Coding for Secure Write-Efficient Memories

Qing Li, *Student Member, IEEE*, and Anxiao (Andrew) Jiang, *Senior Member, IEEE*

***Abstract*— Non-volatile memories suffer from two challenges due to their physical and system-level constraints. One challenge is limited memory lifetime, also called the endurance problem. The other is the difficulty in deleting data securely, called the insecure deletion problem. This paper proposes a coding scheme that addresses both challenges jointly. It studies the secure write-efficient memory (WEM) by analyzing its rewriting-rate equivocation region and secrecy rewriting capacity. It also presents an optimal code construction for a large family of secure WEM channels.**

***Index Terms*— Non-volatile memories, endurance, security, write-efficient memories, wire-tap channel, rewriting-rate-equivocation region, secrecy rewriting capacity, polar codes.**

I. Introduction

NON-VOLATILE memories are becoming ubiquitous due to advantages such as high data density, scaling size, and non-volatility. The two most conspicuous challenges for them are the limited lifetime, i.e., the so-called *endurance* problem, and the difficulty of secure deletion, i.e., the so-called *insecure deletion* problem. Such characteristics are different from traditional storage media, and posing a threat to their further usages. In this work, we propose a novel coding model, secure Write-Efficient Memory (WEM), to address the two challenges jointly, and focus on both information theoretical results, i.e., rewriting-rate-equivocation region and its secrecy rewriting capacity, and coding theory results, i.e., an optimal code construction for a large family of secure WEM, in this paper.

In the following, we present the two challenges in detail (i.e., endurance and insecure deletion), which motivate us to propose the secure WEM model to solve them jointly.

A. Endurance and Rewriting Codes

The first challenge in non-volatile memories is *endurance*. Endurance means non-volatile memory can only experience a limited number of writes due to its physical characteristics, beyond which the memory quality degradation can no longer be accommodated by the memory system.

In the following, we first introduce two types of non-volatile memories, i.e., Phase Change Memories (PCM), and Resistive Random-Access Memories (RRAM). They all have attracted significant research interest due to their scalability, compactness, and simplicity. However, they all suffer from the endurance problem.

A PCM [28] cell is made up of two metal electrodes separated by a resistive heater and a chalcogenide material, the phase change material. The two common states are the crystalline state, which is the Low Resistance State (LRS), and the amorphous state, which is the High Resistance State (HRS).

There are three operations on a PCM cell: read, write (RESET) and erasure (SET). The read operation is to precharge a read voltage on the cell, and measure the resistance. The RESET operation changes the cell state to amorphous. The SET operation changes the cell to crystalline.

PCM has attracted research interest [23], [44] due to its superior resistance ratio, scalability, low-energy switching, and high-speed. Its write endurance ranges from 10^4 to 10^9 SET/RESET cycles, however, because writes induce thermal expansion and contraction within the cell, this degrades injection contacts and limits endurance to hundreds of millions of writes per cell at current processes. These limitations prevent PCM from replacing DRAM in main memory.

Similar to PCM, an RRAM [4] cell can be in three resistance states: virgin-state, on-state (LRS), and off-state (HRS). The virgin state can be *irreversibly* activated by the *forming* operation, while the switching between LRS and HRS is *reversible*, where the changing from LRS to HRS is the RESET, and the reverse operation is the SET operation.

Endurance is still one serious challenge for RRAM, and the limit is around 10^4 writes [4]. It is shown by various electrical tests that its endurance degrades due to lowering resistance in the HRS attributed to the accumulation of defects and the difficulty to RESET from LRS as we cycle the device repeatedly.

Rewriting code is a technique to solve the endurance problem from the coding theory perspective. Fig. 1 presents the rewriting code model, where the rewriter selects a new codeword $y_0^{N-1} = (y_0, y_1, \cdots, y_{N-1})$ based on the message – which is M– to rewrite to the underlying storage medium, and the current cell state of the storage medium $x_0^{N-1} = (x_0, x_1, \cdots, x_{N-1})$ such that a predefined constraint between x_0^{N-1} and y_0^{N-1} is always satisfied.

Based on various constraints, different rewriting code models [27] such as write-once memory (WOM) codes [11], [16], [17], [38], WEM codes [1], and Floating

Manuscript received December 11, 2015; revised July 7, 2016; accepted November 21, 2016. Date of publication December 1, 2016; date of current version January 18, 2017. This work was presented at the 2014 52nd Annual Allerton Conference on Communication, Control and Computing and the 2015 53rd Annual Allerton Conference on Communication, Control and Computing.

Q. Li was with the Department of Computer Science and Engineering, Texas A&M University, College Station, TX 77843 USA. He is now with ScaleFlux, San Jose, CA 95112 USA (e-mail: qingli@cse.tamu.edu).

A. Jiang is with the Department of Computer Science and Engineering and the Department of Electrical and Computing Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: ajiang@cse.tamu.edu).

Communicated by M. Schwartz, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2016.2634553

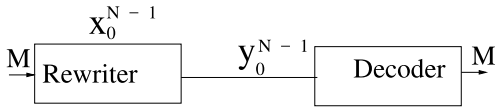

Fig. 1. Rewriting code model, where M is the message to rewrite, x_0^{N-1} is the current cell state, and y_0^{N-1} is the rewrite codeword.

codes [22] etc, have been proposed, and optimal code constructions [8], [29], [41], [42] have been shown. For WOM, the constraint is $y_i \geq x_i$ for $i = 0, 1, \cdots, N-1$, that is, the cell level can only increase but not decrease.

We repeat the definition of WEM as follows, before which we present some notations.

Let $\mathcal{X}$ be the alphabet of the symbol stored in a cell. $\forall x, y \in \mathcal{X}$, 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 rewriting cost of changing the N cell levels from x_0^{N-1} to y_0^{N-1}. Here we abuse the same notation $\varphi(\cdot)$ to denote both the rewriting costs of two cells and two sets of N cells, and the exact meaning can be obtained based on the context.

Let $\mathcal{D} \subseteq \mathbb{N}$ denote 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 $\mathbf{R} : \mathcal{D} \times \mathcal{X}^N \to \mathcal{X}^N$, which changes the N cells' levels to represent the new input data.

Definition 1: [1] An (N, L, D) write-efficient memory code consists of

- $\mathcal{D} = \{0, 1, \cdots, L-1\}$ and $\bigcup_{i=0}^{L-1} \mathcal{C}_i$, where $\mathcal{C}_i \subseteq \mathcal{X}^N$ is the set of codewords representing data i. We require $\forall i \neq j$, $\mathcal{C}_i \bigcap \mathcal{C}_j = \emptyset$;
- A rewriting function $\mathbf{R}(i, x_0^{N-1})$ such that $\varphi(x_0^{N-1}, \mathbf{R}(i, x_0^{N-1})) \leq D$ for any $i \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
- A decoding function $\mathbf{D}(y_0^{N-1})$ such that $\mathbf{D}(\mathbf{R}(i, x_0^{N-1})) = i$ for any $i \in \mathcal{D}$.

That is, the constraint is for each rewrite the rewriting cost of changing the current cell state x_0^{N-1} to the rewrite codeword y_0^{N-1} has to be no more than a predefined constraint. Note that another WEM model with an average rewrite cost constraint is also presented in [1]. We present a concrete example of WEM in Fig. 2.

WEM code can be used to solve the endurance issue in both PCM and RRAM by appropriately modelling the costs of RESET and SET operations [20], [21], [26]. For example, Jacobvitz et al. proposed coset coding [20], [21] to extend the PCM lifetime by reducing the number of bits flipped during the lifetime of the memory, which is essentially a variant of WEM with the Hamming distance metric.

B. Insecure Deletion and Wiretap Codes

The second challenge for non-volatile memories is *insecure deletion* (or *insecure erasure*) ([35], [37], [45]). Insecure deletion means data manager systems produce multiple copies

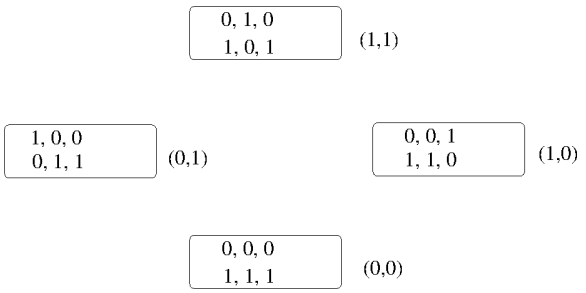

Fig. 2. An example of (3, 4, 1) WEM. Two sequences of numbers inside a box are codewords, and the number outside a box is the data represented by the codewords inside the box. For example, both codewords (0, 0, 0) and (1, 1, 1) represent data (0, 0). The rewriting cost metric is the Hamming distance, that is, $\varphi(0, 0) = \varphi(1, 1) = 0$ and $\varphi(0, 1) = \varphi(1, 0) = 1$.

of data that can not be deleted completely; however, a sophisticated attacker can recover and obtain information about the data.

