Fifty-third Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 29 - October 2, 2015

Polar Codes for Secure Write-Efficient Memories

Qing Li* **and Anxiao (Andrew) Jiang***
* Computer Sci. and Eng. Dept.,Texas A & M University, College Station, TX, 77843
*{qingli, ajiang}@cse.tamu.edu

***Abstract*—Secure Write-Efficient Memory (WEM) was proposed in [11] to solve the endurance and the insecure deletion problems in flash memories. Information theoretical results, i.e., the achievable region and the secrecy rewriting capacity, have been obtained. In this work, a code construction for secure WEM is presented and it is optimal for a large family of secure WEM.**

I. Introduction

In this section, we present the background of secure Write-Efficient Memories including their motivations and formal definitions, brief obtained information theory results in [11], and show our contributions.

A. Motivation of secure Write-Efficient Memories

Flash memories are significant non-volatile memory techniques. The smallest unit of flash memory is a cell, which contains a control gate, a floating gate and so on. Data is represented by the number of electrons trapped in the floating gate. There are three basic operations on a cell, program, i.e., to eject electrons into the floating gate, read, i.e., to measure the number of electrons in the floating gate, and erase, i.e., to remove electrons from the floating gate. Each flash chip is composed of blocks, each block consists of pages, and a page is made up of cells. Similarly, there are three operations for a block, i.e., program, read and erase, however, the unit of programming and reading is a page, and the unit of erasing is a block.

There are two challenges in flash memories, one is the well-known *endurance* problem and the other one is the less well-known *insecure deletion* problem. The endurance problem means flash memory can only experience a limited number of program/erase cycles after which its reliability can not be guaranteed. The current code solution for endurance is the rewriting codes, e.g., Write-Once Memories [15], and Write-Efficient Memories (WEM) [1], etc. Recently there is a large amount of work for rewriting code [3], [4], [6], [12], [16] showing the existance of optimal constructions for them and system work [14], [18] showing various benefits rewriting code bringing to flash memories.

Insecure deletion means *Flash Translation Layer* (FTL) produces multiple copies of data that can not be deleted completely as they are either impossible or costly, however, a sophisticated attacker can recover and obtain information about the data.

We illustrate the insecure deletion in detail here. The first reason causing this is the existence of multiple copies of codewords in flash memories. Flash memories are not perfect as there are various errors, thus a strong error correcting code is used to combat errors. *Memory scrubbing* is also used to protect flash memories, which is to correct a noisy codeword and write a new error-free codeword back to memories. However, due to the *out-of-place* rewriting policy, the updated codeword is stored at a new physical address and the original codeword remains in memories. Those mechanisms lead to multiple copies of codewords existing in memories. Other reasons causing this are weal leveling and garbage collection. A recent study by Desnoyers [5] theoretically estimates that on overage $3 \sim 13$ copies of codewords can be generated for one write issued by a user, and the exact number depends on the work load traffic and various algorithms (e.g., garbage collection algorithms) used.

For current flash memory solutions, when to delete data, it is either impossible or costly to delete all copies of codewords corresponding to the data due to the imperfections of the physical erasure process and the FTL [7]. However, when the flash memory is attacked by an eavesdropper, (who is able to trace all copies of codewords corresponding to the same data, and is aware of all encoding and decoding algorithms, thus leading to much stronger decoding ability than the decoder having access to a single codeword [10]), the sensitive information can be leaked. Unfortunately, there is barely no coding solution to solve the insecure deletion for flash memories.

In a recent paper [11], a new coding scheme was proposed, *Secure Write-Efficient Memories*. The significance of secure WEM is two-fold, on the practical side it is the first coding model combating both the endurance and the insecure deletion; on the theoretical side it extends the current research scope of rewriting codes in a similar way as wiretap channel coding [17] extends the channel coding model.

B. Definition of secure WEM

In the secure WEM setting (shown in Figure 1), Alice wishes to store messages in a limited lifetime

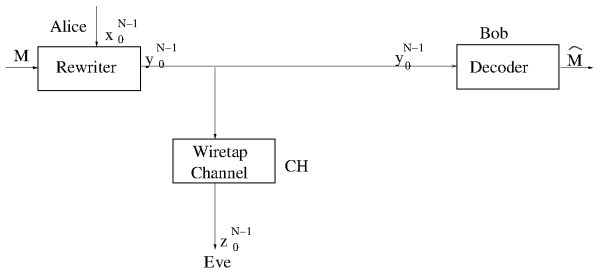

Fig. 1. The secure WEM model. CH is the wiretap channel. $M, x_0^{N-1}, y_0^{N-1}, z_0^{N-1}$ and $\hat{M}$ are the message to rewrite, the current cell states, the rewrite codeword, the wiretap channel's output and the estimated message, respectively.

storage medium using a rewriting code, WEM [1], the messages are accessible to Bob through a storage channel, which is assumed noiseless for simplicity, but her transmissions also reach an eavesdropper Eve through a wiretap channel. Alternatively, let M be the message that Alice wishes to store. Based on the message M and the current N cell state vector x_0^{N-1}, the rewriter maps M to an N-bit codeword y_0^{N-1}. This codeword is transmitted through the noiseless storage channel and the wiretap channel resulting y_0^{N-1} and z_0^{N-1}. The decoder estimates y_0^{N-1} to recover the message M.

The goal of secure WEM codes is to design a rewriting coding scheme such that it is possible to store messages cost-effectively and securely. Being cost-effective means for each rewrite the defined rewriting cost, i.e., which is measured by $\varphi(x_0^{N-1}, y_0^{N-1})$ for a defined cost $\varphi(\cdot)$, has to be less than a predefined number to solve the endurance problem. Being secure means the uncertainty of the eavesdropper about the message M after observing the wiretap channel output z_0^{N-1}, i.e., which is measured by $\frac{1}{N}H(M|z_0^{N-1})$ [17], also satisfies a predefined constraint to solve the insecure deletion problem.

The following notations will be used to define secure WEM. For Alice and Bob, let $\mathcal{X}$ be the alphabet of the symbols stored in a cell, and $\mathcal{Z}$ be that for Eve. $\forall x, y \in \mathcal{X}$, let the *rewriting cost* of changing a cell's level from x to y be $\varphi(x, y)$, which may be time or energy taken. Given N cells and $x_0^{N-1}, y_0^{N-1} \in \mathcal{X}^N$, let $\varphi(x_0^{N-1}, y_0^{N-1}) = \frac{1}{N}\sum_{i=0}^{N-1}\varphi(x_i, y_i)$ be the *average rewriting cost* of changing the N cell levels from x_0^{N-1} to y_0^{N-1}.

