Low-Complexity Channel Resolvability Codes for the Symmetric Multiple-Access Channel

Rémi A. Chou and Matthieu R. Bloch
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
Email: {remi.chou,matthieu}@gatech.edu

Jörg Kliewer
Department of Electrical and Computer Engineering
New Jersey Institute of Technology
Newark, New Jersey 07102–1982
Email: jkliewer@njit.edu

***Abstract*—We investigate channel resolvability for the l-user multiple-access channel (MAC) with two different families of encoders. The first family consists of invertible extractors, while the second one consists of injective group homomorphisms, and was introduced by Hayashi for the point-to-point channel resolvability. The main benefit of these two families is to provide explicit low-complexity channel resolvability codes in the case of symmetric MACs. Specifically, we provide two examples of families of invertible extractors suitable for MAC resolvability with uniform input distributions, one based on finite-field multiplication, which can be implemented in $O(n \log n)$ for a limited range of values of the encoding blocklength n, and a second based on modified Toeplitz matrices, which can be implemented in $O(n \log n)$ for a wider range of values of n. We also provide an example of family of injective group homomorphisms based on finite-field multiplication suitable for MAC resolvability with uniform input distributions, which can be implemented in $O(n \log n)$ for some values of n.**

I. Introduction

While most information-theoretic studies focus on the analysis of coding mechanisms ensuring *reliability*, recent investigations of information-theoretic problems involving strong secrecy [1], [2], [3] and coordination [4] have highlighted the usefulness of coding mechanisms ensuring *channel resolvability* [5]. The design of explicit codes for channel resolvability is, however, still largely unexplored; to the best of our knowledge, the only known low-complexity codes achieving the fundamental limits of channel resolvability are polar codes in the case of symmetric channels [6]. This property of polar codes turns out to be a key ingredient to perform strong coordination for a class of symmetric sources [6] and to achieve strong secrecy over symmetric wiretap channels [7], which motivates the investigation of alternative coding schemes for channel resolvability with a different complexity-performance tradeoff. In particular, polar codes may be unsuitable in situations with stringent delay constraints, since they require relatively large block lengths to be effective. Furthermore, the study of resolvability for the MAC is of interest as it enables the design of codes for coded cooperative jamming with strong secrecy [8], which will be the subject of future investigations.

In this paper, we provide two different constructions for MAC resolvability [9]. In Section III, we present a first construction based on invertible extractors, which highlights the connection between [10] and [11], since channel resolvability coupled with channel coding leads to strong secrecy over the wiretap channel. In Section IV, we present our second construction, which is an extension of resolvability for the point-to-point channel performed with injective group homomorphisms [12]. In Section V, we then show how MAC symmetry allows one to further simplify the analysis. We conclude the paper in Section VI by presenting two explicit low-complexity MAC resolvability codes. In Section VI-A, we propose codes based on families of extractors initially used in [11] and [10] for wiretap codes. In Section VI-B, we finally develop codes based on a family of injective group homomorphisms.

The research was supported in part by NSF grants CCF-1320304 and CCF-1440014.

II. Problem Statement

Let $l \in \mathbb{N}^*$ and $\mathcal{L} \triangleq [\![1, l]\!]$. Define a MAC $(\mathcal{X}_{\mathcal{L}}, W_{Z|X_{\mathcal{L}}}, \mathcal{Z})$ with $\mathcal{Z}$, $\mathcal{X}_i$, $i \in \mathcal{L}$, finite alphabets, and $\mathcal{X}_{\mathcal{L}} \triangleq (\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_l)$. The MAC is such that the inputs are independent. We note $q_{ZX_{\mathcal{L}}} \triangleq W_{Z|X_{\mathcal{L}}} \prod_{i \in \mathcal{L}} q_{X_i}$ for uniform distribution q_{X_i}, $i \in \mathcal{L}$. We denote by $q_{X_{\mathcal{L}}}$ the uniform distribution on $\mathcal{X}_{\mathcal{L}}$, and we denote by q_{Z^n} the corresponding independent identically distributed (i.i.d.) channel output distribution, i.e.

$$\forall \mathbf{z} \in \mathcal{Z}^n, q_{Z^n}(\mathbf{z}) = \prod_{i=1}^{n} \sum_{x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}} W_{Z|X_{\mathcal{L}}}(z_i|(x_{\mathcal{L}})_i) q_{X_{\mathcal{L}}}((x_{\mathcal{L}})_i),$$

where $Z^n = (Z_1, \cdots, Z_n)$ is a vector of n random variables, $\mathbf{z} = (z_1, \cdots, z_n)$ is a vector of n sample values. We also note $X_{\mathcal{L}} \triangleq (X_1, \cdots, X_l)$, while a particular realization $i \in [\![1, n]\!]$ is denoted by $(x_{\mathcal{L}})_i$, and $\mathbf{x}_{\mathcal{L}} \triangleq ((x_{\mathcal{L}})_1, \cdots, (x_{\mathcal{L}})_n)$.

The problem of channel resolvability consists in asking whether one can approximate the distribution q_{Z^n} by using codewords chosen uniformly at random in a $(\{2^{nR_i}\}_{i \in \mathcal{L}}, n)$ code. If $\mathcal{C}_{\mathcal{L}}$ denotes the corresponding codebook, the distribution induced by the code is then

$$\forall \mathbf{z} \in \mathcal{Z}^n, \quad p_{Z^n}(\mathbf{z}) = \sum_{\mathbf{x}_{\mathcal{L}} \in \mathcal{C}_{\mathcal{L}}} W_{Z^n|X_{\mathcal{L}}^n}(\mathbf{z}|\mathbf{x}_{\mathcal{L}}) \frac{1}{|\mathcal{C}_{\mathcal{L}}|}.$$

Rates $\{R_i\}_{i \in \mathcal{L}}$ are achievable if there exists a sequence of $(\{2^{nR_i}\}_{i \in \mathcal{L}}, n)$ codes such that $\lim_{n \to \infty} \mathbb{V}(q_{Z^n}, p_{Z^n}) = 0$. For any $\mathcal{J} \subseteq \mathcal{L}$, we note $R_{\mathcal{J}} \triangleq \sum_{j \in \mathcal{J}} R_j$.