Note that this issue is caused not by the physical characteristics of the underlying storage media but by the top layer system management schemes, which employ *out-of-place updating*. Such schemes are actually quite common in the system and application level: 1) Log-Structured File system (LSF) [39], which was proposed originally for hard disks, and now is widely used in non-volatile memory systems [5]. One of its goals is to reduce hard disk seek and rotation time by only allowing sequential writes on the hard disk and replacing in-place updates with out-of-place updates. LSF also employs the logical-to-physical mapping table and garbage collection; 2) Log-structured merge (LSM) [40] tree based databases, which are inspired by LSF, and widely used, e.g., BigTable at Google, Cassrandra at Facebook, and Dynamo at Amazon, etc.

The out-of-place updating scheme leads to the existence of multiple copies of codewords in the storage system. The ratio between the number of codewords in physical memories and the number of logical codewords issued by hosts is defined as *write amplification*. Write amplification depends on many factors, such as mapping table granularity, garbage collection algorithms and the workload traffic, etc. There are a large number of research works estimating the value of write amplification such as [15], [47], and [32]. For example, a recent study by Desnoyers [15] theoretically estimates that in certain scenario (i.e., with the so called greedy garbage collection algorithms, page mapping and uniform workload) the write amplification can be as high as $3 \sim 13$, and this number is further confirmed by another research [47].

The out-of-place updating scheme leads to two disadvantages: 1) the secure data deletion problem as shown by Reardon [36] "neither of these systems (log-structured file systems) provide temporal data deletion guarantees and that deleted data remains indefinitely on these systems if the storage medium is not used after the data is marked for deletion"; 2) a much stronger decoder who has access to redundant copies of codewords [31], [43].

We use the example in Fig. 3 to illustrate the secure deletion problem. Let $\mathcal{X}, \mathcal{Z}$ be two alphabets of the symbol stored in a cell, M be sensitive data stored at a logical address LA_0, $y_0^{N-1} \in \mathcal{X}^N$ be its codeword (which may not be a

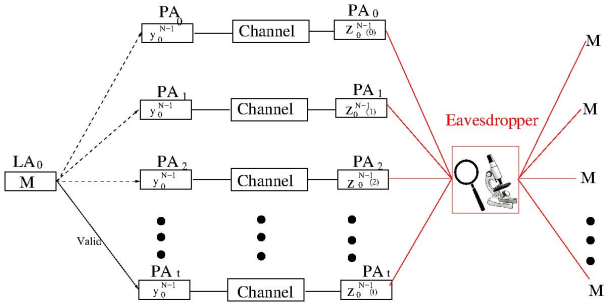

Fig. 3. Illustration and modelling of insecure deletion in non-volatile memories.

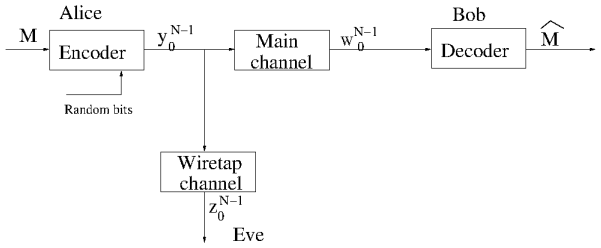

Fig. 4. Wiretap codes model. M is the message to send to Bob, y_0^{N-1} is the encoded codeword, w_0^{N-1} and z_0^{N-1} are noisy codewords of y_0^{N-1} passing through the main channel and the wiretap channel, respectively, and $\hat{M}$ is the estimate of M given by Bob.

rewriting codeword) initially stored at PA_0. Due to out-of-place updates and garbage collections etc, copies of y_0^{N-1} may be stored at PA_1, PA_2, $\cdots$, PA_t gradually, only one of which is mapped to LA_0 (indicated by the valid arrow in Fig. 3). $z_0^{N-1}(0), z_0^{N-1}(1), \cdots, z_0^{N-1}(t) \in \mathcal{Z}^N$ are noisy codewords of y_0^{N-1} at PA_0, $\cdots$, PA_t, respectively. When M is deleted by current methods, some of $z_0^{N-1}(0), \cdots, z_0^{N-1}(t)$ remain in raw memory. When the memory is attacked by a powerful eavesdropper who has access to the remaining codewords, the sensitive information of M can be leaked by using redundant copies of codewords.

Wiretap channel codes [18], [34], [46] provide unconditional information-theoretic security. More precisely, in the wiretap code setting (see Fig. 4), Alice wishes to send message M to Bob through a *main channel*, but her transmissions are also accessible to an eavesdropper Eve through another channel, *wiretap channel*. That is, Alice selects a codeword y_0^{N-1} based on the message M and random bits to send through the main channel and the wiretap channel. w_0^{N-1} and z_0^{N-1} are noisy codewords of y_0^{N-1} passing through the two channels, respectively. After receiving w_0^{N-1}, Bob maps it to an estimate of the original message. The goal of wiretap channel codes is to design a *reliable* and *secure* communication scheme, that is, Bob can reliably recover the message, while the information leaked to Eve is negligible.

Wiretap channel codes have gained escalating practical interest due to their striking benefits over conventional cryptography. Popular as wiretap channel code is for secure wireless communication [33], there have not been many research works [10] considering its application to non-volatile memory storages, and even fewer for the secure deletion problem.

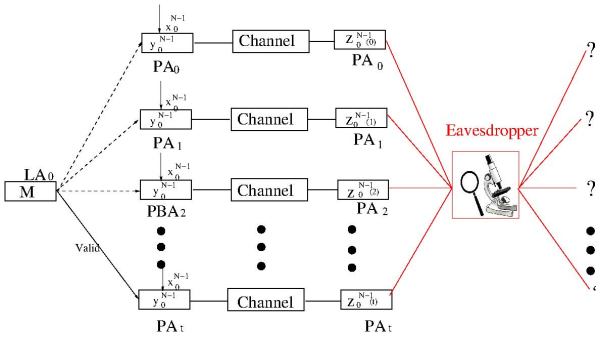

Fig. 5. Illustration and modelling of rewriting codes with security constraint in non-volatile memories.

C. Contribution and Structure of This Paper

In this paper, we first propose a new coding model – secure Write Efficient Memory– which has both properties of rewriting codes and wiretap channel codes [46] to jointly solve the endurance and insecure deletion problem. Fig. 5 presents the big picture of this setting, where the sensitive data M is encoded using a *rewriting codeword* y_0^{N-1}, noisy codewords of y_0^{N-1} are accessible to both a legal decoder, who can reliably retrieve M, and an eavesdropper, whose knowledge of M is negligible to *satisfy the security constraint*. The rigorous definition of the code is deferred to a later section.

To the best knowledge of the authors, this is the first work to study rewriting codes with a security concern under the wiretap channel setting. To that end, in this work we first explore the fundamental information theoretical results, i.e., achievable rate region and its capacity. Secondly, we present an optimal (i.e., achieve the whole rate region) code construction based on Polar codes for a large family of secure WEM.

The rest of this paper is structured as follows. In Section slowromancapii@, we formally define the secure Write-Efficient Memory model. In Section slowromancapiii@, we present the achievable regions for secure WEM and the secrecy rewriting capacities. The proof is presented in the Appendix Section. The code constructions are presented in Section slowromancapiv@. The conclusion and future work are shown in Section slowromancapv@.

II. Problem Definitions

In this section, we first define some notations used throughout this paper, and then formally present the secure WEM model.

A. Notations

Let $\mathcal{X}, \mathcal{W}, \mathcal{Z}$ be the alphabets of the symbol stored in a cell. Assume the sequence of data written to the storage medium is $\{M_1, \cdots, M_t\}$, where we assume M_i for $1 \leq i \leq t$ is uniformly distributed over $\mathcal{D}$, and the average rewriting cost is $\bar{D} \stackrel{def}{=} \lim_{t\to\infty} \frac{1}{t} \sum_{i=1}^{t} \varphi(x_0^{N-1}(i), \mathbf{R}(M_i, x_0^{N-1}(i)))$, where $x_0^{N-1}(i)$ is the current cell states before the i^{th} update.

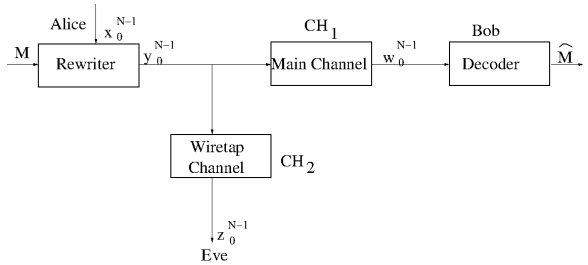

Fig. 6. The secure WEM model. CH_1, CH_2 are the main channel and the wiretap channel, respectively. $M, x_0^{N-1}, y_0^{N-1}, z_0^{N-1}, w_0^{N-1}$ and $\hat{M}$ are the message to rewrite, the current cell states, the rewrite codeword, the wiretap channel's output, the main channel's output and the estimated message, respectively.

B. Secure WEM With a Maximum Rewriting Cost Constraint

In the secure WEM setting (shown in Fig. 6), Alice wishes to store messages in a limited lifetime storage medium using the rewriting code, WEM [1], the messages are accessible to Bob through a storage channel but her transmissions also reach an eavesdropper Eve through a *noisier* wiretap channel.