Let $\mathcal{D} \subseteq \mathbb{N}$ and it denotes the $|\mathcal{D}|$ possible values of the data stored in the N cells. Let the *decoding function* be $\mathbf{D} : \mathcal{X}^N \to \mathcal{D}$, which maps the N cells' levels to the data they represent. Let the *rewriting function* be $\mathbf{R} : \mathcal{X}^N \times \mathcal{D} \to \mathcal{X}^N$, which changes the N cells' levels to represent the new input data.

We present the definition of secure WEM codes in the following.

Definition 1. An $(N, 2^{NR}, R_e, D)$ secure write-efficient memory code with a wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|X})$ and the rewriting cost function $\varphi(\cdot)$ consists of

- $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$ and its corresponding codewords $\bigcup_{i=0}^{2^{NR}-1}\mathcal{C}_i$, where $\mathcal{C}_i \subseteq \mathcal{X}^N$ is the set of codewords representing data i. We require $\forall i \neq j$, $\mathcal{C}_i \bigcap \mathcal{C}_j = \emptyset$;
- $\mathbf{R}(M, x_0^{N-1})$ such that
  - $\varphi(x_0^{N-1}, \mathbf{R}(M, x_0^{N-1})) \leq D$ for any $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
  - $\frac{1}{N}H(M|z_0^{N-1}) \geq R_e - \epsilon$ for any $M \in \mathcal{D}, z_0^{N-1} \in \mathcal{Z}^n$, $\epsilon > 0$ as $N \to \infty$.
- $\mathbf{D}(y_0^{N-1})$ such that $\mathbf{D}(\mathbf{R}(x_0^{N-1}, M)) = M$ for all $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$.

That is, the first condition indicates that each data is represented by a group of codewords, the first requirement of the rewriting function indicates that during each rewrite the average rewriting cost between the current codeword x_0^{N-1} and the updated codeword y_0^{N-1} is less than a predefined number, the second requirement of the rewriting function indicates that the leaked information of the message at the eavesdropper is limited, and the last one indicates that the decoder knows the rewritting message given a rewriting codeword.

C. Main results of secure WEM [11]

Previous work of [11] introduces us the model of secure WEM, and presents us some information theory results, for which we recap in the following.

The following notations will be used. Let $\mathcal{P}(\mathcal{X} \times \mathcal{X})$ be the set of joint probability distributions over $\mathcal{X} \times \mathcal{X}$. For a pair of random variables $(X, Y) \in (\mathcal{X}, \mathcal{X})$, let $P_{XY}, P_X, P_{X|Y}$ denote the joint probability distribution, the marginal distribution, and the conditional probability distribution, respectively. $E(\cdot)$ denotes the expectation operator. If X is uniformly distributed over $\{0, 1, \cdots, q-1\}$, denote it by $X \sim U(q)$.

Fixed D, $\varphi(\cdot)$ and $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|X})$, $(R, R_e) \in \mathbb{R}^2$ is *achievable* if there exists an $(N, 2^{NR}, R_e, D)$ codes. The set of all achievable tuples is denoted by $\mathcal{R}^{swem}$, *rewriting-rate-equivocation region*. The *secrecy rewriting capacity* is $C^{swem}(D) \stackrel{def}{=} \sup_R\{R : (R, R) \in \mathcal{R}^{swem}\}$, i.e., the maximal R such that (R, R) is achievable.

The $\mathcal{R}^{swem}$ was obtained in [11] and shown in the following theorem:

Theorem [11] 2. Define $\mathcal{R}(P_{XY}) =$

$$\{(R, R_e): \begin{array}{ll} R & \leq H(Y|X) \\ R_e & \leq H(Y|Z) \\ R_e & \leq R \end{array}\},$$

where $P_{XY} \in \mathcal{P}(D) \stackrel{def}{=} \{P_{XY} : P_X = P_Y, E(\varphi(X, Y)) \leq D\}$, the joint distribution of X, Y, Z factorizes as $P_X P_{Y|X} P_{Z|Y}$, and the $P_{Z|Y}$ is given by $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$. Then $\mathcal{R}^{swem} = \bigcup_{P_{XY}} \mathcal{R}(P_{XY})$.

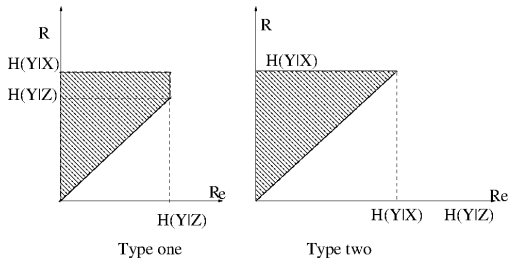

Fig. 2. Typical shape of $\mathcal{R}(P_{XY})$.

The typical shapes of the above achievable region $\mathcal{R}(P_{XY})$ are presented in Figure 11: type one is the case where $H(Y|Z) \leq H(Y|X)$ for a given $P_{XY} \in \mathcal{P}(D)$, and type two is the other case.

By specializing Theorem 2 to the case $R = R_e$, we obtain the following result for secrecy rewriting capacity.

Corollary 3. The secrecy rewriting capacity of secure WEM $(N, 2^{NR}, R_e, D)$ code with wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$ and the rewriting cost function $\varphi(\cdot)$ is:
$C^{swem}(D) = \max_{P_{XY} \in \mathcal{P}(D)} \{\min\{H(Y|X), H(Y|Z)\}\}$,
where the definition of $\mathcal{P}(D)$ is the same as above.

D. Contribution and structure of this paper

In this paper, we present an optimal (i.e., achieve the whole rewriting-rate-equivocation region) code construction based on polar codes for secure WEM for a large family of secure WEM. The remaining of this paper is structured as follows: in Section II, we present a brief introduction of polar codes and some useful terms; in Section III, we present a polar code construction for secure WEM, which achieves the whole region of secure WEM.

II. Polar code terms and notations

In this part, we present a brief introduction to polar codes [2] so that some terms can be understood later.

Let $W = (\mathcal{X}, \mathcal{Y}, W_{Y|X})$ be a binary-input discrete memoryless channel. Let $G_2^{\otimes n}$ be n-th Kronecker product of $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ for $n \in \mathbb{N}$. Let $Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W_{Y|X}(y|0) W_{Y|X}(y|1)}$ be the Bhattacharyya parameter.

