:N}} \triangleq \prod_{i=1}^N q_{XUV}$, then the output of these hash functions are almost jointly uniformly distributed.

Lemma 4. *Let $p_{\bar{E}}^{unif}, p_{\bar{D}}^{unif}, p_{\bar{F}}^{unif}$ denote the uniform distributions over $\{0,1\}^{r_X}$, $\{0,1\}^{r_U}$, $\{0,1\}^{r_V}$, respectively. We have*

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

where $\delta_T(N)$ is such that $\lim_{N\to\infty} \delta_T(N) = 0$.

Using Lemma 4, one can prove the following lemma, which shows that in each encoding block, the random variables induced by the coding scheme approximate well the target distribution.

Lemma 5. *For Block $i \in [\![1,k]\!]$,*

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

where $\delta_i(N)$ is such that $\lim_{N\to+\infty} \delta_i(N) = 0$.

Using Lemmas 4 and 5, one can prove, as stated in the next lemma, that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent of the channel output in Block $i-1$.

Lemma 6. *For $i \in [\![2, k]\!]$,*

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

where $\delta_i^{(1)}(N)$ is such that $\lim_{N\to+\infty} \delta_i^{(1)}(N) = 0$.

Using Lemma 6, one can prove the next lemma, which shows that the recycled randomness in Block $i \in [\![2, k]\!]$ is almost independent of the channel outputs in Blocks 1 to $i-1$ considered jointly.

Lemma 7. *For $i \in [\![2, k]\!]$, we have*

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

where $\delta_i^{(C)}(N)$ such that $\lim_{N\to\infty} \delta_i^{(C)}(N) = 0$.

Using Lemma 7, one can prove the next lemma, which shows that the channel outputs of all the blocks are asymptotically independent.

Lemma 8. *We have*

$$\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, \prod_{i=1}^{k} \widetilde{p}_{Z_i^{1:N}}\right) \leq (k-1) \max_{j\in[\![2,k]\!]} \delta_j^{(C)}(N),$$

where $(\delta_j^{(C)}(N))_{j\in[\![2,k]\!]}$ is defined in Lemma 7.

Using Lemmas 5 and 8, one can show, as stated in the following lemma, that the target output distribution is well approximated jointly over all blocks.

Lemma 9. *For block $i \in [\![1, k]\!]$, we have*

$$\mathbb{V}\left(\widetilde{p}_{Z_{1:k}^{1:N}}, q_{Z^{1:kN}}\right) \leq k\left(\max_{j\in[\![2,k]\!]} \delta_j^{(C)}(N) + \max_{j\in[\![1,k]\!]} \delta_j(N)\right),$$

where $(\delta_j^{(C)}(N))_{j\in[\![2,k]\!]}$ is defined in Lemma 7 and $(\delta_j(N))_{j\in[\![1,k]\!]}$ is defined in Lemma 5.

Finally, one can show that the encoding scheme of Section IV-C achieves the desired rate pair.

Lemma 10. *Let $\epsilon_0 > 0$. For k large enough, the rate pair $(R_1, R_U + R_V)$ is achievable and*

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

VI. Concluding Remarks

We showed that the problem of code construction for multiple access channel resolvability can be reduced to the simpler problem of code construction for source resolvability. Our approach allows to construct codes that achieve the multiple access channel resolvability region for arbitrary channels with binary input alphabets from source resolvability codes. The crux of our construction is randomness recycling implemented with distributed hashing across a block-Markov encoding scheme.

Acknowledgment

This work was supported in part by NSF grant CCF-1850227.

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] 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.

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

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

[18] 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.

[19] 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.

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

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

[22] R. Chou and A. Yener, "Secret-key generation in many-to-one networks: An integrated game-theoretic and information-theoretic approach," *IEEE Trans. Inf. Theory*, vol. 8, pp. 5144–5159, 2019.