Alternatively, in Fig. 6, the N-dimensional vector $x_0^{N-1} \in \mathcal{X}^N$ is the current cell states and the message M is the new information to write, which is independent of x_0^{N-1}. A rewriter uses both x_0^{N-1} and M to choose a new codeword $y_0^{N-1} \in \mathcal{X}^N$, which will be programmed as the N cells' new states. The codeword y_0^{N-1} passes through a noisy main memoryless channel CH_1 $\mathbb{W} = (\mathcal{X}, \mathcal{W}, W_{W|Y})$, and the noisy codeword $w_0^{N-1} \in \mathcal{W}^N$ is its output. The codeword y_0^{N-1} also passes through an even noisier and memoryless wiretap channel CH_2, $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$, $Y \in \mathcal{X}$.

Compared to the setting in Fig. 3, the model proposed in Fig. 6 is simplified in that here Eve can only reach one noisier codeword instead of multiple ones, and we left the case where Eve receives multiple codewords as our future work.

The assumption that CH_2 is noisier than CH_1 is due to the fact that a decoding of w_0^{N-1} at a legitimate decoder always happens prior to the deletion of w_0^{N-1} as after deletion the mapping table entry is marked invalid and the legitimate decoder has no access to w_0^{N-1}, thus z_0^{N-1} accumulates more disturb/interferences than w_0^{N-1} [9], [19], [30] because of read/write operations occurring after the legitimate decoding. Note that it is possible that a codeword is accessible by an eavesdropper before its deletion, however, this is out of the scope of this paper.

Due to the above reasons we assume that CH_1 is noiseless for simplicity, and leave the noisy case as the future work. For this reason, we omit the rigorous definition of the notion *noisier*, and interested readers are referred to [7].

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 the *weak security condition* $\lim_{N\to\infty} \frac{1}{N} H(M|z_0^{N-1})$ [46], also satisfies a predefined constraint to solve the insecure deletion problem.

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

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

- A message set $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$ 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 $\forall i \neq j$, $\mathcal{C}_i \bigcap \mathcal{C}_j = \emptyset$;
- A rewriting function $\mathbf{R}(M, x_0^{N-1})$ such that
  - $\varphi(x_0^{N-1}, \mathbf{R}(M, x_0^{N-1})) \leq D$ for any $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
  - and $\frac{1}{N} H(M|z_0^{N-1}) \leq R_e$ for any $M \in \mathcal{D}, z_0^{N-1} \in \mathcal{Z}^N$, $\epsilon > 0$ and $N \to \infty$.
- A decoding function $\mathbf{D}(y_0^{N-1})$ 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 rewriting cost of changing a current codeword x_0^{N-1} to its 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; the last one indicates that the decoder knows the rewriting message given a rewriting codeword.

Also note that in the above the security measure is the weak security condition. Beside it, other security measures, such as the strong security condition [7] and the recently proposed semantic security measure [6], also exist, and we leave them as future work.

Fixing D, the rewriting cost function $\varphi(\cdot)$ and the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$, a tuple $(R, R_e) \in \mathbb{R}^2$ is said to be *achievable* if there exists a sequence of $(N, 2^{NR}, R_e, D)$ codes. When $R_e = R$, we say it achieves full secrecy. The set of all achievable tuples is denoted by $\mathcal{R}^{swem}$, *rewriting-rate-equivocation region*. The secrecy rewriting capacity is $C^{swem}(D) \stackrel{def}{=} \sup_R\{R : (R, R) \in \mathcal{R}^{swem}\}$.

C. Secure WEM With an Average Rewriting Cost Constraint

The secure WEM code in definition 2 puts a constraint on the maximal rewriting cost, and we now define a code with an average rewriting cost constraint.

Definition 3: An $(N, 2^{NR}, R_e, D)_{ave}$ secure write-efficient memory code for wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$ and the rewriting cost function $\varphi(\cdot)$ consists of

- A message set $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$ 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 $\forall i \neq j$, $\mathcal{C}_i \bigcap \mathcal{C}_j = \emptyset$;
- A rewriting function $\mathbf{R}(M, x_0^{N-1})$ such that
  - $\bar{D} \leq D$;
  - and $\frac{1}{N} H(M|z_0^{N-1}) \geq R_e - \epsilon$ for any $M \in \mathcal{D}, z_0^{N-1} \in \mathcal{Z}^N$, $\epsilon > 0$ and $N \to \infty$.

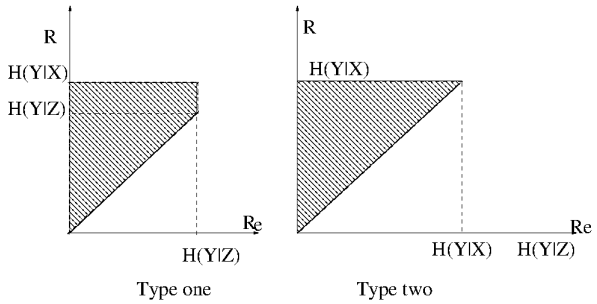

Fig. 7. Typical shapes of the achievable region in Theorem 4.

- A decoding function $\mathbf{D}(y_0^{N-1})$ such that $\mathbf{D}(\mathbf{R}(x_0^{N-1}, M)) = M$ for any $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$.

That is, compared with $(N, 2^{NR}, R_e, D)$ code, the rewriting cost constraint for each rewrite is replaced by the average rewriting cost constraint over the whole rewriting process.

Similarly, a tuple $(R, R_e)_{ave} \in \mathbb{R}^2$ is said to be *achievable* if there exists a sequence of $(N, 2^{NR}, R_e, D)_{ave}$ code. When $R_e = R$, we say it achieves full secrecy. The set of all achievable tuples is denoted by $\mathcal{R}_{ave}^{swem}$, and $C_{ave}^{swem}(D) \stackrel{def}{=} \sup_R\{R : (R, R)_{ave} \in \mathcal{R}_{ave}^{swem}\}$.

III. Results on the Achievable Region and Capacity

In this section, we present the main information theoretical results of this paper, i.e., to characterize the rewriting-rate-equivocation region and present capacity results.

A. Characterizing the Achievable Region

The following theorems present the main contributions of this paper, which characterize the achievable region for secure WEM. We defer their proofs to the Appendix Section.

Theorem 4: Define $\mathcal{R}(P_{XY}) =$

$$\left\{(R, R_e): \begin{array}{r} R \le H(Y|X) \\ R_e \le H(Y|Z) \\ R_e \le R \end{array}\right\},$$

where $P_{XY} \in \mathcal{P}(D) \stackrel{def}{=} \{P_{XY} : P_X = P_Y, E(\varphi(X, Y)) \le D\}$, 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 wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$.

Then, the rewriting-rate-equivocation region of the secure WEM is the convex region: $\mathcal{R}^{swem} = \bigcup_{P_{XY}} \mathcal{R}(P_{XY})$.

The first inequality of $\mathcal{R}(P_{XY})$ in Theorem 4 is the same as the rewriting rate for write-efficient memories [1, Th. 2], which is an immediate result as secure WEM is a special case of WEM. The second inequality is one of the main results of this paper.

The typical shapes of the above achievable region $\mathcal{R}(P_{XY})$ are presented in Fig. 7: type one is the case where $H(Y|Z) \le H(Y|X)$ for a given $P_{XY} \in \mathcal{P}(D)$, and type two is the other case.

The result for R_{ave}^{swem} is presented in the following:

Theorem 5: The rewriting-rate-equivocation region for secure WEM with an average rewriting cost constraint is the same as that of secure WEM with a maximal rewriting cost constraint, i.e., $\mathcal{R}_{ave}^{swem} = \mathcal{R}^{swem}$.

B. Secrecy Rewriting Capacity

In this subsection, we study secrecy rewriting capacities by utilizing Theorem 4 and Theorem 5. We mainly present the results for $C^{swem}(D)$ as $C_{ave}^{swem}(D)$ is the same as $C^{swem}(D)$ based on Theorem 5.

By specializing Theorem 4 to full secrecy, we obtain the following result for secrecy rewriting capacity.

Corollary 6: The secrecy rewriting capacity of secure WEM $(N, 2^{NR}, R_e, D)$ code with wiretap channel $\mathbb{P} = (\mathcal{Z}, \mathcal{Y}, \mathcal{P}_{\mathcal{Z}|\mathcal{Y}})$ 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 that of Theorem 4.

Let us examine some extreme cases: when the eavesdropper obtains the same observation as the legitimate decoder, in this case no confidential messages can be securely transmitted. From the above theorem, we know that if $Y = Z$, then $H(Y|Z) = 0$, and thus $C^{swem}(D) = 0$. On the other hand, when there is no eavesdropper, i.e., $Z \in \emptyset$, the result should coincide with original WEM code [1]. From theorem 4, we know that $C^{wem}(D) = \max_{P_{XY} \in \mathcal{P}(D)} H(Y|X)$, which is exactly the rewriting capacity of WEM.

We define the following terms to obtain further simpler results for secrecy rewriting capacity.

Definition 7: The WEM is *more capable* than wiretap channel $\mathbb{P} = (\mathcal{Z}, \mathcal{Y}, P_{\mathcal{Z}|\mathcal{Y}})$ if $I(X; Y) \ge I(Y; Z)$ for every $P_{XY} \in \mathcal{P}(D)$. The WEM is *less capable* than wiretap channel $\mathbb{P} = (\mathcal{Z}, \mathcal{Y}, \mathcal{P}_{\mathcal{Z}|\mathcal{Y}})$ if $I(X; Y) < I(Y; Z)$ for every $P_{XY} \in \mathcal{P}(D)$.