978-1-4799-5999-0/14/$31.00 ©2014 IEEE

III. MAC Resolvability with Invertible Extractors

In this section we consider MAC resolvability codes built from invertible extractors. This method is inspired from [11] and [10], which consider invertible extractors to construct wiretap codes, but do not consider resolvability directly. The proof technique is different from the one in [10], and neither requires [10, Lemma 5.1] nor [10, Lemma 5.4].

A. Construction and result

Let $i \in \mathcal{L}$ be the index of the input of the MAC. We assume $\mathcal{X}_i \triangleq \mathbb{F}_2$. For a seed $\mathbf{s}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, we consider a universal$_2$ extractor

$$\mathrm{Ext}_i : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^{n-k_i} : (\mathbf{s}_i, \mathbf{x}_i) \mapsto \mathbf{b}_i,$$

which means $\mathbb{P}[\mathrm{Ext}_i(\mathbf{S}_i, \mathbf{x}_i) = \mathrm{Ext}_i(\mathbf{S}_i, \mathbf{x}_i')] \leq 2^{-(n-k_i)}$, for all $\mathbf{x}_i \neq \mathbf{x}_i'$ and uniformly distributed $\mathbf{S}_i$. For $\mathbf{s}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, $\mathbf{b}_i \in \mathbb{F}_2^{n-k_i}$ we define the pre-image of $\mathbf{b}_i$ as $\mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i} \triangleq \{\mathbf{x}_i \in \mathbb{F}_2^n : \mathrm{Ext}_i(\mathbf{s}_i, \mathbf{x}_i) = \mathbf{b}_i\}$. Moreover, we impose that Ext_i is regular, that is, $\{\mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i}\}_{\mathbf{b}_i \in \mathbb{F}_2^{n-k}}$ is a partition of $\mathbb{F}_2^n$ into bins indexed by $\mathbf{b}_i$ and of equal size 2^{k_i}. The inverter Inv_i of Ext_i is defined as

$$\mathrm{Inv}_i : \mathbb{F}_2^n \times \mathbb{F}_2^{n-k_i} \times \mathbb{F}_2^{k_i} \to \mathbb{F}_2^n : (\mathbf{s}_i, \mathbf{b}_i, \mathbf{r}_i) \mapsto \mathbf{x}_i,$$

such that for fixed $\mathbf{s}_i$ and $\mathbf{b}_i$, $\mathbf{r}_i \mapsto \mathrm{Inv}_i(\mathbf{s}_i, \mathbf{b}_i, \mathbf{r}_i)$ defines an encoder with rate $R_i \triangleq k_i/n$ for the codebook $\mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i}$, which outputs a codeword uniform in $\mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i}$ when $\mathbf{r}_i$ is chosen uniformly at random in $\mathbb{F}_2^{k_i}$. We assume $S_\mathcal{L} \triangleq (\mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_l)$ and $B_\mathcal{L} \triangleq (\mathbf{B}_1, \mathbf{B}_2, \cdots, \mathbf{B}_l)$ uniformly distributed.

Theorem 1. *Let $n \in \mathbb{N}$, $\mathbf{s}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, $\mathbf{b}_i \in \mathbb{F}_2^{n-k_i}$, $i \in \mathcal{L}$. Assume the following encoders*

$$\{f_n^{(i)} : \mathbb{F}_2^{k_i} \to \mathbb{F}_2^n : \mathbf{r}_i \mapsto \mathrm{Inv}_i(\mathbf{s}_i, \mathbf{b}_i, \mathbf{r}_i)\}_{i\in\mathcal{L}},$$

with rates $R_i \triangleq k_i/n$, for $i \in \mathcal{L}$. Then, for the rate region $\{\{R_i\}_{i\in\mathcal{L}} : R_\mathcal{J} \geq I(Z; X_\mathcal{J}), \mathcal{J} \subseteq \mathcal{L}\backslash\{\emptyset\}\}$, we have

$$\lim_{n\to\infty} \mathbb{E}_{S_\mathcal{L},B_\mathcal{L}}[\mathbb{D}(p_{Z^n}, q_{Z^n})] = 0.$$

Note that Theorem 1 only shows existence of codes and does not provide an explicit scheme, since we average over $S_\mathcal{L}$ and $B_\mathcal{L}$.

B. Proof of Theorem 1

We note $\mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}} \triangleq \prod_{i\in\mathcal{L}} \mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i}$, where $\prod$ denotes the cartesian product. Averaging over all the codebooks, we have

$$\begin{aligned}
&\mathbb{E}_{S_\mathcal{L},B_\mathcal{L}}[\mathbb{D}(p_{Z^n}, q_{Z^n})] \\
&\overset{(a)}{=} \sum_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) q_{B_\mathcal{L}}(\mathbf{b}_\mathcal{L}) \\
&\quad \sum_{\mathbf{z}} \sum_{\mathbf{x}_\mathcal{L} \in \mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}} \frac{W(\mathbf{z}|\mathbf{x}_\mathcal{L})}{|\mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}|} \log \left[\frac{\sum_{\mathbf{x}'_\mathcal{L} \in \mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}} \frac{W(\mathbf{z}|\mathbf{x}'_\mathcal{L})}{|\mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}|}}{q_{Z^n}(\mathbf{z})} \right] \\
&\overset{(b)}{=} \sum_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L},\mathbf{z},\mathbf{x}_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) \frac{\mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L}) = \mathbf{b}_\mathcal{L}\}}{2^{l\cdot n}} W(\mathbf{z}|\mathbf{x}_\mathcal{L}) \\
&\quad \times \log \left[\frac{\sum_{\mathbf{x}'_\mathcal{L}} \mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}'_\mathcal{L}) = \mathbf{b}_\mathcal{L}\} W(\mathbf{z}|\mathbf{x}'_\mathcal{L})}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \right] \\
&= \sum_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L},\mathbf{z},\mathbf{x}_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) \frac{\mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L}) = \mathbf{b}_\mathcal{L}\}}{2^{l\cdot n}} W(\mathbf{z}|\mathbf{x}_\mathcal{L}) \\
&\quad \times \log \left[\frac{\sum_{\mathbf{x}'_\mathcal{L}} \mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}'_\mathcal{L}) = \mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L})\} W(\mathbf{z}|\mathbf{x}'_\mathcal{L})}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \right] \\
&\overset{(c)}{=} \sum_{\mathbf{s}_\mathcal{L},\mathbf{z},\mathbf{x}_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) \frac{W(\mathbf{z}|\mathbf{x}_\mathcal{L})}{2^{l\cdot n}} \\
&\quad \times \log \left[\frac{\sum_{\mathbf{x}'_\mathcal{L}} \mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}'_\mathcal{L}) = \mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L})\} W(\mathbf{z}|\mathbf{x}'_\mathcal{L})}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \right] \\
&\overset{(d)}{\leq} \sum_{\mathbf{z},\mathbf{x}_\mathcal{L}} \frac{W(\mathbf{z}|\mathbf{x}_\mathcal{L})}{2^{l\cdot n}} \log \Bigg[\sum_{\mathbf{s}_\mathcal{L},\mathbf{x}'_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) W(\mathbf{z}|\mathbf{x}'_\mathcal{L}) \\
&\qquad \times \frac{\mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}'_\mathcal{L}) = \mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L})\}}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \Bigg], \quad (1)
\end{aligned}$$