Let $N = 2^n$, and the polar code, which is denoted as $C_N(F, u_F)$, is $\{x_0^{N-1} = u_0^{N-1} G_2^{\otimes n} : u_{F^c} \in \{0,1\}^{|F^c|}\}$, where $\forall F \subseteq \{0, 1, \cdots, N-1\}$, u_F is the subvector $u_i : i \in F$, and $u_F \in \{0,1\}^{|F|}$. By convention, F is the *frozen set* and u_F is the *frozen set value*.

Denote $W_N^{(i)} : \{0,1\} \to \mathcal{Y}^N \times \{0,1\}^i$ the i-th *sub-channel* with input set $\{0,1\}$, output set $\mathcal{Y}^N \times \{0,1\}^i$, and the transition probability $W_N^{(i)}(y_0^{N-1}, u_0^{i-1}|u_i) \stackrel{def}{=} \frac{1}{2^{N-1}} \sum_{u_{i+1}^{N-1}} W^N(y_0^{N-1}|u_0^{N-1})$, where $W^N(y_0^{N-1}|u_0^{N-1})$ is $\prod_{i=0}^{N-1} W_{Y|X}(y_i|(u_0^{N-1} G_2^{\otimes n})_i)$, and $(u_0^{N-1} G_2^{\otimes n})_i$ denotes the i-th element of $u_0^{N-1} G_2^{\otimes n}$.

Let $\beta < 1/2$ be a fixed positive constant, define a good sub-channel set as $\mathcal{G}_N(W, \beta) = \{i \in \{0, 1, \cdots, N-1\} : I(W_N^{(i)}) > \frac{1}{N} 2^{-N^\beta}\}$, and define a bad sub-channel set as $\mathcal{B}_N(W, \beta) = \{i \in \{0, 1, \cdots, N-1\} : I(W_N^{(i)}) \leq \frac{1}{N} 2^{-N^\beta}\}$. By abusing notations, we also define a good sub-channel set as $\mathcal{G}'_N(W, \beta) = \{i \in \{0, 1, \cdots, N-1\} : Z(W_N^{(i)}) < 1 - (\frac{1}{N} 2^{-N^\beta})^2\}$ and define a bad sub-channel set as $\mathcal{B}'_N(W, \beta) = \{i \in \{0, 1, \cdots, N-1\} : Z(W_N^{(i)}) \geq 1 - (\frac{1}{N} 2^{-N^\beta})^2\}$.

Based on [9, Lemma 2.6], $\lim_{N\to\infty} \frac{1}{N} |\mathcal{B}_N(W, \beta)| = \lim_{N\to\infty} \frac{1}{N} |\mathcal{B}'_N(W, \beta)| = 1 - I(W)$, and $\lim_{N\to\infty} \frac{1}{N} |\mathcal{G}_N(W, \beta)| = \lim_{N\to\infty} \frac{1}{N} |\mathcal{G}'_N(W, \beta)| = I(W)$.

III. Optimal code construction

In this section, we present a polar code construction for a special case of secure WEM and prove that the code construction achieves the whole achievable region. Due to space limitation, we only present the code constructions for type one rewriting-rate-equivocation region of secure WEM.

A. Symmetric secure WEM

In this subsection, we define symmetric secure WEM, which is a large family of secure WEM, and it is the symmetric secure WEM that our polar code construction is focusing in this paper.

Recall that the rewriting capacity of WEM is $\mathcal{R}(D) = \max_{P_{XY} \in \mathcal{P}(D)} H(Y|X)$ [1]. Analogous to a symmetric channel, a symmetric WEM is such a WEM that its rewriting capacity is achieved when current cell state alphabet (i.e., X) and updated cell state alphabet (i.e., Y) are uniformly distributed. That is, for symmetric WEM its capacity is determined as $\mathcal{R}(D) = \max_{P_{XY} \in \mathcal{P}^s(D)} H(Y|X)$, where $\mathcal{P}^s(D) \stackrel{def}{=} \{P_{XY} : P_X = P_Y, X \sim U(q), E(\varphi(X, Y)) \leq D\}$ and q is the number of states for X.

For a P_{XY} achieving rewriting capacity of a symmetric WEM, it induces a channel $\mathbb{W} = (X, Y, W_{Y|X})$, and we term it WEM *channel*. A symmetric secure WEM is such a secure WEM model that both the WEM and the wiretap channel are symmetric. Further, we consider the case where the WEM channel is *stochastically degraded* with respect to the wiretap channel, i.e., the type one rewriting-rate-equivocation region of secure WEM. Besides, the code construction presented here focuses on symmetric rewriting cost, i.e., $\varphi(0,1) = \varphi(1,0)$, the Hamming distrance metric.

We present a concrete example of symmetric secure WEM we are considering in the following:

Example 1. Let the rewriting cost metric be the Hamming distance metric, i.e., $\varphi(0,1) = \varphi(1,0) = 1$ and $\varphi(0,0) = \varphi(1,1) = 0$, in this case the capacity of symmetric WEM is $H(D)$ where $0 \leq D \leq 1/2$ and the WEM channel induced is a Binary Symmetric Channel (BSC) with parameter D. Let the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$ be a BSC with flipping rate p $(0 \leq p \leq 1/2)$. In this case, the secrecy capacity is $H(p)$ based on Corollary 3. When $D > p$, the WEM channel stochastically degrades with respect to the wiretap channel, and it is one example of symmetric secure WEMs we are focusing in this work.

B. Optimal code construction achieving the capacity

The outline of the code construction is presented in Figure 3: Given the WEM channel and the wiretap channel, we divide all sub-channels to three parts, i.e., sub-channels bad for both channels, the sub-channel index set is denoted as set $\mathcal{M} \subseteq \mathbb{N}$, sub-channels good for both channels, the sub-channel index set is denoted as set $\mathcal{M}_2 \subseteq \mathbb{N}$, and remaining sub-channels, the sub-channel index set is denoted as the set $\mathcal{M}_1 \subseteq \mathbb{N}$.