With the above notations, we have the following results for secrecy rewriting capacity.

Corollary 8: The secrecy rewriting capacity $C^{swem}(D)$ is $\max_{P_{XY} \in \mathcal{P}(D)} H(Y|X)$ if WEM is less capable than wiretap channel $\mathbb{P}$, (which is effectively the rewriting capacity of write-efficient memory [1, Theorem 2]) and $H(Y|Z)$ for $P_{XY} \in \mathcal{P}(D)$ if WEM is more capable than wiretap channel.

We present the following concrete example:

Example 9: Consider the following binary secure WEM $(N, 2^{NR}, R_e, D)$, where the rewriting cost function is the Hamming distance, and wiretap channel $\mathbb{P}$ is the binary symmetric channel with flipping rate p. Based on [1, Theorem 4], the WEM rewriting capacity is $\mathcal{R}(D) = H(D)$ in this case. Therefore, if WEM is less capable, then $C^{swem}(D) = H(p)$; if WEM is more capable, then $C^{swem}(D) = H(D)$.

IV. Polar Codes-Based Construction for Secure WEM

In this section, we present a code construction based on Polar codes for secure WEM, and prove that such codes achieve the whole rewriting-rate-equivocation region for a family of secure WEM.

A. A Brief Introduction to Polar Codes

The Polar code [3] was invented by Arikan in 2008, and it is the first theoretically proven capacity approaching code for symmetric channels. Polar code is a milestone in coding theory not only for its great success in channel coding but also for its remarkable performances in lossy source coding [24] , wiretap channel coding [2], [13], [34], write-once memories [8], etc. In this part, to help understand our results, we present a brief introduction to Polar codes.

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*. The Polar code ensemble is $C_N(F) = \{C_N(F, u_F), \forall u_F \in \{0,1\}^{|F|}\}$.

Denote $W_N^{(i)} : \{0,1\} \to \mathcal{Y}^N \times \{0,1\}^i$ the i-th *sub-channel* with the input set $\{0,1\}$, the output set $\mathcal{Y}^N \times \{0,1\}^i$, and the transition probability $W_N^{(i)}(y_0^{N-1}, u_0^{i-1}|u_i) \overset{def}{=} \frac{1}{2^{N-1}} \sum_{u_{i+1}^{N-1}} W^N(y_0^{N-1}|u_0^{N-1})$, 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 $\mathcal{B}_N(W,\beta) = \{i \in \{0,1,\cdots,N-1\} : I(W_N^{(i)}) \le \frac{1}{N}2^{-N^\beta}\}$. With a little abuse of 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 $\mathcal{B}'_N(W,\beta) = \{i \in \{0,1,\cdots,N-1\} : Z(W_N^{(i)}) \ge 1 - (\frac{1}{N}2^{-N^\beta})^2\}$.

Based on [25, 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 $\lim_{N\to\infty} \frac{1}{N}|\mathcal{G}_N(W,\beta)| = \lim_{N\to\infty} \frac{1}{N}|\mathcal{G}'_N(W,\beta)| = I(W)$.

B. Polar Codes are Optimal for Stochastically Degraded Secure-WEM Channels

1) Symmetric Secure WEM: In this part, 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 focuses on 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 whose rewriting capacity is achieved when current cell state (i.e., X) and updated cell state (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 $\mathcal{P}^s(D) \overset{def}{=} \{P_{XY} : P_X = P_Y, X \sim U(q), E(\varphi(X,Y)) \le D\}$ and q is the number of states for X.

Note that $\mathcal{R}(D)$ can be obtained through the following optimization function:

$$\begin{aligned} &\max : H(Y|X),\\ &\text{s.t.} : \sum_x \frac{1}{q}P(y|x) = \sum_y \frac{1}{q}P(x|y) = \frac{1}{q},\\ &\qquad \sum_x\sum_y \frac{1}{q}P(y|x)\varphi(y,x) \le D. \end{aligned} \tag{1}$$

Let $P^*(y|x)$ be the probability distribution maxmizing the objective function of (1). $P^*(y|x)$ plays the role of a channel. By convention, we call $P^*(y|x)$ a *WEM channel*, and denote it by $\mathbb{W} = (X, Y, W_{Y|X})$.

$$\begin{aligned} \frac{W_N^{(i)}(v_0^{N-1}, e_0^{i-1}|1)}{W_N^{(i)}(v_0^{N-1}, e_0^{i-1}|0)} &= \frac{\sum_{e_{i+1}^{N-1}} W^N(v_0^{N-1}|e_0^{i-1}1e_{i+1}^{N-1})}{\sum_{e_{i+1}^{N-1}} W^N(v_0^{N-1}|e_0^{i-1}0e_{i+1}^{N-1})},\\ &= \frac{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|e_0^{i-1}1e_{i+1}^{N-1} + (v_0^{N-1}+w_0^{N-1})(G_2^{\otimes n})^{-1})}{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|e_0^{i-1}0e_{i+1}^{N-1} + (v_0^{N-1}+w_0^{N-1})(G_2^{\otimes n})^{-1})},\\ &= \frac{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|f_0^{i-1}1e_{i+1}^{N-1})}{\sum_{e_{i+1}^{N-1}} W^N(w_0^{N-1}|f_0^{i-1}0e_{i+1}^{N-1})},\\ &= \frac{W_N^{(i)}(w_0^{N-1}, f_0^{i-1}|1)}{W_N^{(i)}(w_0^{N-1}, f_0^{i-1}|0)}, \end{aligned} \tag{2}$$

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 $j \le i-1$.

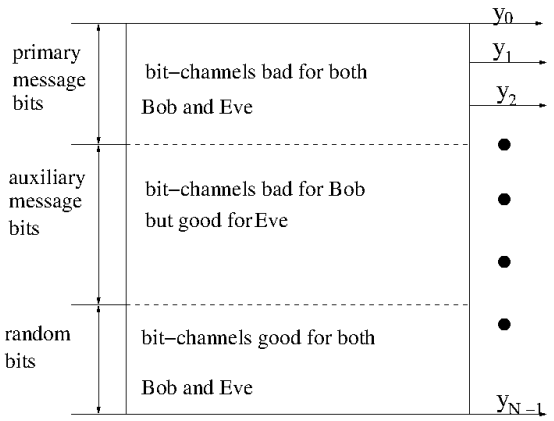

Fig. 8. Illustration of the Polar code construction for symmetric secure WEM achieving the capacity, where the output y_0^{N-1} is permuted in such a way that sub-channels are positioned as the above figure.

A symmetric secure WEM is such a secure WEM model that both the WEM channel $\mathbb{W}$ and the wiretap channel $\mathbb{P}$ are symmetric. Furthermore, we consider the case where the WEM channel is *stochastically degraded* with respect to the wiretap channel, which belongs to the case of 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 distance metric.

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

Example 10: Continue with example 9 of WEM with Hamming distance metric. 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 1 when $D > p$. Also in this case the WEM channel is stochastically degraded with respect to the wiretap channel, and it is one example of symmetric secure WEMs we focuse on in this work.

2) Optimal Code Construction Achieving Capacity: In the following we present optimal code constructions for symmetric secure WEM where the cost constraint is the average case only, and omit those for the symmetric secure WEM with the maximal rewriting cost constraint as their code constructions are identical.

The outline of the code construction is presented in Fig. 8: Given the WEM channel and the wiretap channel, we divide all sub-channels to three parts, i.e., sub-channels bad for both channels, whose sub-channel index set is denoted by set $\mathcal{M} \subseteq \mathbb{N}$, sub-channels good for both channels, whose sub-channel index set is denoted by set $\mathcal{M}_2 \subseteq \mathbb{N}$, and remaining sub-channels, whose sub-channel index set is denoted by the set $\mathcal{M}_1 \subseteq \mathbb{N}$.

Then the data $u_{\mathcal{M}}$ is represented by codewords of Polar code with frozen set $\mathcal{M}$, and frozen set value $u_{\mathcal{M}}$. 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 $\mathcal{M}$.

Algorithm 1 A Code Construction for Binary Symmetric Secure WEM

The $(N, 2^{NR}, R, D)_{ave}$ code is $\mathcal{C} = \bigcup_{u_{\mathcal{M}}} C_N(\mathcal{M}, u_{\mathcal{M}})$, where $C_N(\mathcal{M}, u_{\mathcal{M}})$ is a Polar code with the frozen set $\mathcal{M}$ set as above and $|\mathcal{M}| = NR$.

Algorithm 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 uniform distributed message known by both rewriter and decoder and $+$ is over GF(2).
2: Apply SC (Successive Cancellation) encoding [25] 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, $u_j =$

$$\begin{cases} u_{\mathcal{M}}(M)_{f(j)} & j \in \mathcal{M} \\ m_1 & j \in \mathcal{M}_1,\ m_1 \text{ is randomly chosen,} \\ m & \text{w.p. } \frac{W_N^{(i)}(u_0^{j-1}, v_0^{N-1}|m)}{\sum_{m'} W_N^{(i)}(u_0^{j-1}, v_0^{N-1}|m')}, \end{cases}$$

and $\hat{y}_0^{N-1} = u_0^{N-1} G_2^{\otimes n}$.
3: $y_0^{N-1} = \hat{y}_0^{N-1} + g_0^{N-1}$.