where (a) holds because Inv_i uniformly draws an element in $\mathcal{P}_{\mathbf{s}_i,\mathbf{b}_i}$, $i \in \mathcal{L}$, (b) holds because $\mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L}) = \mathbf{b}_\mathcal{L}\} \triangleq \prod_{i\in\mathcal{L}} \mathbb{1}\{\mathrm{Ext}_i(\mathbf{s}_i, \mathbf{x}_i) = \mathbf{b}_i\}$, $|\mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}| = 2^{k_\mathcal{L}}$, $q_{B_\mathcal{L}}(\mathbf{b}_\mathcal{L}) = 2^{l\cdot n - k_\mathcal{L}}$, with $k_\mathcal{J} \triangleq \sum_{j\in\mathcal{J}} k_j$ for $\mathcal{J} \subseteq \mathcal{L}$, and by definition of $\mathcal{P}_{\mathbf{s}_\mathcal{L},\mathbf{b}_\mathcal{L}}$, (c) holds because $\sum_{\mathbf{b}_\mathcal{L}} \mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L}) = \mathbf{b}_\mathcal{L}\} = 1$, (d) holds by Jensen's inequality.

Assume that $\mathbf{x}_\mathcal{L} \neq \mathbf{x}'_\mathcal{L}$, we separate the sum $\sum_{\mathbf{x}'_\mathcal{L} \neq \mathbf{x}_\mathcal{L}}$, by introducing $\mathcal{J} \subseteq \mathcal{L}$ such that $\forall j \in \mathcal{J}, \mathbf{x}_j \neq \mathbf{x}'_j$. By convention $\mathcal{J} = \emptyset$ corresponds to $\mathbf{x}_\mathcal{L} = \mathbf{x}'_\mathcal{L}$. Hence,

$$\begin{aligned}
&\sum_{\mathbf{s}_\mathcal{L},\mathbf{x}'_\mathcal{L}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) W(\mathbf{z}|\mathbf{x}'_\mathcal{L}) \frac{\mathbb{1}\{\mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}'_\mathcal{L}) = \mathrm{Ext}_\mathcal{L}(\mathbf{s}_\mathcal{L}, \mathbf{x}_\mathcal{L})\}}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \\
&= \sum_{\mathcal{J}\subseteq\mathcal{L}} \sum_{\mathbf{s}_\mathcal{L},\mathbf{x}'_\mathcal{J}} q_{S_\mathcal{L}}(\mathbf{s}_\mathcal{L}) W(\mathbf{z}|\mathbf{x}'_\mathcal{J}\mathbf{x}_{\mathcal{J}^c}) \\
&\qquad \times \frac{\mathbb{1}\{\mathrm{Ext}_\mathcal{J}(\mathbf{s}_\mathcal{J}, \mathbf{x}'_\mathcal{J}) = \mathrm{Ext}_\mathcal{J}(\mathbf{s}_\mathcal{J}, \mathbf{x}_\mathcal{J})\}}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \\
&= \sum_{\mathcal{J}\subseteq\mathcal{L}} \sum_{\mathbf{s}_{\mathcal{J}^c},\mathbf{x}'_\mathcal{J}} q_{S_{\mathcal{J}^c}}(\mathbf{s}_{\mathcal{J}^c}) W(\mathbf{z}|\mathbf{x}'_\mathcal{J}\mathbf{x}_{\mathcal{J}^c}) \\
&\qquad \times \frac{\mathbb{P}[\mathrm{Ext}_\mathcal{J}(\mathbf{S}_\mathcal{J}, \mathbf{x}'_\mathcal{J}) = \mathrm{Ext}_\mathcal{J}(\mathbf{S}_\mathcal{J}, \mathbf{x}_\mathcal{J})]}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \\
&\overset{(a)}{\leq} \sum_{\mathcal{J}\subseteq\mathcal{L}} \sum_{\mathbf{s}_{\mathcal{J}^c},\mathbf{x}'_\mathcal{J}} q_{S_{\mathcal{J}^c}}(\mathbf{s}_{\mathcal{J}^c}) W(\mathbf{z}|\mathbf{x}'_\mathcal{J}\mathbf{x}_{\mathcal{J}^c}) \frac{2^{-(n\cdot|\mathcal{J}|-k_\mathcal{J})}}{2^{k_\mathcal{L}} q_{Z^n}(\mathbf{z})} \\
&= \sum_{\mathcal{J}\subseteq\mathcal{L}} \sum_{\mathbf{x}'_\mathcal{J}} W(\mathbf{z}|\mathbf{x}'_\mathcal{J}\mathbf{x}_{\mathcal{J}^c}) \frac{2^{-n\cdot|\mathcal{J}|}}{2^{k_{\mathcal{J}^c}} q_{Z^n}(\mathbf{z})} \\
&= \sum_{\mathcal{J}\subseteq\mathcal{L}} \frac{1}{2^{k_{\mathcal{J}^c}}} \frac{W(\mathbf{z}|\mathbf{x}_{\mathcal{J}^c})}{q_{Z^n}(\mathbf{z})} \\
&= 1 + \sum_{\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}} \frac{1}{2^{k_\mathcal{J}}} \frac{W(\mathbf{z}|\mathbf{x}_\mathcal{J})}{q_{Z^n}(\mathbf{z})} \\
&\overset{(b)}{\leq} 1 + \begin{cases} \sum_{\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}} \frac{2^{-nH(Z|X_\mathcal{J})(1-\epsilon)}}{2^{nR_\mathcal{J}} 2^{-nH(Z)(1+\epsilon)}}, \text{ if } (\mathbf{x}_\mathcal{L}, \mathbf{z}) \in \mathcal{T}_\epsilon^n(XZ) \\ 2^l \mu_Z^{-n}, \text{ if } (\mathbf{x}_\mathcal{L}, \mathbf{z}) \notin \mathcal{T}_\epsilon^n(XZ) \end{cases} \quad (2)
\end{aligned}$$

where (a) holds because Ext_i, $i \in \mathcal{L}$, is universal$_2$, and (b) holds for any $\epsilon > 0$ with $\mu_Z \triangleq \min_{z\in supp(q_Z)} q_Z(z)$ by standard arguments of typicality.