Then the polar code with frozen set $\mathcal{M}$, and frozen set value $u_{\mathcal{M}}$ represents data $u_{\mathcal{M}}$. The rewriting function $\mathbf{R}(M, x_0^{N-1})$ is to fill in bits of $\mathcal{M}$ by M, bits of $\mathcal{M}_1$ by random bits, and bits of $\mathcal{M}_2$ by bits determined by successive cancellation encoding. The decoding function $\mathbf{D}(y_0^{N-1})$ is to retrieve the value represented by bits of $\mathcal{M}$.

Formally, let $\mathcal{G}'_N(\mathbb{W}, \beta)$ and $\mathcal{G}_N(\mathbb{P}, \beta)$ denote good sub-channel sets for the WEM channel $\mathbb{W}$ and the wiretap channel $\mathbb{P}$, and let $\mathcal{B}'_N(\mathbb{W}, \beta)$ and $\mathcal{B}_N(\mathbb{P}, \beta)$ denote the bad sub-channels for them, respectively. When $\mathbb{W}$ is stochastically degraded with respect to $\mathbb{P}$, it implies that $\mathcal{B}_N(\mathbb{P}, \beta) \subseteq \mathcal{B}'_N(\mathbb{W}, \beta)$ [9]. Let $\mathcal{M} \stackrel{def}{=} \mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{B}_N(\mathbb{P}, \beta) = \mathcal{B}_N(\mathbb{P}, \beta)$, $\mathcal{M}_1 \stackrel{def}{=} \mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{G}_N(\mathbb{P}, \beta)$ and $\mathcal{M}_2 \stackrel{def}{=} \mathcal{G}'_N(\mathbb{W}, \beta)$. We know that $\lim_{N\to\infty} \frac{|\mathcal{M}|}{N} = H(Y|Z)$, $\lim_{N\to\infty} \frac{|\mathcal{M}_1|}{N} = H(Y|X) - H(Y|Z)$ and $\lim_{N\to\infty} \frac{|\mathcal{M}_2|}{N} = I(X;Y)$.

The code construction for binary symmetric secure WEM is presented in Algorithm III.1:

Algorithm III.1 A code construction for binary symmetric secure WEM

1: The $(N, 2^{NR}, R, D)_{ave}$ code is $\mathcal{C} = C_N(\mathcal{M}, u_{\mathcal{M}})$, where $C_N(\mathcal{M}, u_{\mathcal{M}}(M))$ is a polar code with the frozen set $\mathcal{M}$ as above, frozen set value M, the binary representation of M is $u_{\mathcal{M}}(M)$, and $|\mathcal{M}| = NR$.

That is, the $(N, 2^{NR}, R, D)$ code is the *polar code ensemble* of codeword length N and frozen set $\mathcal{M}$ determined above, and each polar code $\mathcal{C}_N(\mathcal{M}, u_{\mathcal{M}}(M))$ $(0 \leq M \leq 2^{NR} - 1)$ of the ensemble represents the data with the binary representation $u_{\mathcal{M}}(M)$.

The rewriting operation $y_0^{N-1} = \mathbf{R}(M, x_0^{N-1})$ is presented in Algorithm III.2, where m_1 is a random bit, $u_{\mathcal{M}}(M)_j$ is the j^{th} bit of the binary representation of M, $f(\cdot) : \{0, 1, ..., |\mathcal{M}| - 1\} \to \mathcal{M}$ is a one-to-one mapping, and $W(y|x)$ is determined by the WEM channel $\mathbb{W} = (X, Y, W_{Y|X})$.

Algorithm III.2 The rewriting operation $y_0^{N-1} = \mathbf{R}(M, x_0^{N-1})$.

1: Let $v_0^{N-1} = x_0^{N-1} + g_0^{N-1}$, where g_0^{N-1} is a common and uniformly distributed message, and $+$ is over GF(2).

2: Apply SC (Successive Cancellation) encoding [9] to $(v_0^{N-1})_{\mathcal{M}_2}$, and this results in a vector $u_0^{N-1} = \hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M))$, that is, $u_j =$
$$\begin{cases} u_{\mathcal{M}}(M)_{f(j)} & \text{if } j \in \mathcal{M} \\ m_1 & \text{if } j \in \mathcal{M}_1,\ m_1 \text{ is randomly chosen,} \\ m & \text{with probability } \frac{W_N^{(i)}(u_0^{j-1}, v_0^{N-1}|m)}{\sum_{m'} W_N^{(i)}(u_0^{j-1}, v_0^{N-1}|m')}, \end{cases}$$
and $\hat{y}_0^{N-1} = u_0^{N-1} G_2^{\otimes n}$.

3: $y_0^{N-1} = \hat{y}_0^{N-1} + g_0^{N-1}$.

That is, u_0^{N-1} is assembled by rewriting message M, auxiliary random message M_1 (which is to make sure the security constraint is satisfied), and random message determined by SC encoding (which is to make sure the rewriting cost constraint is satisfied).

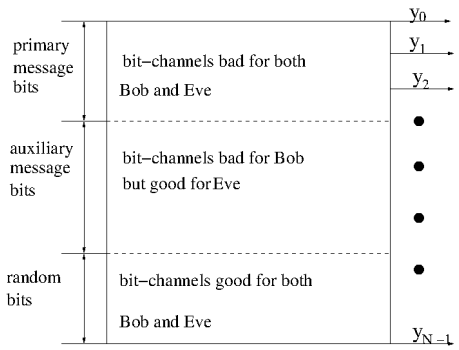

Fig. 3. Illustration of the polar code construction for symmetric secure WEM achieving the capacity, where the output y_0^{N-1} is permuted in such a way that sub-channels are positioned as above.

The decoding function $u_{\mathcal{M}}(M) = \mathbf{D}(y_0^{N-1})$ is presented in Algorithm III.3:

That is, $\mathbf{D}(y_0^{N-1})$ is to retrieve the value represented by bits of $\mathcal{M}$.

C. Theoretical analysis of the code construction

In this part, we present the theoretical analysis showing that the presented code construction is optimal.

Algorithm III.3 The decoding operation $u_{\mathcal{M}}(M) = \mathbf{D}(y_0^{N-1})$.

1: $\hat{y}_0^{N-1} = y_0^{N-1} + g_0^{N-1}$.
2: $u_{\mathcal{M}}(M) = (\hat{y}_0^{N-1}(G_2^{\otimes n})^{-1})_{\mathcal{M}}$.