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

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 $\mathcal{B}_N(\mathbb{P},\beta) \subseteq \mathcal{B}'_N(\mathbb{W},\beta)$ [25]. Let $\mathcal{M} \overset{def}{=} \mathcal{B}'_N(\mathbb{W},\beta) \bigcap \mathcal{B}_N(\mathbb{P},\beta) = \mathcal{B}_N(\mathbb{P},\beta)$, $\mathcal{M}_1 \overset{def}{=} \mathcal{B}'_N(\mathbb{W},\beta) \bigcap \mathcal{G}_N(\mathbb{P},\beta)$ and $\mathcal{M}_2 \overset{def}{=} \mathcal{G}'_N(\mathbb{W},\beta)$. 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 1.

The rewriting operation is presented in Algorithm 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 $\mathbb{W} = (X, Y, W_{Y|X})$.

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

The decoding function is to retrieve bits in $\mathcal{M}$, and the algorithm is presented in Algorithm 3.

3) Theoretical Analysis: In this part, we present the theoretical analysis to show that the presented code construction is optimal. We start with calculating the probability of a randomly 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 satisfied 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 randomly 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 that $e_{\mathcal{R}}$ 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 the condition under which $\hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1))_{\mathcal{M}^c} = \hat{U}(w_0^{N-1},\ u_{\mathcal{M}}(M_2))_{\mathcal{M}^c}$. Note that in the following $+$ is over GF(2).

Lemma 11: 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 all elements of $\mathcal{M}_1$ have access to the same random source, we have $e_i = f_i + ((v_0^{N-1} + w_0^{N-1})(G_2^{\otimes n})^{-1})_i$.

Secondly consider $i \in \mathcal{M}_2$, and it is proved using a skill similar to [25, Lemma 3.12] as shown in equation 2.

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 is the rewriting data, thus it is easy to obtain that

$$P(e_{\mathcal{R}}|M) = \sum_{v_0^{N-1}} P(v_0^{N-1}) P(e_0^{N-1}|v_0^{N-1}),$$

$$= \sum_{v_0^{N-1}} \frac{1}{2^N} P(e_0^{N-1}|v_0^{N-1})$$

as v_0^{N-1} is uniformly distributed.

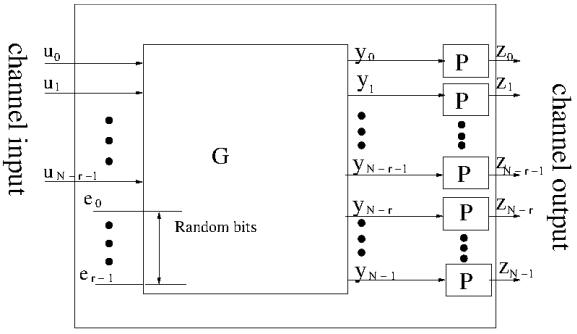

Fig. 9. Illustration of the induced channel, where the output y_0^{N-1} is permitted the same way as before such that sub-channels are positioned as the above figure, and where the channel inputs are u_0^{N-r-1} (i.e., rewriting data) and the channel outputs are z_0^{N-1} (i.e., noisy codeword of y_0^{N-1} though wiretap channel).

The following theorem shows that on average the probability that $e_{\mathcal{R}}$ is chosen given the rewriting data M is the same for every M.

Theorem 12: $P(e_{\mathcal{R}}|M)$ is independent of M, i.e., $P(e_{\mathcal{R}}|M_1) = P(e_{\mathcal{R}}|M_2)$ for $M_1, M_2 \in \mathcal{M}$.

Proof: The correctness holds by the fact that for each v_0^{N-1} there is a unique w_0^{N-1} such that $e_{\mathcal{R}} = \hat{U}(v_0^{N-1}, u_{\mathcal{M}}(M_1)) = \hat{U}(w_0^{N-1}, u_{\mathcal{M}}(M_2))$ 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: In this part, we investigate an induced channel by our code construction and show that it is symmetric. The symmetric channel plays a key role in our proof of the optimal code construction.

The induced channel is pictorially presented in Fig. 9, 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. Note that $e_{\mathcal{R}}$ is partially determined by successive cancellation encoding, i.e., for bits in $\mathcal{M}_2$, and is partially randomly selected for the remaining bits, i.e., for bits in $\mathcal{M}_1$. Let (u_0^{N-r-1}, e_0^{r-1}) denote the vector u_0^{N-1} with $u_{\mathcal{R}} = u_0^{N-r-1}$ and $u_{\mathcal{R}^c} = e_0^{r-1}$.

Next, we define its channel transition probability as $\mathcal{Q}(z_0^{N-1}|u_0^{N-r-1}) =$

$$\sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_{i=0}^{N-1} P(z_i|((u_0^{N-r-1}, e_0^{r-1})G_2^{\otimes n})_i), \qquad (2)$$

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}, it is determined as the previous part, and $P(z|y)$ is determined by the wiretap channel $\mathbb{P} = (\mathcal{Y}, \mathcal{Z}, P_{Z|Y})$. For convenience, we denote our channel by $\mathbb{Q}(\mathbb{P}, \mathcal{R}) = (\mathcal{X}^{N-r}, \mathcal{Z}^N, \mathcal{Q}_{Z^N|U^{N-r}})$. where $\mathcal{X} = \{0,1\}$.

Note that our definition of $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ shares some similarities with the induced channel in [34][Section VI-C]], that is, the inputs of both channels are data communicated to decoders, and the outputs of them are both noisy codewords through the wiretap channel. However, the channels differ in their

transition probabilities, which stems from how the random bits are determined, i.e., for channel in [34], the random bits are chosen independently and uniformly, and for our channel, the random bits are partially determined by successive cancellation encoding and are partially determined independently and uniformly. The similarities can also be found in their proofs, and for this reason we present its proof in sketch in the following theorem.

We now present the main result of this part in the following theorem, which shows the channel $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ is a symmetric channel.

Theorem 13: $\mathbb{Q}(\mathbb{P}, \mathcal{R})$ 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 [34, Th. 11] presents the necessary condition for the channel to be symmetric.

> 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
>
> $$W(y|a + x) = W(a.y|x) \tag{7}$$
>
> 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 [3], 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. We can further verify that 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 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. 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:

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

$$\begin{aligned}(x_0^{N-r-1} + y_0^{N-r-1}) \circ z_0^{N-1} &= ((x_0^{N-r-1}, 0_0^{r-1}) + (y_0^{N-r-1}, 0_0^{r-1})) G_2^{\otimes n} \cdot z_0^{N-1}, \\ &= (x_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot ((y_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot z_0^{N-1}), \\ &= x_0^{N-r-1} \circ (y_0^{N-r-1} \circ z_0^{N-1}),\end{aligned} \tag{3}$$

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

$$\begin{aligned}&\mathcal{Q}(z_0^{N-1}|a_0^{N-r-1} + x_0^{N-r-1}) \\ &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P(z_0^{N-1}|(((a_0^{N-r-1}, 0_0^{r-1}) + (x_0^{N-r-1}, e_0^{r-1})) G_2^{\otimes n}))_i, &(4)\\ &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P((a_0^{N-r-1}, 0_0^{r-1}) G_2^{\otimes n} \cdot z_0^{N-1}|(x_0^{N-r-1}, e_0^{r-1}) G_2^{\otimes n}))_i, &(5)\\ &= \sum_{e_0^{r-1}} P(e_0^{r-1}) \prod_i P(a_0^{N-r-1} \circ z_0^{N-1}|(x_0^{N-r-1}, e_0^{r-1}) G_2^{\otimes n}))_i, &(6)\\ &= \mathcal{Q}(a_0^{N-r} \circ z_0^{N-1}|x_0^{N-r-1}),\end{aligned}$$

where

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

(5) follows from [3, 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 $P^N(z_0^{N-1}|x_0^{N-1}) = \prod_{i=0}^{N-1} P(z_i|x_i)$;

(6) follows from our definition of the operation $\circ$, and also from Theorem 12.

where the correctness of the second item is shown in equation (3).

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 (4) $\sim$ (6). ∎

c) Rewriting cost constraint and security constraint: We first focus on the rewriting cost constraint. From [29, Th. 9], we know that as long as $\mathcal{M}_2 \subseteq \mathcal{G}'_N(\mathbb{W}, \beta)$, with high probability $\varphi(x_0^{N-1}, y_0^{N-1}) \leq D$ 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 technique similar to [34].

$$
\begin{aligned}
& I(M; z_0^{N-1}) \\
& \leq I(\hat{u}_M; \hat{z}_0^{N-1}), && (7)\\
& = I(\bar{u}_M; \bar{z}_0^{N-1}), && (8)\\
& = \sum_{i=0}^{|\mathcal{M}|-1} I(\bar{u}_i; \bar{z}_0^{N-1}|\bar{u}_0, \cdots, \bar{u}_{i-1}), && (9)\\
& = \sum_{i=0}^{|\mathcal{M}|-1} I(\bar{u}_i; \bar{z}_0^{N-1}\bar{u}_0^{i-1}), && (10)\\
& = \sum_{i=0}^{|\mathcal{M}|-1} C(\mathbb{P}_N^{(i)}), && (11)
\end{aligned}
$$

where

- (7) 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;
- (8) is due to the permutation such that u_0^{N-1} is arranged as Fig. 8;
- (9) is due to the chain rule of mutual information;
- (10) is due to $\bar{u}_i$ is independent of each other;
- (11) is due to $\mathbb{P}_N^{(i)}$ is the i-th virtual bit channel induced by the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$ (refer to Section slowromancapii@ 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 1. 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) Conclusion for theoretical performance: Thus based on analysis from *a)* $\sim$ *d)*, we have the following conclusion for theoretical performances of the proposed code construction:

Theorem 14: 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.