Hence, by (1), (2) we have $\mathbb{E}_{S_\mathcal{L},B_\mathcal{L}}[\mathbb{D}(p_{Z^n},q_{Z^n})] \leq A+B$, where

$$\begin{aligned} A &\triangleq \sum_{(\mathbf{x}_\mathcal{L},\mathbf{z})\notin\mathcal{T}_\epsilon^n(XZ)} q(\mathbf{x}_\mathcal{L},\mathbf{z})\log\left[1+2^l\mu_Z^{-n}\right] \\ &\leq \frac{n2^{l/n}}{\mu_Z}\mathbb{P}[(X_\mathcal{L}^n,Z^n)\notin\mathcal{T}_\epsilon^n(XZ)] \\ &\leq \frac{n2^{l/n}}{\mu_Z}2|\mathcal{X}_\mathcal{L}||\mathcal{Z}|2^{-2n\epsilon^2\mu_{X_\mathcal{L}Z}} \overset{n\to\infty}{\longrightarrow} 0, \end{aligned}$$

and

$$\begin{aligned} B &\triangleq \sum_{(\mathbf{x}_\mathcal{L},\mathbf{z})\in\mathcal{T}_\epsilon^n(XZ)} q(\mathbf{x}_\mathcal{L},\mathbf{z})\log\left[1+\sum_{\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}}\frac{2^{-nH(Z|X_\mathcal{J})(1-\epsilon)}}{2^{nR_\mathcal{J}}2^{-nH(Z)(1+\epsilon)}}\right] \\ &\leq \sum_{\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}}\exp_2\left[-n(R_\mathcal{J}-I(Z;X_\mathcal{J})-2\epsilon H(Z))\right], \end{aligned}$$

which concludes the proof.

IV. MAC Resolvability with injective group homomorphisms

In this section, we consider MAC resolvability codes based on a class of injective group homomorphisms, introduced in [12] for point-to-point channel resolvability.

A. Construction and result

Let $n\in\mathbb{N}$ and $i\in\mathcal{L}$. Let $\mathcal{M}_i$ be an Abelian group with $|\mathcal{M}_i|\triangleq 2^{nR_i}$. We note $M_i\triangleq|\mathcal{M}_i|$, $M_\mathcal{L}\triangleq\prod_{i=1}^l M_i$. Assume that $\mathcal{X}_i^n$ is also an Abelian group. For $\mathbf{x}_i\in\mathcal{X}_i^n$, $\mathbf{m}_i\in\mathcal{M}_i$, we note $\mathbf{m}_\mathcal{L}\triangleq(\mathbf{m}_1,\mathbf{m}_2,\dots\mathbf{m}_l)$. Consider a family of encoders that take as input $\mathbf{m}_i$ and output $F_i(\mathbf{m}_i)+G_i^n$, where

- F_i is drawn in a family $\mathcal{F}_i$ of injective group homomorphism and verifies $F_i:\mathcal{M}_i\to\mathcal{X}_i^n$, such that for $\mathbf{x}_i\neq\mathbf{0}$, $\mathbf{m}_i\neq\mathbf{0}$,
$$\mathbb{P}[F_i(\mathbf{m}_i)=\mathbf{x}_i]\leq\frac{1}{|\mathcal{X}_i^n|}, \tag{3}$$
- G_i^n is drawn in $\mathcal{X}_i^n$ uniformly.

We define the direct products $\mathcal{M}_\mathcal{L}\triangleq\mathcal{M}_1\times\mathcal{M}_2\times\ldots\times\mathcal{M}_l$ and $\mathcal{X}_\mathcal{L}^n\triangleq\mathcal{X}_1^n\times\mathcal{X}_2^n\times\ldots\times\mathcal{X}_l^n$. We note $F_\mathcal{L}:\mathcal{M}_\mathcal{L}\to\mathcal{X}_\mathcal{L}^n, m_\mathcal{L}\mapsto(F_1(m_1),F_2(m_2),\dots,F_l(m_l))$ and $G_\mathcal{L}^n\triangleq(G_1^n,G_2^n,\dots,G_l^n)$.

Theorem 2. *Let $n\in\mathbb{N}$. Assume the following encoders*

$$\{f_n^{(i)}:\mathcal{M}_i\to\mathcal{X}_i^n:\mathbf{m}_i\mapsto F_i(\mathbf{m}_i)+G_i^n\}_{i\in\mathcal{L}},$$

with rates $\{R_i\}_{i\in\mathcal{L}}$. Then, for the rate region $\{\{R_i\}_{i\in\mathcal{L}}: R_\mathcal{J}\geq I(Z;X_\mathcal{J}),\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}\}$, we have

$$\lim_{n\to\infty}\mathbb{E}_{F_\mathcal{L},G_\mathcal{L}^n}[\mathbb{D}(p_{Z^n},q_{Z^n})]=0.$$

Note that as in Theorem 1, Theorem 2 does not provide an explicit scheme, since we average over $F_\mathcal{L}$ and $G_\mathcal{L}^n$.