We start with calculating the probability of a random selected vector in part a), which is used to prove that the induced *channel* is symmetric in part b), then with the symmetric channel we proceed to prove the rewriting cost constraint as well as the security constraint are satisified in part c), the capacity approaching property is proved in part d), and the theoretical performance of the proposed code construction is concluded in part e).

a) The probability of a random selected vector: Let $\mathcal{R} = \mathcal{M}_1 \bigcup \mathcal{M}_2$, and let $e_{\mathcal{R}}$ denote the random bits determined by the above algorithm. In this part we focus on the average probability $e_{\mathcal{R}}$ is selected given the rewriting data M, $P(e_{\mathcal{R}|M})$ (over v_0^{N-1}), and we show that $P(e_{\mathcal{R}|M})$ is independent of M.

Let e_0^{N-1} denote a vector by assembling a rewriting message M and $e_{\mathcal{R}}$, and we know that

$$P(e_0^{N-1}|v_0^{N-1}) = \prod_i P_{E_i|E_0^{i-1},V_0^{N-1}}(e_i|e_0^{i-1}, v_0^{N-1}),$$

where v_0^{N-1} is the random vector determined in our rewriting function, and $P_{E_i|E_0^{i-1},V_0^{N-1}}(e_i|e_0^{i-1}, v_0^{N-1}) = \frac{W_N^{(i)}(e_0^{i-1}, v_0^{N-1}|e_i)}{\sum_{e_i'} W_N^{(i)}(e_0^{i-1}, v_0^{N-1}|e_i')}$ if $i \in \mathcal{M}_2$, $\frac{1}{2}$ if $i \in \mathcal{M}_1$ and 1 otherwise.

The following lemma presents us the condition under which $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_{\mathcal{M}^c} = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))_{\mathcal{M}^c}$, i.e., the random bits determined by the algorithm are the same.

Lemma 4. Let $M_1, M_2 \in \{0, \cdots, 2^{|\mathcal{M}|-1}\}$, $u_{\mathcal{M}}(M_1), u_{\mathcal{M}}(M_2) \in \{0,1\}^{|\mathcal{M}|}$, let $v_0^{N-1}, w_0^{N-1} \in \{0,1\}^N$ such that $v_0^{N-1} + w_0^{N-1} = x_0^{N-1}G_2^{\otimes n}$ where $(x_0^{N-1})_{\mathcal{M}} = u_{\mathcal{M}}(M_1) + u_{\mathcal{M}}(M_2)$ and $(x_0^{N-1})_{\mathcal{M}^c}$ is the zero vector, then under the coupling through a common source of randomness, $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_{\mathcal{M}^c} = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))_{\mathcal{M}^c}$.

Proof: Let e_0^{N-1} and f_0^{N-1} be the result of $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))$ and $\hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))$. We prove that $e_i = f_i + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_i$ for $0 \le i \le N-1$ by induction. This holds true for $i = 0$.

Now suppose this also holds true for $i-1$, and now consider the case for i. As $e_i = f_i + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_i$ holds true for the case when $i \in \mathcal{M}$, we only consider the other case when $i \in \mathcal{M}^c$.

Firstly consider $i \in \mathcal{M}_1$, since they have access to the same random source, clearly $e_i = f_i + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_i$.

Secondly consider $i \in \mathcal{M}_2$, and it is proved using a skill similar to [9, Lemma 3.12] as shown in equation 1.

Thus $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_i = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))_i$ when they have access to the same random source. Thus we conclude $e_i = f_i + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_i$, and $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_{\mathcal{M}^c} = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))_{\mathcal{M}^c}$. ∎

Let $P(e_{\mathcal{R}}|M)$ denote the average probability (over v_0^{N-1}) that $e_{\mathcal{R}}$ is chosen given M, and $P(e_{\mathcal{R}}|M) = \sum_{v_0^{N-1}} P(v_0^{N-1})P(e_0^{N-1}|v_0^{N-1}) = \sum_{v_0^{N-1}} \frac{1}{2^N} P(e_0^{N-1}|v_0^{N-1})$, as v_0^{N-1} is uniformly distributed.

The next theorem shows on average the probability that $e_{\mathcal{R}}$ is chosen given M is the same for any M.

Theorem 5. $P(e_{\mathcal{R}}|M)$ is independent of M, i.e., $P(e_{\mathcal{R}}|M_1) = P(e_{\mathcal{R}}|M_2)$ for any M_1, M_2.

Proof: The correctness holds by the fact that for each v_0^{N-1} there is a unique w_0^{N-1} such that $e_{\mathcal{R}} = \hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_{\mathcal{M}^c} = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))_{\mathcal{M}^c}$ based on the previous lemma. ∎

As $P(e_{\mathcal{R}}|M)$ is independent of M, hereafter we will omit M and write $P(e_{\mathcal{R}}|M)$ as $P(e_{\mathcal{R}})$.

b) The induced channel is symmetric: The induced channel is presented in Figure 4, where the input is $N-r$ bits $u_{\mathcal{M}}$, representing the rewriting data, and the output of the channel is z_0^{N-1}, the output of y_0^{N-1} through the wiretap channel. Let (v_0^{N-r-1}, e_0^{r-1}) denote the vector u_0^{N-1} with $u_{\mathcal{R}} = v_0^{N-r-1}$ and $u_{\mathcal{R}^c} = e_0^{r-1}$, i.e., assemblng the rewriting data v_0^{N-r-1} and the random information e_0^{r-1} .

For this channel its channel transition probability is denoted as $\mathcal{Q}(z_0^{N-1}|u_0^{N-r-1})$, which is

$$\sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_{i=0}^{N-1} P(z_i|((u_0^{N-r-1}, e_0^{r-1})G_2^{\otimes n})_i),$$

where $P(e_0^{r-1})$ denotes the probability e_0^{r-1} is selected given the rewriting data vector u_0^{N-r-1} (its value is determined as the previous part), and $P(z|x)$ is determined by the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|X})$. For convenience, we denote our channel as $\mathbb{Q}(\mathbb{P}, \mathcal{R}) = (\mathcal{X}^{N-r}, \mathcal{Z}^N, \mathcal{Q}_{Z^N|U^{N-r}})$. where $\mathcal{X} = \{0,1\}$.

We now present the main result in the following theorem, which presents us $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ is symmetric.