C. Optimal Code Construction Achieving the Whole Rewriting-Rate-Equivocation Region

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

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

$$
\left\{ (R, R_e) : \begin{array}{ll} R & \leq H(Y|X) \\ R_e & \leq H(Y|Z) \\ R_e & \leq R \\ H(Y|Z) & \leq H(Y|X) \end{array} \right\}, \qquad (12)
$$

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 Fig. 8, some auxiliary message bits carry information.

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

Theorem 15: For any symmetric secure WEM code (R, R_e) satisfying (12), when the WEM channel is stochastically degraded with respect to the wiretap channel, there exists a Polar code achieving the whole rewriting-rate-equivocation 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 [29, Lemma 7] or [24, Th. 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

$$
\begin{aligned}
&I(M; z_0^{N-1}) \\
&\quad \leq \sum_{i=0}^{|\mathcal{M}^1 \bigcup \mathcal{M}^2|-1} C(\mathbb{P}_N^{(i)}), && (13)\\
&\quad \leq \sum_{i=0}^{|\mathcal{M}^2|-1} C(\mathbb{P}_N^{(i)}) + \frac{|\mathcal{B}_N(\mathbb{P}, \beta)|}{N} 2^{-N^\beta}, && (14)\\
&\quad \leq N(R - R_e) + \epsilon, && (15)
\end{aligned}
$$

where

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

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

(15) 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. ■

D. Optimal Code for Secure WEM With Type-Two Region

In this subsection, we present the Polar code for secure WEM of type-two region. The code construction and analysis are similar to the previous ones, therefore in the following we present briefly its code construction and the main result without a detailed proof.

The family of secure WEM of type-two region we focus on is still the symmetric secure WEM, the rewriting cost metric is still symmetric, but here the wiretap channel is stochastically degraded with respect to the WEM channel.

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

$$
\left\{ (R, R_e) : \begin{array}{lll} R & \leq H(Y|X) \\ R_e & \leq R \\ H(Y|X) & \leq H(Y|Z) \end{array} \right\}, \qquad (16)
$$

for a $P_{XY} \in \mathcal{P}^s(D)$, the code construction for an $(N, 2^{NR_e}, R_e, D)$ symmetric secure WEM is as follows: When $\mathbb{P}$ is stochastically degraded with respect to $\mathbb{W}$, it implies that $\mathcal{B}'_N(\mathbb{W}, \beta) \subseteq \mathcal{B}_N(\mathbb{P}, \beta)$. Thus, let $\mathcal{M} = \mathcal{B}'_N(\mathbb{W}, \beta)$, $\mathcal{M}_1 = \emptyset$ and $\mathcal{M}_2 = \mathcal{G}'_N(\mathbb{W}, \beta)$. The $(N, 2^{NR_e}, R_e, D)_{ave}$ code is $\mathcal{C} = \bigcup_{u_\mathcal{M}} C_N(\mathcal{M}, u_\mathcal{M})$, where $C_N(\mathcal{M}, u_\mathcal{M})$ is a Polar code with the frozen set $\mathcal{M}$.

That is, compared to the previous code construction, the difference is data are represented by bits of $\mathcal{B}'_N(\mathbb{W}, \beta)$, and there is no need to fill in random bits. The $(N, 2^{NR}, R_e, D)$ is $\mathcal{C} = C_N(\mathcal{M}', u_{\mathcal{M}'})$, where $\mathcal{M}' \subset \mathcal{M}$ and $|\mathcal{M}'| = NR$, $\mathcal{M}_2 = \mathcal{M} - \mathcal{M}'$ $\mathcal{M}_2 = \mathcal{G}'_N(\mathbb{W}, \beta)$.

The rewriting function and the decoding function are the same as Algorithm 2 and Algorithm 3, respectively.

We summarize its performance in the following theorem.

Theorem 16: For any symmetric secure WEM code (R, R_e) satisfying (16), when the wiretap channel is stochastically degraded with respect to the WEM channel, there exists a Polar code achieving the whole rewriting-rate-equivocation region.

V. Concluding Remarks

In this paper, we propose a secure WEM model to address both the endurance and secure-deletion problems for non-volatile memories. We analyze the rewriting-rate-equivocation region, as well as the secrecy rewriting capacity. We further present code constructions based on Polar codes. There are still some important open problems, e.g., secure WEM codes with an optimal error correction capability. They remain as our future research topics.

Appendix

In this section, we show that the regions presented in Theorem 4 and Theorem 5 are achievable. We mainly focus on the proof of Theorem 4 since the proof of Theorem 5 is quite similar. For simplicity, we only present details of type one region of Fig. 7, and present just a sketch proof for type-two region due to its similarity.

The proof for type one region is divided into the following three steps and we present them in detail in the following parts:

- Step 1: We use a random-coding argument to show the existence of a sequence $(N, 2^{NR}, R_e, D)$ code such that $\frac{1}{N} I \stackrel{def}{=} \frac{1}{N} H(M) - \frac{1}{N} H(M|z_0^{N-1}) \leq \epsilon$ for some $\epsilon > 0$ and $R \leq H(Y|Z)$. This shows that the following sub-region of type one region is achievable: $\mathcal{R}'(P_{XY}) \stackrel{def}{=}$

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

  where $P_{XY} \in \mathcal{P}(D)$.
- Step 2: We show that the entire type one region in Theorem 4 is achievable with a minor modification of the code construction presented in step 1.
- Step 3: We show that the $\mathcal{R}^{swem}$ is convex.

A. Step 1: Achieving Region $\mathcal{R}'(P_{XY})$

1) Background on Strong Typical-Sequences: We first present some background about strong typical-sequences. For more details, interested readers are referred to [14].

Let x_0^{N-1} be a sequence with N elements drawn from $\mathcal{X}$. Define the type of x_0^{N-1} by $\pi(x|x_0^{N-1}) = \frac{|\{i: x_i = x\}|}{N}$. The set $\mathcal{T}_\epsilon^N(X)$ is defined as:

$$
\mathcal{T}_\epsilon^N(X) = \{x_0^{N-1} : |\pi(x|x_0^{N-1}) - P_X(x)| \leq \epsilon, \forall x\}.
$$

That is, the set of sequences for which the empirical frequency is within ϵ of the probability $P_X(x)$ for every $x \in \mathcal{X}$.

Let (x_0^{N-1}, y_0^{N-1}) be a pair of sequences with elements drawn from $(\mathcal{X}, \mathcal{Y})$. Define their joint type: $\pi(x, y|x_0^{N-1}, y_0^{N-1}) = \frac{|\{i: (x_i, y_i) = (x, y)\}|}{N}$ for $(x, y) \in \mathcal{X} \times \mathcal{Y}$. We denote $\mathcal{T}_\epsilon^N(XY) = \{(x_0^{N-1}, y_0^{N-1}) : |\pi(x, y|x_0^{N-1}, y_0^{N-1}) - P_{XY}(x, y)| \leq \epsilon, \forall (x, y)\}$.

For $x_0^{N-1} \in \mathcal{T}_\epsilon^N(X)$ and $P_{Y|X}$, we define the conditional typical sequence $\mathcal{T}_{Y|X}^N(x_0^{N-1}) = \{y_0^{N-1} : (x_0^{N-1}, y_0^{N-1}) \in \mathcal{T}_\epsilon^N(XY)\}$.

The following results will be used: i

1) For a vector x_0^{N-1}, where x_i is chosen i.i.d. $\sim P_X$,

$$
Pr(x_0^{N-1} \in \mathcal{T}_\epsilon^N(X)) \to 1 \text{ as } N \to \infty. \qquad (17)
$$

2) For vectors x_0^{N-1}, y_0^{N-1}, where (x_i, y_i) is chosen i.i.d. $\sim P_{XY}$,

$$Pr((x_0^{N-1}, y_0^{N-1}) \in \mathcal{T}_\epsilon^N(XY)) \to 1 \text{ as } N \to \infty. \quad (18)$$

3) For $x_0^{N-1} \in \mathcal{T}_\epsilon^N(X)$, and y_0^{N-1} is independently chosen according to P_Y, then $Pr((x_0^{N-1}, y_0^{N-1}) \in \mathcal{T}_{Y|X}^N(x_0^{N-1})) \in$

$$[2^{-N(I(X;Y)+\lambda)}, 2^{-N(I(X;Y)-\lambda)}], \quad (19)$$

for some $\lambda(\epsilon) > 0$ with $\lambda \to 0$ as $\epsilon \to 0$.