B. Proof sketch of Theorem 2

Observe that the direct products $\mathcal{M}_\mathcal{L}$ and $\mathcal{X}_\mathcal{L}^n$ are Abelian groups. Hence, $F_\mathcal{L}$ is an injective group homomorphism. Averaging over all the family of encoders, we can show

$$\begin{aligned} &\mathbb{E}_{F_\mathcal{L},G_\mathcal{L}^n}[\mathbb{D}(p_{Z^n},q_{Z^n})] \\ &\overset{(a)}{\leq}\sum_{\mathbf{z},\mathbf{m}_\mathcal{L},\mathbf{x}_\mathcal{L}}\frac{q(\mathbf{z},\mathbf{x}_\mathcal{L})}{M_\mathcal{L}} \\ &\qquad\times\log\left[\frac{1}{M_\mathcal{L}}\sum_{\mathbf{m}'_\mathcal{L},f_\mathcal{L}}p_{F_\mathcal{L}}(f_\mathcal{L})\frac{W(\mathbf{z}|f_\mathcal{L}(\mathbf{m}'_\mathcal{L}-\mathbf{m}_\mathcal{L})+\mathbf{x}_\mathcal{L})}{q_{Z^n}(\mathbf{z})}\right] \\ &\overset{(b)}{\leq}\log\left[1+\sum_{\mathcal{J}\subseteq\mathcal{L}\setminus\{\emptyset\}}\frac{1}{M_\mathcal{J}}\frac{W(\mathbf{z}|\mathbf{x}_\mathcal{J})}{q_{Z^n}(\mathbf{z})}\right]. \end{aligned}$$

where (a) is obtained after some computations using the fact that $f_\mathcal{L}$ is a group homomorphism, and by Jensen's inequality, (b) can be seen as the counterpart of Equation (2) and can be proved using Condition (3) instead of the universal$_2$ property. We then conclude with a proof similar to the one in Section III-B. We omit the details due to space constraints.

V. Resolvability for the symmetric MAC

We have shown in Sections III and IV that there exists some families of invertible extractors and injective group homomorphisms suitable for MAC resolvability. However, we have not provided explicit codes, since (i) we have not provided explicit families of encoders, and (ii) we perform an averaging over all the members of the family of encoders in Theorems 1 and 2. When the MAC is symmetric, we show in this section how to deal with (i). We will deal with (ii) in Section VI.

We consider symmetric MACs $W_{Z|X_\mathcal{L}}$ in the sense that, for any $a_\mathcal{L}\in\mathcal{X}_\mathcal{L}$ there exists a permutation π_a such that for any $x_\mathcal{L}\in\mathcal{X}_\mathcal{L}$, for any $z\in\mathcal{Z}$, we have

$$W(z|a_\mathcal{L}+x_\mathcal{L})=W(\pi_a\circ z|x_\mathcal{L}).$$

Symmetry allows us to remove one averaging in Theorems 1 and 2 as follows.

Lemma 1. *Let $n\in\mathbb{N}$. We consider the encoders of Theorem 1 and assume a symmetric MAC. Let $\mathbf{b}_i,\mathbf{b}'_i\in\mathbb{F}_2^{n-k_i}$, $i\in\mathcal{L}$, then we have*

$$\mathbb{E}_{S_\mathcal{L},B_{\mathcal{L}=\mathbf{b}_\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})]=\mathbb{E}_{S_\mathcal{L},B_{\mathcal{L}=\mathbf{b}'_\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})].$$

The proof of Lemma 1 is similar to the proof of Lemma 2 and is thus omitted.

Lemma 2. *Let $n\in\mathbb{N}$. We consider the encoders of Theorem 2 and assume a symmetric MAC. For any $\mathbf{g}_\mathcal{L},\mathbf{g}'_\mathcal{L}\in\mathcal{X}_\mathcal{L}^n$, we have*

$$\mathbb{E}_{F_\mathcal{L},G^n_{\mathcal{L}=\mathbf{g}_\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})]=\mathbb{E}_{F_\mathcal{L},G^n_{\mathcal{L}=\mathbf{g}'_\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})].$$

Proof. Let $\mathbf{g}_\mathcal{L},\mathbf{g}'_\mathcal{L}\in\mathcal{X}_\mathcal{L}^n$. Let $\mathbf{d}_\mathcal{L}\triangleq\mathbf{g}'_\mathcal{L}-\mathbf{g}_\mathcal{L}$ and $\pi_\mathbf{d}$ such that for any $x_\mathcal{L}$, $W(\mathbf{z}|\mathbf{x}_\mathcal{L}+\mathbf{d}_\mathcal{L})=W(\pi_\mathbf{d}\circ\mathbf{z}|\mathbf{x}_\mathcal{L})$.

$$
\begin{aligned}
&\mathbb{E}_{F_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})]\\
&=\sum_{f_{\mathcal{L}}} p_{F_{\mathcal{L}}}(f_{\mathcal{L}})\sum_{\mathbf{z}}\sum_{\mathbf{m}_{\mathcal{L}}}\frac{W(\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}_{\mathcal{L}})}{M_{\mathcal{L}}}\\
&\qquad\times\log\left[\frac{1}{M_{\mathcal{L}}}\frac{\sum_{\mathbf{m}_{\mathcal{L}}}W(\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}_{\mathcal{L}})}{\sum_{\mathbf{x}_{\mathcal{L}}}W(\mathbf{z}|\mathbf{x}_{\mathcal{L}})q_{X^n_{\mathcal{L}}}(\mathbf{x}_{\mathcal{L}})}\right]\\
&=\sum_{f_{\mathcal{L}}} p_{F_{\mathcal{L}}}(f_{\mathcal{L}})\sum_{\mathbf{z}}\sum_{\mathbf{m}_{\mathcal{L}}}\frac{W(\pi_{\mathbf{d}}\circ\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}_{\mathcal{L}})}{M_{\mathcal{L}}}\\
&\qquad\times\log\left[\frac{1}{M_{\mathcal{L}}}\frac{\sum_{\mathbf{m}_{\mathcal{L}}}W(\pi_{\mathbf{d}}\circ\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}_{\mathcal{L}})}{\sum_{\mathbf{x}_{\mathcal{L}}}W(\pi_{\mathbf{d}}\circ\mathbf{z}|\mathbf{x}_{\mathcal{L}})q_{X^n_{\mathcal{L}}}(\mathbf{x}_{\mathcal{L}})}\right]\\
&\overset{(a)}{=}\sum_{f_{\mathcal{L}}} p_{F_{\mathcal{L}}}(f_{\mathcal{L}})\sum_{\mathbf{z}}\sum_{\mathbf{m}_{\mathcal{L}}}\frac{W(\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}'_{\mathcal{L}})}{M_{\mathcal{L}}}\\
&\qquad\times\log\left[\frac{1}{M_{\mathcal{L}}}\frac{\sum_{\mathbf{m}_{\mathcal{L}}}W(\mathbf{z}|f_{\mathcal{L}}(\mathbf{m}_{\mathcal{L}})+\mathbf{g}'_{\mathcal{L}})}{\sum_{\mathbf{x}'_{\mathcal{L}}}W(\mathbf{z}|\mathbf{x}'_{\mathcal{L}})q_{X^n_{\mathcal{L}}}(\mathbf{x}'_{\mathcal{L}})}\right]\\
&=\mathbb{E}_{F_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}'_{\mathcal{L}}}[\mathbb{D}(p_{Z^n},q_{Z^n})],
\end{aligned}
$$