Theorem 6. $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ *is symmetric.*

Proof: Given a channel $(\mathcal{X}, \mathcal{Y}, W_{Y|X})$, we first recall the definition of symmetric channel from group theory. *A group action* of an abelian group $\mathcal{A}$ on a set $\mathscr{Y}$ is a function $\mathcal{A} \times \mathscr{Y} \to \mathscr{Y}$, denoted $(a, y) \to a \cdot y$, with the following properties:

- $0 \cdot y = y$ for all $y \in \mathscr{Y}$, where 0 is the unit of $\mathcal{A}$;
- $(a+b) \cdot y = a \cdot (b \cdot y)$ for all $a, b \in \mathcal{A}$ and all $y \in \mathscr{Y}$, where $+$ denotes the group operation for $\mathcal{A}$.

The following result from [13, Theorem 11] states a necessary condition such that the channel is symmetric.

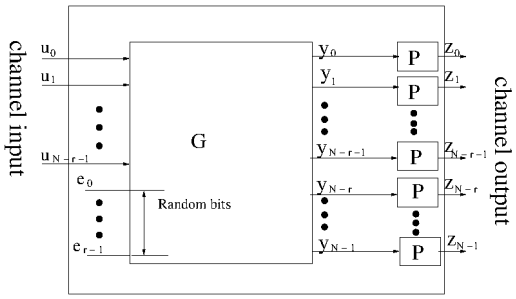

Fig. 4. Illustration of the induced channel, where the output y_0^{N-1} is permuted the same way as before such that sub-channels are positioned as the above figure; and where the channel inputs are u_0^{N-r-1} (i.e., rewriting data) and the channel outputs are z_0^{N-1} (i.e., noisy codeword of y_0^{N-1} though wiretap channel).

> Let $(\mathcal{X}, \mathcal{Y}, W_{Y|X})$ be a discrete memoryless channel, and suppose that $\mathcal{X}$ is an abelian group under the binary operation $+$. Further, suppose that there exists a group action $\cdot$ of $\mathcal{X}$ on $\mathcal{Y}$ such that
> $$W(y|a+x) = W(a.y|x)$$
> for all $a, x \in \mathcal{X}$ and all $y \in \mathcal{Y}$. Then $(\mathcal{X}, \mathcal{Y}, W_{Y|X})$ is a symmetric channel.

For $\mathbb{Q}(\mathbb{P}, \mathcal{R}) = (\mathcal{X}^{N-r}, \mathcal{Z}^N, \mathcal{Q}_{Z^N|U^{N-r}})$, we first explore an action of $\mathcal{X}^{N-r}$, denoted as $\cdot$, such that $(\mathcal{X}^{N-r}, \cdot)$ is an abelian group, and we then explore a group action, denoted as $\circ$ of the abelian group $\mathcal{X}^{N-r}$ on $\mathcal{Z}^N$, such that $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ is symmetrical based on the above cited result. We first explore the operation of $\cdot$ in the following two paragraphs: Let π_1 be a permutation on $\mathcal{Z}$ and it is an involution, that is $\pi_1 = \pi_1^{-1}$. Let π_0 be the identity permutation on $\mathcal{Z}$. Following Arikan [2], let the group action of the additive group of $\mathcal{X} = \{0, 1\}$ on the set $\mathcal{Z}$ be $x \cdot z = \pi_x(z)$ for all $x \in \mathcal{X}$ and $z \in \mathcal{Z}$. The group action has the property $(x+y) \cdot z = x \cdot (y \cdot z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ which can be verified based on enumeration. Therefore, the additive group $\mathcal{X}$ with the operation $\cdot$ is an abelian group.

Similarly, let $x_0^{N-1} \cdot z_0^{N-1} = (x_0 \cdot z_0, \cdots, x_{N-1} \cdot z_{N-1})$ for all $x_0^{N-1} \in \mathcal{X}^N$ and $z_0^{N-1} \in \mathcal{Z}^N$. The action has the following two properties

- $(x_0^{N-1} + y_0^{N-1}) \cdot z_0^{N-1} = x_0^{N-1} \cdot (y_0^{N-1} \cdot z_0^{N-1})$;
- $(x_0^{N-1} \cdot y_0^{N-1}) \cdot z_0^{N-1} = x_0^{N-1} \cdot (y_0^{N-1} \cdot z_0^{N-1})$,

where the first one is based on the property $(x+y) \cdot z = x \cdot (y \cdot z)$, and the second one is based on the property $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Therefore, the additive group $\mathcal{X}^N$ with the operation $\cdot$ is an abelian group.

We then explore the operation of $\circ$ in the following: Define $\circ$ as $x_0^{N-r-1} \circ z_0^{N-1} \stackrel{def}{=} (x_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot z_0^{N-1}$. We can verify that the defined action is a *group action* as it satisfies the following two requirements:

- $0_0^{N-r-1} \circ z_0^{N-1} = z_0^{N-1}$;
- $(x_0^{N-r-1} + y_0^{N-r-1}) \circ z_0^{N-1} = x_0^{N-r-1} \circ (y_0^{N-r-1} \circ z_0^{N-1})$,

where the correctness of the second item is shown in equation 2.

We finish the proof by showing that $\mathcal{Q}(z_0^{N-1}|a_0^{N-r-1} + x_0^{N-r-1}) = \mathcal{Q}(a_0^{N-r} \circ z_0^{N-1}|x_0^{N-r-1})$ as shown in equations $3 \sim 5$: ∎

c) Rewriting cost constraint and security constraint: We first focus on the rewriting cost constraint. From [12, Theorem 9], we know that as long as $\mathcal{M}_2 \subseteq \mathcal{G}'_N(\mathbb{W}, \beta)$, with high probability $\varphi(x_0^{N-1}, y_0^{N-1}) \leq D$

$$\begin{aligned}
\frac{W_N^{(i)}(v_0^{N-1}, e_0^{i-1}|1)}{W_N^{(i)}(v_0^{N-1}, e_0^{i-1}|0)} &= \frac{\sum_{e_{i+1}^{N-1}} W^N(v_0^{N-1}|e_0^{i-1}1e_{i+1}^{N-1})}{\sum_{e_{i+1}^{N-1}} W^N(v_0^{N-1}|e_0^{i-1}0e_{i+1}^{N-1})}, \\
&= \frac{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|e_0^{i-1}1e_{i+1}^{N-1} + (v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})}{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|e_0^{i-1}0e_{i+1}^{N-1} + (v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})}, \\
&= \frac{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|f_0^{i-1}1e_{i+1}^{N-1})}{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|f_0^{i-1}0e_{i+1}^{N-1})}, \\
&= \frac{W_N^{(i)}(w_0^{N-1}, f_0^{i-1}|1)}{W_N^{(i)}(w_0^{N-1}, f_0^{i-1}|0)}, \qquad (1)
\end{aligned}$$

where the third equation is due to the assumption that $((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_{\mathcal{M}^c}$ is the zero vector and the assumption $e_j = f_j + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_j$ for $j \leq i-1$.

for arbitrary x_0^{N-1}, y_0^{N-1}, i.e., $Pr(\varphi(x_0^{N-1}, y_0^{N-1}) \geq D + \sigma) < 2^{-N^\beta}$ for $\sigma > 0$. Therefore based on our selection of $\mathcal{M}_2$, which is $\mathcal{M}_2 = \mathcal{G}'_N(\mathbb{W}, \beta)$, the rewriting cost constraint is satisfied with high probability.