4) For any $x_0^{N-1} \in \mathcal{T}_\epsilon^N(X)$, we have $|\mathcal{T}_{Y|X}^N(x_0^{N-1})| \in$

$$[(N+1)^{-|\mathcal{X}||\mathcal{Y}|}2^{NH(Y|X)}, 2^{NH(Y|X)}]. \quad (20)$$

2) Rewriting Function Being Random to Achieve Full Secrecy: In this part, we explore one desired property of rewriting function, i.e., it should be stochastic to achieve full secrecy, when (x_0^{N-1}, y_0^{N-1}) has the property (x_i, y_i) is chosen i.i.d. $\sim P_{XY} \in \mathcal{P}(D)$.

For convenience, we write the rewriting function as $y_0^{N-1} = \mathbf{R}(M, x_0^{N-1}, M_1, M_2)$ where M_1 and M_2 are independent of M and x_0^{N-1}, M_1 and M_2 are constant if $\mathbf{R}(\cdot)$ is deterministic, and at least one of them is a random variable otherwise. M_1 and M_2 play significant roles in deriving the rewriting-rate-equivocation region, i.e., whether only M_1, M_2, or both of them should be random, and how to determine their random values. For example, in the following M_1 and M_2 are both random in order to achieve the full secrecy, while only M_2 is random in order to achieve the entire type one region.

In the following, we bound I using M, M_1, M_2 in equation (21), equation (22) and equation (23).

Therefore, if

$$\frac{1}{N}H(M_1) = I(Y;Z) - I(X;Y) + \sigma_1, \quad (24)$$

which implies that the rewriting function $\mathbf{R}(M, x_0^{N-1}, M_1, M_2)$ is random,

$$\frac{1}{N}H(M_1M_2|z_0^{N-1}M) \le \sigma_2, \quad (25)$$

and

$$H(x_0^{N-1}|M_1M_2Mz_0^{N-1}) - H(x_0^{N-1}|y_0^{N-1}) \le \sigma_3 \quad (26)$$

for $\sigma_i \ge 0$ for $i = 1, 2, 3$, the full secrecy is possible.

In the following subsection, we present a code construction having all those properties to achieve full secrecy.

3) Enhanced Secure WEM: The achievability of the region $\mathcal{R}'(P_{XY})$ is obtained by designing a specific random code construction for the following enhanced secure WEM such that the equation (24), and inequalities (25) and (26) hold.

We define the enhanced secure WEM (as shown in Fig. 10) as follows:

Definition 17: An $(N, 2^{NR}, 2^{NR_1}, 2^{NR_2}, D)$ code for type one enhanced secure WEM with wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Y|Z})$ and the rewriting cost function $\varphi(\cdot)$ consists of:

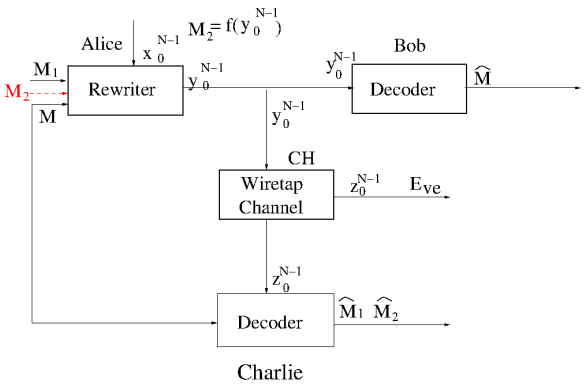

Fig. 10. Type one enhanced secure WEM model. CH is the wiretap channel. M, M_1 are messages to rewrite, where M is the primary message, M_1 is the auxiliary message and may not carry information, x_0^{N-1} is the current cell states, y_0^{N-1} is the rewrite codeword, M_2 is the random factor determined by $f(y_0^{N-1})$, z_0^{N-1} is the wiretap channel's output, $\hat{M}_1$, $\hat{M}_2$ and $\hat{M}$ are estimated messages corresponding to M_1, M_2 and M, respectively.

- A *primary* message set $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$, an *auxiliary* message set $\mathcal{R}_1 = \{0, 1, \cdots, 2^{NR_1} - 1\}$ and a *random* message set $\mathcal{R}_2 = \{0, 1, \cdots, 2^{NR_2} - 1\}$;
- A *stochastic* rewriting function for Alice: $\mathbf{R}_A : \mathcal{R}_1 \times \mathcal{D} \times \mathcal{X}^N \to \mathcal{X}^N$ such that $\varphi(x_0^{N-1}, \mathbf{R}_A(M_1, M, x_0^{N-1})) \le D$ for all $M \in \mathcal{D}, M_1 \in \mathcal{R}_1$ and $x_0^{N-1} \in \mathcal{X}^N$;
- An *auxiliary* function for Alice to determine the random argument in $\mathbf{R}_A$, $f : \mathcal{X}^N \to \mathcal{R}_2$. And a *deterministic* rewriting function for Alice: $\mathbf{R}'_A : \mathcal{R}_1 \times \mathcal{R}_2 \times \mathcal{D} \times \mathcal{X}^N \to \mathcal{X}^N$ such that $\mathbf{R}'_A(M_1, f(\mathbf{R}_A(x_0^{N-1}, M, M_1)), M, x_0^{N-1}) = \mathbf{R}_A(x_0^{N-1}, M, M_1)$ for all $M_1 \in \mathcal{R}_1, M \in \mathcal{D}, x_0^{N-1} \in \mathcal{X}^N$;
- A decoding function for Bob: $\mathbf{D}_B : \mathcal{X}^N \to \mathcal{D}$ such that $\mathbf{D}_B(\mathbf{R}_A(M_1, M, x_0^{N-1})) = M$ for all $M \in \mathcal{D}, M_1 \in \mathcal{R}_1$ and $x_0^{N-1} \in \mathcal{X}^N$;
- A *virtual* decoding function for Charlie: $\mathbf{D}_C : \mathcal{Z}^N \times \mathcal{D} \to \mathcal{R}_1 \times \mathcal{R}_2$.

That is, the original secure WEM is enhanced by 1) splitting the message set into $\mathcal{D}$ and $\mathcal{R}_1$, and introducing a random variable $M_2 \in \mathcal{R}_2$. Note that $M_1 \in \mathcal{R}_1$ is a dummy message to achieve full secrecy in this part, and carries partial information otherwise (see the following part). That is, we sacrifice rewriting rate to gain full secrecy. M_2 does not carry any information; 2) for each stochastic rewriting codeword $y_0^{N-1} = \mathbf{R}_A(M_1, M, x_0^{N-1})$, the implicit random variable M_2 can be obtained by the auxiliary function $f(\cdot)$; 3) the same rewriting codeword $y_0^{N-1} = \mathbf{R}_A(M_1, M, x_0^{N-1})$ can also be obtained by the deterministic rewriting function $\mathbf{R}'_A(M_1, M_2, M, x_0^{N-1})$; and 4) introducing a virtual decoder Charlie, who accesses to z_0^{N-1} and the message M, and is to give estimates of M_1 and M_2, $\hat{M}_1$ and $\hat{M}_2$. The role of Charlie is motivated by the inequation 25, i.e., $\frac{1}{N}H(M_1M_2|z_0^{N-1}M) \le \sigma_2$, and it leads to decoding M_1 and M_2 with z_0^{N-1} and M available.

The reliability of Charlie is measured by $P_e = Pr((M_1, M_2) \ne (\hat{M}_1, \hat{M}_2))$.

We present a random code construction for the above enhanced secure WEM as follows, and we illustrate the code construction using Fig. 11:

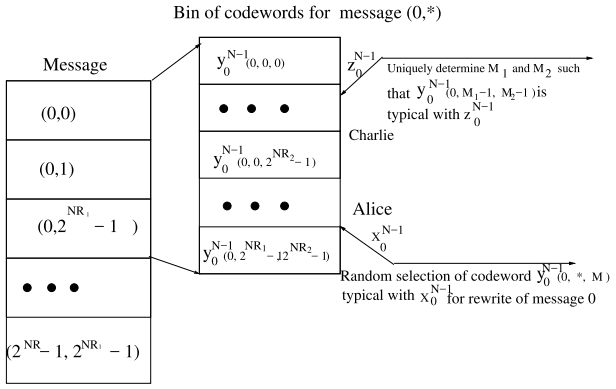

Fig. 11. Illustration of binning structure, rewriting process for Alice and decoding process for Charlie for type one enhanced secure WEM.

4) Random Code Construction for Type One Enhanced Secure WEM :

- Codebook generation: Randomly divide $\mathcal{T}_\epsilon^N(X)$ into $2^{N(R+R_1)}$ bins $\mathcal{B}(M, M_1)$ where $M \in \mathcal{D}$ and $M_1 \in \mathcal{R}_1$. Let $R_2 = H(X) - R - R_1$, and for each codeword in bin $\mathcal{B}(M, M_1)$, index it by $M_2 \in \{0, 1, ..., 2^{NR_2} - 1\}$. Abusing of notation, we index x_0^{N-1} by $\mathcal{B}(M, M_1, M_2)$ or $x_0^{N-1}(M, M_1, M_2)$.
- $\mathbf{R}_A$: given M, M_1 and x_0^{N-1}, randomly choose M_2 such that $y_0^{N-1} = \mathcal{B}(M, M_1, M_2) \in \mathcal{T}_{P_{Y|X}}^N(x_0^{N-1})$ for any M_2;
- f: given the rewriting codeword $y_0^{N-1} = \mathcal{B}(M, M_1, M_2)$, output M_2. $\mathbf{R}'_A$ is to output $\mathcal{B}(M, M_1, M_2)$ with M, M_1, M_2;
- $\mathbf{D}_B$: given y_0^{N-1}, output M such that $y_0^{N-1} = \mathcal{B}(M, M_1, M_2)$ for any M_1 and M_2;
- $\mathbf{D}_C$: given M, z_0^{N-1}, output a unique $\hat{M}_1, \hat{M}_2$ such that $y_0^{N-1} = \mathcal{B}(M, \hat{M}_1, \hat{M}_2) \in \mathcal{T}_{P_{Y|Z}}^N(z_0^{N-1})$.