where (a) holds because $q_{X^n_{\mathcal{L}}}$ is uniform. □

The remaining averaging in Theorems 1 and 2 consists in choosing at random an encoder in some set, which requires a uniform random number. We next show how the rate of this uniform random number can be made negligible, by reusing the same encoder over several transmission blocks.

Lemma 3. *Let $t\in\mathbb{N}$. Define $N\triangleq n\cdot t$. Consider the encoder $e^n(\cdot)\triangleq Inv_{\mathcal{L}}(\mathbf{s}_{\mathcal{L}},\mathbf{b}_{\mathcal{L}},\cdot)$, with $Inv_{\mathcal{L}}(\mathbf{s}_{\mathcal{L}},\mathbf{b}_{\mathcal{L}},\cdot)\triangleq(Inv_1(\mathbf{s}_1,\mathbf{b}_1,\cdot),\cdots,Inv_l(\mathbf{s}_l,\mathbf{b}_l,\cdot))$, where $\mathbf{s}_i\in\mathbb{F}_2^n$, $\mathbf{b}_i\in\mathbb{F}_2^{n-k_i}$, and Inv_i is defined as in Section III, $i\in\mathcal{L}$. We note $p_{Z^N|\mathcal{S}_{\mathcal{L}}=\mathbf{s}_{\mathcal{L}},\mathcal{B}_{\mathcal{L}}=\mathbf{b}_{\mathcal{L}}}$ the induced distribution by the concatenated outputs of encoder e^n, on t blocks of size n, where for each block the same encoder e^n is used. We note $p_{Z^n|\mathcal{S}_{\mathcal{L}}=\mathbf{s}_{\mathcal{L}},\mathcal{B}_{\mathcal{L}}=\mathbf{b}_{\mathcal{L}}}$ the induced distribution by the output of encoder e^n, on 1 block of size n. Then, we have*

$$
\begin{aligned}
&\mathbb{E}_{\mathcal{S}_{\mathcal{L}}}[\mathbb{V}(p_{Z^N|\mathcal{S}_{\mathcal{L}}=\mathbf{s}_{\mathcal{L}},\mathcal{B}_{\mathcal{L}}=\mathbf{b}_{\mathcal{L}}},q_{Z^N})]\\
&\qquad\le t\cdot\mathbb{E}_{\mathcal{S}_{\mathcal{L}}}[\mathbb{V}(p_{Z^n|\mathcal{S}_{\mathcal{L}}=\mathbf{s}_{\mathcal{L}},\mathcal{B}_{\mathcal{L}}=\mathbf{b}_{\mathcal{L}}},q_{Z^n})].
\end{aligned}
$$

Since $\mathbb{E}_{\mathcal{S}_{\mathcal{L}}}[\mathbb{V}(p_{Z^n|\mathcal{S}_{\mathcal{L}}=\mathbf{s}_{\mathcal{L}},\mathcal{B}_{\mathcal{L}}=\mathbf{b}_{\mathcal{L}}},q_{Z^n})]$ decreases exponentially fast with n in the proof of Theorem 1 by Pinsker's inequality, t can be chosen $O(e^{\alpha n})$ with a suitably small α; in other words, the effective rate of the seed $\mathbf{s}_{\mathcal{L}}$ is $O(\frac{\log n}{n})$. The proof of Lemma 3 is similar to the proof of Lemma 4 and is thus omitted. The technique used is referred to as "hybrid argument" in the computer science literature. Note that the proof requires the triangle inequality and consequently does not apply to relative entropy.

Lemma 4. *Let $t\in\mathbb{N}$. Define $N\triangleq n\cdot t$. Consider the encoder $e^n(\cdot)\triangleq f_{\mathcal{L}}(\cdot)+\mathbf{g}_{\mathcal{L}}$, with $f_{\mathcal{L}}$ and $\mathbf{g}_{\mathcal{L}}$ defined as in Section IV. We note $p_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}$ the induced distribution by the concatenated outputs of encoder e^n, on t blocks of size n, and where for each block the same encoder e^n is used. We note $p_{Z^n|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}$ the induced distribution by the output of encoder e^n, on 1 block of size n. Then, we have*

$$
\begin{aligned}
&\mathbb{E}_{F_{\mathcal{L}}}[\mathbb{V}(p_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},q_{Z^N})]\\
&\qquad\le t\cdot\mathbb{E}_{F_{\mathcal{L}}}[\mathbb{V}(p_{Z^n|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},q_{Z^n})].
\end{aligned}
$$

Proof. Let $\mathbf{g}_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}^n$. Let U be a uniform random variable over $\mathcal{M}_{\mathcal{L}}^t$, written as $U=(U_1^{nR_{\mathcal{L}}}||U_2^{nR_{\mathcal{L}}}||\dots||U_t^{nR_{\mathcal{L}}})$, where $(\cdot||\cdot)$ denotes concatenation. Let also $\bar{U}$ be a uniform random variable over $\mathcal{X}_{\mathcal{L}}^N$, written as $\bar{U}=(\bar{U}_1^{l\cdot n}||\bar{U}_2^{l\cdot n}||\dots||\bar{U}_t^{l\cdot n})$. For $i\in[\![0,t]\!]$, we note $p^{(i)}_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}$ the induced distribution by the concatenation of the i outputs of $f_{\mathcal{L}}(\cdot)+\mathbf{g}_{\mathcal{L}}$ with input $U_j^{nR_{\mathcal{L}}}$ for $j\in[\![1,i]\!]$, and the $t-i$ outputs of $W_{Z^n|X^n_{\mathcal{L}}}$ with input $\bar{U}_j^{l\cdot n}$ for $j\in[\![i+1,t]\!]$. Hence, $p^{(t)}_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}=p_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}$ and $p^{(0)}_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}=q_{Z^N}$. We thus have by the triangle inequality,