We next focus on the security constraint, and we apply a skill similar to [13].

$$\begin{aligned} I(M; z_0^{N-1}) & \\ &\leq I(\hat{u}_M; \hat{z}_0^{N-1}), && (6)\\ &= I(\bar{u}_M; \bar{z}_0^{N-1}), && (7)\\ &= \sum_{i=0}^{|\mathcal{M}|} I(\bar{u}_i; \bar{z}_0^{N-1} | \bar{u}_0, \cdots, \bar{u}_{i-1}), && (8)\\ &= \sum_{i=0}^{|\mathcal{M}|} I(\bar{u}_i; \bar{z}_0^{N-1} \bar{u}_0^{i-1}), && (9)\\ &= \sum_{i=0}^{|\mathcal{M}|} C(\mathbb{P}_N^{(i)}), && (10) \end{aligned}$$

where

(6) follows from the channel $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ is symmetric, and $\hat{u}_M$ and $\hat{z}_0^{N-1}$ denote versions of u_M and z_0^{N-1} when u_i and z_i are uniformly and independently distributed;

(7) is due to the permutation such that u_0^{N-1} is arranged as Figure 3;

(8) is due to the chain rule of mutual information;

(9) is due to $\bar{u}_i$ is independent of each other;

(10) is due to $\mathbb{P}_N^{(i)}$ is i-th virtual bit channel induced by the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$ (refer to Section II for its definition).

Based on our selection of $\mathcal{M}$, which is $\mathcal{B}_N(\mathbb{P}, \beta)$, we know that $C(\mathbb{P}_N^{(i)}) \leq 2^{-N^\beta}$ and further obtain $\frac{I(M; z_0^{N-1})}{N} \leq \frac{|\mathcal{B}_N(\mathbb{P}, \beta)|}{N} 2^{-N^\beta}$, which is approaching 0 as $N \to \infty$.

Therefore, we can conclude that the security constraint is satisfied since $\frac{1}{N} H(M | z_0^{N-1}) = \frac{1}{N} H(M) - \frac{1}{N} I(M; z_0^{N-1}) \to R$ as $N \to \infty$.

d) Capacity approaching property: When the WEM channel is stochastically degraded with respect to the wiretap channel, the secrecy capacity is $H(Y|Z)$ as shown by Corollary 3. Based on our code construction we know that $\lim_{N \to \infty} \frac{|\mathcal{M}|}{N} = H(Y|Z)$, thus the construction is achieving the secrecy capacity asymptotically.

e) Theoretical performance conclusion: Thus based on analysis from $a) \sim d)$, we have the following conclusion for theoretical performance of our proposed code construction:

Theorem 7. For any symmetric secure WEM, when the WEM channel is stochastically degraded with respect to the wiretap channel, the proposed polar code scheme achieves the secrecy capacity.

D. Optimal code construction achieving the whole region

In this subsection, we extend the above code construction to achieve the whole rewriting-rate-equivocation region.

$$\begin{aligned} (x_0^{N-r-1} + y_0^{N-r-1}) \circ z_0^{N-1} &= ((x_0^{N-r-1}, 0_0^{r-1}) + (y_0^{N-r-1}, 0_0^{r-1})) G_2^{\otimes n} \cdot z_0^{N-1} \\ &= (x_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot ((y_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot z_0^{N-1}) \\ &= x_0^{N-r-1} \circ (y_0^{N-r-1} \circ z_0^{N-1}), \end{aligned} \quad (2)$$

where the second equation is based on the property $(x_0^{N-1} + y_0^{N-1}) \cdot z_0^{N-1} = x_0^{N-1} \cdot (y_0^{N-1} \cdot z_0^{N-1})$.

$$\begin{aligned} \mathcal{Q}(z_0^{N-1} | a_0^{N-r-1} + x_0^{N-r-1}) &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P(z_0^{N-1} | (((a_0^{N-r-1}, 0_0^{r-1}) + (x_0^{N-r-1}, e_0^{r-1})) G_2^{\otimes n}))_i, && (3)\\ &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P((a_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot z_0^{N-1} | (x_0^{N-r-1}, e_0^{r-1}) G_2^{\otimes n}))_i, && (4)\\ &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P(a_0^{N-r-1} \circ z_0^{N-1} | (x_0^{N-r-1}, e_0^{r-1}) G_2^{\otimes n}))_i, && (5)\\ &= \mathcal{Q}(a_0^{N-r} \circ z_0^{N-1} | x_0^{N-r-1}), \end{aligned}$$

where

(3) follows from the definition of $\mathcal{Q}(z_0^{N-1} | u_0^{N-r-1})$;

(4) follows from [2, Proposition 12]. i.e., $P^N(z_0^{N-1} | (a_0^{N-1} + x_0^{N-1}) G_2^{\otimes n}) = P^N(a_0^{N-1} G_2^{\otimes n} \cdot z_0^{N-1} | x_0^{N-1} G_2^{\otimes n})$ and $P^N(z_0^{N-1} | x_0^{N-1}) = \prod_{i=0}^{N-1} P(z_i | x_i)$;

(5) follows from our definition of the operation $\circ$, and also from Theorem 5.