$$
\begin{aligned}
&\mathbb{E}_{F_{\mathcal{L}}}[\mathbb{V}(p_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},q_{Z^N})]\\
&\le\sum_{i=1}^{t}\mathbb{E}_{F_{\mathcal{L}}}\left[\mathbb{V}\left(p^{(i-1)}_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},p^{(i)}_{Z^N|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}}\right)\right]\\
&\le\sum_{i=1}^{t}\mathbb{E}_{F_{\mathcal{L}}}\left[\mathbb{V}\left(p_{Z^n|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},q_{Z^n}\right)\right]\\
&=t\cdot\mathbb{E}_{F_{\mathcal{L}}}\left[\mathbb{V}\left(p_{Z^n|F_{\mathcal{L}}=f_{\mathcal{L}},G^n_{\mathcal{L}}=\mathbf{g}_{\mathcal{L}}},q_{Z^n}\right)\right],
\end{aligned}
$$

where the second inequality follows from the data processing inequality for the variational distance, and the last equality follows from Lemma 2. □

VI. Low-Complexity Codes for the Symmetric MAC

Thanks to Sections III, IV, V, we are ready to provide low-complexity codes to perform resolvability for a symmetric MAC. We provide two examples of families of invertible extractors and one example of families of injective group homomorphisms.

A. Encoders for MAC resolvability with invertible extractors

1) Invertible extractor with finite-field multiplication: Let $i\in\mathcal{L}$. Define, for any seed $\mathbf{s}_i\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}$, the extractor

$$
\mathrm{Ext}_i:\mathbb{F}_2^n\times\mathbb{F}_2^n\to\mathbb{F}_2^{n-k_i}:(\mathbf{s}_i,\mathbf{x}_i)\mapsto\mathbf{b}_i\triangleq(\mathbf{s}_i^{-1}\odot\mathbf{x}_i)|_{[\![1,n-k_i]\!]},
$$

where $\odot$ is the multiplication in $\mathbb{F}_{2^n}$ and $(\cdot)|_{[\![1,n-k_i]\!]}$ is the truncation of the last k_i bits. Ext_i is a universal$_2$ hash function [10], and the inverter of Ext_i is

$$
\mathrm{Inv}_i:\mathbb{F}_2^n\times\mathbb{F}_2^{n-k_i}\times\mathbb{F}_2^{k_i}\to\mathbb{F}_2^n:(\mathbf{s}_i,\mathbf{b}_i,\mathbf{r}_i)\mapsto\mathbf{s}_i\odot(\mathbf{b}_i\|\mathbf{r}_i),
$$

where $(\cdot\|\cdot)$ denotes the concatenation of two vectors.

The encoding complexity can be performed in $O(n\log n)$, for some, but limited, values of n. Indeed, the finite-field multiplication can be reduced to a ring multiplication, which is a convolution and can be efficiently perform by the number theoretic transform (see for instance [13, Section 7.3]). However, the main issue is to find an irreducible polynomial

in $\mathbb{Z}_2[X]$ of degree n. Although it can be done when n is a Mersenne exponent, that is $2^n - 1$ is prime, it is a difficult problem for arbitrary n.

2) Invertible extractor with Toeplitz matrices: The choice of this family is inspired by [11]. Let $i \in \mathcal{L}$. Define $T_i(\mathbf{S})$ a random Toeplitz matrix in $\mathbb{F}_2^{k_i \times (n-k_i)}$ defined by $T_i(1,j) = S_{k_i+j-1}$ for $j \in [\![1, n-k_i]\!]$ and $T_i(l,1) = S_{k_i-l+1}$ for $l \in [\![1, k_i]\!]$ where $\mathbf{S}_i \triangleq (S_1, S_2, \dots S_{n-1}) \in \mathbb{F}_2^{n-1}$ is a uniform random vector. Define

$$G_i(\mathbf{S}) \triangleq [I_{k_i} | T_i(\mathbf{S})] \in \mathbb{F}_2^{k_i \times n},$$
$$H_i(\mathbf{S}) \triangleq [T_i^T(\mathbf{S}) | I_{n-k_i}]^T \in \mathbb{F}_2^{n \times (n-k_i)}.$$

It is shown in [11] that $\{H_i(\mathbf{s})\}_{\mathbf{s} \in \mathbb{F}_2^{n-1}}$ is a universal$_2$ family of extractors. We define

$$\mathrm{Ext}_i : \mathbb{F}_2^{n-1} \times \mathbb{F}_2^n \to \mathbb{F}_2^{n-k_i} : (\mathbf{s}_i, \mathbf{x}_i) \mapsto \mathbf{b}_i \triangleq \mathbf{x}_i H_i(\mathbf{s}_i),$$
$$\mathrm{Inv}_i : \mathbb{F}_2^{n-1} \times \mathbb{F}_2^{n-k_i} \times \mathbb{F}_2^{k_i} \to \mathbb{F}_2^n : (\mathbf{s}_i, \mathbf{0}, \mathbf{r}_i,) \mapsto \mathbf{r}_i G_i(\mathbf{s}_i).$$

For any $\mathbf{s}_i \in \mathbb{F}_2^{n-1}$, observe that Inv_i draws uniformly an element of $\mathcal{P}_{\mathbf{s}_i, \mathbf{b}_i = \mathbf{0}}$ when $\mathbf{r}_i$ is chosen uniformly at random in $\mathbb{F}_2^{k_i}$, since $\mathrm{rank}(G_i(\mathbf{s}_i)) = k_i$, and by definition of $G_i(\mathbf{s}_i)$ and $H_i(\mathbf{s}_i)$ we have

$$\mathrm{Ext}_i(\mathbf{s}_i, \mathbf{r}_i G_i(\mathbf{s}_i)) = \mathbf{r}_i G_i(\mathbf{s}_i) H_i(\mathbf{s}_i) = \mathbf{0}.$$

Encoding can be performed in $O(n \log n)$, for a wide range of values of n as shown in [14].

3) Explicit MAC resolvability codes: Combing Theorem 1, Lemma 1, and Lemma 3, we obtain the following result for the two families given above.

Theorem 3. *Assume a symmetric MAC. Let $n \in \mathbb{N}$, $\mathbf{s}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, $i \in \mathcal{L}$, and consider the following encoders*

$$\{f_n^{(i)} : \mathbb{F}_2^{k_i} \to \mathbb{F}_2^n : \mathbf{r}_i \mapsto \mathrm{Inv}_i(\mathbf{s}_i, \mathbf{0}, \mathbf{r}_i)\}_{i \in \mathcal{L}},$$

with rates $R_i \triangleq k_i/n$, for $i \in \mathcal{L}$. Then, for the rate region $\{\{R_i\}_{i \in \mathcal{L}} : R_{\mathcal{J}} \geq I(Z; X_{\mathcal{J}}), \mathcal{J} \subseteq \mathcal{L} \backslash \{\emptyset\}\}$, we have

$$\lim_{n \to \infty} \mathbb{E}_{S_{\mathcal{L}}, B_{\mathcal{L}} = \mathbf{0}}[\mathbb{V}(p_{Z^n}, q_{Z^n})] = 0.$$

Moreover, by Lemma 3, the seeds $\mathbf{s}_{\mathcal{L}}$ can be reused multiple times, such that their rate is on the order of $O(\frac{\log n}{n})$.

B. Encoders for MAC resolvability with injective group homomorphisms

1) Finite-field multiplication: Let $i \in \mathcal{L}$. Assume $\mathcal{X}_i = \mathbb{F}_2$. We define

$$F_i : \mathcal{M}_i \to \mathcal{X}_i^n, \mathbf{m}_i \mapsto \mathbf{S}_i \odot (\mathbf{m}_i || \mathbf{0}),$$

where $\mathbf{S}_i$ is a uniform random variable drawn in $\mathbb{F}_2^n \setminus \{\mathbf{0}\}$. We have for $\mathbf{m} \neq \mathbf{0}$ and $\mathbf{x} \neq \mathbf{0}$

$$\mathbb{P}[F_i(\mathbf{m}) = \mathbf{x}] = \sum_{\mathbf{s}_i} P_{\mathbf{S}_i}(\mathbf{s}_i) \mathbb{1}\{\mathbf{s}_i \odot (\mathbf{m} || \mathbf{0}) = \mathbf{x}\}$$
$$= \sum_{\mathbf{s}_i} \frac{1}{2^n} \mathbb{1}\{\mathbf{s}_i = \mathbf{x} \odot (\mathbf{m} || \mathbf{0})^{-1}\} = \frac{1}{2^n} = \frac{1}{|\mathcal{X}_i^n|}.$$

As in Section VI-A, encoding can be performed in $O(n \log n)$ thanks to the number theoretic transform, but again for a limited range of values of n.

2) Explicit MAC resolvability codes: Combining Theorem 2, Lemma 2, and Lemma 4, we obtain the following result for the family given above.

Theorem 4. *Assume a symmetric MAC. Let $n \in \mathbb{N}$, $\mathbf{s}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, $i \in \mathcal{L}$, and consider the following encoders*

$$\{f_n^{(i)} : \mathcal{M}_i \to \mathcal{X}_i^n : \mathbf{m}_i \mapsto F_i(\mathbf{m}_i)\}_{i \in \mathcal{L}},$$

with rates R_i, for $i \in \mathcal{L}$. Then, for the rate region $\{\{R_i\}_{i \in \mathcal{L}} : R_{\mathcal{J}} \geq I(Z; X_{\mathcal{J}}), \mathcal{J} \subseteq \mathcal{L} \backslash \{\emptyset\}\}$, we have

$$\lim_{n \to \infty} \mathbb{E}_{F_{\mathcal{L}}, G_{\mathcal{L}}^n = \mathbf{0}}[\mathbb{V}(p_{Z^n}, q_{Z^n})] = 0.$$

Moreover, by Lemma 4, the seeds $\mathbf{s}_{\mathcal{L}}$ can be reused multiple times, such that their rates is on the order of $O(\frac{\log n}{n})$.

Note that the family of encoders in Section VI-B1 is similar to the one used in Section VI-A1. Consequently, one can wonder whether the family of encoders based on Toeplitz matrix used for MAC resolvability with invertible extractors in SectionVI-A2 can also be used for MAC resolvability with injective group homomorphisms. The answer is no because Equation (3) is not satisfied. Specifically, if we let $i_0 \in \mathcal{L}$, $\mathbf{m} \in \mathbb{F}_2^{k_{i_0}} \backslash \{\mathbf{0}\}$, and define $F_{i_0} : \mathcal{M}_{i_0} \to \mathcal{X}_{i_0}^n, \mathbf{m}_{i_0} \mapsto \mathbf{m}_{i_0} G_{i_0}(\mathbf{S}_{i_0})$, $\mathbf{x} \triangleq (\mathbf{m} || \mathbf{z}) \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}$, where $\mathbf{z} \in \mathbb{F}_2^{n-k_{i_0}}$, we can show

$$\mathbb{P}[F_{i_0}(\mathbf{m}) = \mathbf{x}] = 2^{k_{i_0}} / |\mathcal{X}_i^n|.$$

REFERENCES

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

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

[3] J. Muramatsu and S. Miyake, "Construction of strongly secure wiretap channel code based on hash property," in *Proc. of Symp. Inf. Theory*, 2011, pp. 613–617.

[4] P. Cuff, H. Permuter, and T. Cover, "Coordination capacity," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4181–4206, 2010.

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

[6] M. Bloch, L. Luzzi, and J. Kliewer, "Strong coordination with polar codes," in *Proc. of 50th Allerton Conference on Communication, Control, and Computing*, 2012, pp. 565–571.

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

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

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

[10] M. Bellare and S. Tessaro, "Polynomial-time, semantically-secure encryption achieving the secrecy capacity," *arXiv preprint arXiv:1201.3160*, 2012.

[11] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, 2011.

[12] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *arXiv preprint arXiv:1202.1332*, 2012.

[13] G. Van Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.

[14] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with non-uniform random seeds via dual universal hash function," *arXiv preprint arXiv:1311.5322*, 2013.