Given a $\forall(R, R_e) \in$

$$\{(R, R_e): \begin{array}{ll} R & \leq H(Y|X) \\ R_e & \leq H(Y|Z) \\ R_e & \leq R \\ H(Y|Z) & \leq H(Y|X) \end{array}\}, \quad (11)$$

for a $P_{XY} \in \mathcal{P}^s(D)$, we know that based on the code construction in the previous subsection, we can construct a code construction for $(N, 2^{NR_e}, R_e, D)$ symmetric secure WEM, and partition the set $\{0, 1, \cdots, N-1\}$ into $\mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{B}_N(\mathbb{P}, \beta) = \mathcal{B}_N(\mathbb{P}, \beta)$, $\mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{G}_N(\mathbb{P}, \beta)$ and $\mathcal{G}'_N(\mathbb{W}$. We know that $R_e = \frac{|\mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{B}_N(\mathbb{P}, \beta)|}{N}$. Our code construction for an $(N, 2^{NR}, R_e, D)$ symmetric secure WEM is as follows:

- let $\mathcal{M}^1 = \mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{B}_N(\mathbb{P}, \beta)$ of size NR_e;
- let $\mathcal{M}^2 \subseteq \mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{G}_N(\mathbb{P}, \beta)$ of size $N(R - R_e)$ whose elements have lowest $I(\mathbb{W}_N^{(i)})$;
- let $\mathcal{M} = \mathcal{M}^1 \bigcup \mathcal{M}^2$;
- let $\mathcal{M}_1 = \mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{G}_N(\mathbb{P}, \beta) - \mathcal{M}^2$;
- let $\mathcal{M}_2 = \mathcal{G}'_N(\mathbb{W}, \beta)$;
- the $(N, 2^{NR}, R_e, D)_{ave}$ code is $\mathcal{C} = \bigcup_M C_N(\mathcal{M}, u_{\mathcal{M}}(M))$, where $C_N(\mathcal{M}, u_{\mathcal{M}}(M))$ is a polar code with the frozen set $\mathcal{M}$ and frozen set value M with its binary representation $u_{\mathcal{M}}(M)$.

That is, comparing with the previous code construction, the only difference is that bits of $\mathcal{B}'_N(\mathbb{W}, \beta) \bigcap \mathcal{G}_N(\mathbb{P}, \beta)$ in this case also represent user information, i.e., in Figure 3, some auxiliary message bits carry information.

The rewriting function and the decoding function are the same as previous ones. We conclude its performance in the following theorem.

Theorem 8. For any symmetric secure WEM code (R, R_e) satisfying (11), when the WEM channel is stochastically degraded with respect to the wiretap channel, there exists a polar code achieving the whole region.

Proof: We present the sketch proof as follows. We first focus on the rewriting cost constraint: since $\mathcal{M}_2 \subseteq \mathcal{G}'_N(\mathbb{W}, \beta)$ (the same as the previous subsection), similarly based on [12, Lemma 7] or [8, Theorem 1] we obtain the average rewriting cost $\bar{D} \leq D + O(2^{-N^\beta})$.

Next we focus on the security constraint: with similar arguments of $a) \sim c)$ of the previous subsection, we can prove that the channel $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ is still symmetric in this case; similarly, we obtain

$$\begin{aligned} I(M; z_0^{N-1}) & \\ &\leq \sum_{i=0}^{|\mathcal{M}^1 \bigcup \mathcal{M}^2|} C(\mathbb{P}_N^{(i)}), && (12) \\ &\leq \sum_{i=0}^{|\mathcal{M}^2|} C(\mathbb{P}_N^{(i)}) + \frac{|\mathcal{B}_N(\mathbb{P}, \beta)|}{N} 2^{-N^\beta}, && (13) \\ &\leq N(R - R_e) + \epsilon, && (14) \end{aligned}$$

where

(12) follows from the similar arguments of d) in the previous subsection;

(13) is due to the selection of $\mathcal{M}^1$ and the definition of $\mathcal{B}_N(\mathbb{P}, \beta)$;

(14) is due to the selection of $\mathcal{M}^2$ and the definition of $\mathcal{G}_N(\mathbb{P}, \beta)$.

Thus we further obtain $\frac{1}{N} H(M|z_0^{N-1}) \geq R_e + \epsilon$ as desired. ∎

REFERENCES

[1] R. Ahlswede and Z. Zhang, "Coding for write-efficient memory," *Information and Computation*, vol. 83, no. 1, pp. 80–97, October 1989.

[2] E. Arikan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[3] A. Bhatia, M. Qin, A. Iyengar, B. Kurkoski, and P. H. Siegel, "Lattice-based WOM codes for multievel flash memories," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 5, pp. 939–945, May 2014.

[4] D. Burshtein and A. Strugatski, "Polar Write Once Memory Codes," *IEEE Transacation on Information Theory*, vol. 59, no. 8, pp. 5088–5101, August 2013.

[5] P. Desnoyers, "Analytic modeling of ssd write performance," in *International Systems and Storage conference (SYSTOR 2012)*, June 2012.

[6] E. E. Gad, W. Huang, Y. Li, and J. Bruck, "Rewriting flash memories by message passing," in *Proc. IEEE International Symposium on Information Theory(ISIT)*, Hongkong, June 2015.

[7] S. C. Joel Reardon and D. Basin, "SoK: Secure Data Deletion," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.

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

[9] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, EPFL, 2010.

[10] Q. Li, H. Chang, A. Jiang, and E. F. Haratsch, "Joint Decoder of Content-Replication Codes for NAND Flash Memories," in *Proc. 53rd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, CA, October 2015.

[11] Q. Li and A. Jiang, "Coding for secure write-efficient memories," in *Proc. 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton 2014)*, Monticello, IL, October 2014, pp. 505–512.

[12] ——, "Polar codes are optimal for Write-efficient Memories," in *Proc. 51st Annual Allerton Conference on Communication, Control and Computing (Allerton 2013)*, Monticello, IL, October 2013, pp. 660–667.

[13] H. Mahdavifar and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, October 2011.

[14] S. Odeh and Y. Cassuto, "NAND Flash Architectures Reducing Writes Amplification Through Multi-Write Codes," in *IEEE 30th Symposium on Mass Storage Systems on Technologies (MSST)*, 2014.

[15] R. L. Rivest and A. Shamir, "How to reuse a write-once memory," *Informaton and Control*, vol. 55, pp. 1–19, 1982.

[16] K. Santhosh, V. Avinash, N. Krishna, and P. Henry, "Spatially-coupled codes for write-once memories," in *Proc. 53rd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, CA, October 2015.

[17] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, January 1975.

[18] G. Yadgar, E. Yaakobi, and A. Schuster, "Write Once, Get 50% Free, Saving SSD Erase Costs Using WOM Codes," in *Proceedings of the 10th USENIX conference on File and Storage Technologies (FAST'15)*, 2015, pp. 257–271.