5) Analysis of the Random Code Construction: The above construction has the property (x_i, y_i) i.i.d. $\sim \mathcal{P}(D)$ and $\mathbf{D}_B$ satisfies the constraint $\mathbf{D}_B(\mathbf{R}_A(M_1, M, x_0^{N-1})) = M$. We next consider the rewriting function.

Let us first consider the probability of rewriting failure, i.e., $Pr(\text{no } y_0^{N-1} \in \mathcal{B}(M, M_1) \text{ such that } y_0^{N-1} \in \mathcal{T}_{P_{Y|X}}^N(x_0^{N-1}))$

$$\begin{aligned}
&= (1 - \frac{1}{2^{N(R+R_1)}})^{|\mathcal{T}_{P_{Y|X}}^N(x_0^{N-1})|}, \\
&= (1 - \frac{1}{2^{N(R+R_1)}})^{2^{N(R+R_1)}|\mathcal{T}_{P_{Y|X}}^N(x_0^{N-1})|2^{-N(R+R_1)}}, \\
&\le e^{-(2^{NH(Y|X)-N(R+R_1)})}, \qquad (27)
\end{aligned}$$

where inequation (27) is based on the property (20). Therefore, if $R + R_1 \le H(Y|X)$, the above probability tends to be 0 and we have a desired y_0^{N-1}. We further know that $R_2 \ge I(X; Y)$ since $R_2 = H(X) - R - R_1$. Finally, we analyze the condition under which the average error probability $E(P_e)$

$$\begin{aligned}
&= E(Pr(M_1, M_2) \neq (\hat{M}_1, \hat{M}_2)) \\
&= Pr((M_1, M_2) = (j, k)) \cdot \\
&\quad E(Pr((\hat{M}_1, \hat{M}_2) \neq (j, k) | (M_1, M_2) = (j, k)))
\end{aligned}$$

tends to be 0 as $N \to 0$. If $P_e \to 0$ holds, we know that $\frac{1}{N} H(M_1 M_2 | z_0^{N-1} M) \le \sigma_2$ based on Fano's inequality.

By the symmetry of the code construction, the average error probability does not depend on (M_1, M_2), thus we assume $(M_1, M_2) = (1, 1)$. Further, without less of generality, we assume that $M = 1$.

Define the following error events: $\mathcal{E}_{1,1} \overset{def}{=}$

$$\{(y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ) \text{ and } y_0^{N-1} = \mathcal{B}(1, 1, 1)\},$$

and $\mathcal{F}_{j,k} \overset{def}{=}$

$$\{(y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ) \text{ and } y_0^{N-1} \in \mathcal{B}(1, j, k)\}.$$

By the union bound, $E(Pr((\hat{M}_1, \hat{M}_2) \neq (1, 1)|$

$$\begin{aligned}
I &= I(M; z_0^{N-1}), \\
&= I(M x_0^{N-1} M_1 M_2; z_0^{N-1}) - I(M_1 M_2 x_0^{N-1}; z_0^{N-1} | M), \\
&= I(y_0^{N-1}; z_0^{N-1}) - I(M_1 M_2 x_0^{N-1}; z_0^{N-1} M), \\
&= I(y_0^{N-1}; z_0^{N-1}) - H(M_1 M_2 x_0^{N-1}) + H(M_1 M_2 x_0^{N-1} | z_0^{N-1} M), \qquad (21) \\
&= I(y_0^{N-1}; z_0^{N-1}) - H(M_1 M_2) - H(x_0^{N-1}) + H(M_1 M_2 x_0^{N-1} | z_0^{N-1} M), \\
&= I(y_0^{N-1}; z_0^{N-1}) - I(y_0^{N-1}; x_0^{N-1}) - H(M_1) - H(M_2) - H(x_0^{N-1} | y_0^{N-1}) \\
&\quad + H(M_1 M_2 | M z_0^{N-1}) + H(x_0^{N-1} | M_1 M_2 M z_0^{N-1}), \\
&= N I(Y; Z) - N I(Y; X) - H(M_1) - H(M_2) - H(x_0^{N-1} | y_0^{N-1}) \\
&\quad + H(M_1 M_2 | M z_0^{N-1}) + H(x_0^{N-1} | M_1 M_2 M z_0^{N-1}), \qquad (22) \\
&\le N I(Y; Z) - N I(Y; X) - H(M_1) - H(x_0^{N-1} | y_0^{N-1}) + H(x_0^{N-1} | M_1 M_2 M z_0^{N-1}) \\
&\quad + H(M_1 M_2 | M z_0^{N-1}), \qquad (23)
\end{aligned}$$

where

(21) is due to $y_0^{N-1} = \mathbf{R}(M, x_0^{N-1}, M_1, M_2)$, and M_1, M_2 and x_0^{N-1} are independent of M;

(22) is due to (x_i, y_i) is i.i.d. according to $P_{XY} \in \mathcal{P}(D)$ based on our assumption, and the wiretap channel is memoryless.

$(M_1, M_2) = (1,1))$

$$\leq Pr(\mathcal{E}_{1,1}^c) + \bigcup_{(j,k)\neq(1,1)} Pr(\mathcal{F}_{j,k}),$$
$$\leq \sum_{j,k} Pr((y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ)|y_0^{N-1}$$
$$= \mathcal{B}(1,j,k)) + \epsilon', \quad (28)$$
$$\leq 2^{N(R_1+R_2-I(Y;Z)+\lambda)} + \epsilon', \quad (29)$$

where inequation (28) is based on the property (18), and inequation (29) is based on the property (19).

Therefore, when $R_1 + R_2 \leq I(Y;Z)$, that is, $R_1 = I(Y;Z) - I(X;Y) + \sigma_1$, $E(Pr((\hat{M}_1, \hat{M}_2) \neq (1,1)|(M_1, M_2) = (1,1))) \leq \epsilon$. Hence, we obtain that $R \leq H(Y|Z) + \sigma$. Based on Fano's inequality [12, lemma 7.9.1], we obtain that $\frac{1}{N}H(M_1M_2|z_0^{N-1}M) \leq \frac{1}{N} + Pr((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2))(R_1 + R_2) \leq \sigma_2$.

Based on our code construction, y_0^{N-1} is uniquely determined by M, M_1, M_2, therefore $H(x_0^{N-1}|MM_1M_2z_0^{N-1}) = H(x_0^{N-1}|y_0^{N-1}z_0^{N-1}) \leq H(x_0^{N-1}|y_0^{N-1}) + \sigma_3$. That is, $\frac{1}{N}I \leq \sigma_1 + \sigma_2 + \sigma_3$ based on inequation (23). Therefore, (R, R) is achievable for $R \leq H(Y|Z)$.

B. Step 2: Achieving the Entire Type One Region $\mathcal{R}(P_{XY})$

The key idea is to modify step 1 such that we let the dummy message M_1 transmit additional information.

The code construction is modified as follows,

- $\mathbf{D}_B$: given y_0^{N-1}, output M and M_1 such that $y_0^{N-1} = \mathcal{B}(M, M_1, M_2)$ for any M_2.

The remaining parts are the same as step 1.

The analysis of the above code construction is as follows.

By checking the analysis for rewriting cost constraint of step 1, we know that as long as $R + R_1 \leq H(Y|X)$, there exists a codeword satisfying the rewriting cost constraint.

Next, consider the equivocation rate:

$$\frac{1}{N}H(MM_1|z_0^{N-1}) \geq \frac{1}{N}H(M|z_0^{N-1}),$$
$$= \frac{1}{N}H(M) - \frac{1}{N}I(M; z_0^{N-1}).$$

With similar techniques as step 1, i.e. $I(M; z_0^{N-1}) \leq \sigma$, we can prove that $\frac{1}{N}H(MM_1|z_0^{N-1}) \geq R - \sigma$. Thus, we obtain that $(R + R_1, R - \sigma)$ is achievable, where $R + R_1 \leq H(Y|X)$ and $R \leq H(Y|Z)$.

C. Step 3: $\mathcal{R}^{swem}$ is Convex

We show that $\mathcal{R}^{swem}$ is convex by proving that, for any $P_{X_1Y_1}, P_{X_2Y_2} \in \mathcal{P}(D)$, the convex hull of $\mathcal{R}(P_{X_1Y_1})$ and $\mathcal{R}(P_{X_2Y_2})$ is in $\mathcal{R}^{swem}$.

Let $(R_1, R_{e1}) \in \mathcal{R}(P_{X_1Y_1})$ for some random variables X_1, Y_1 and Z_1 whose joint distribution is such that $\forall(x,y,z) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$, $P_{X_1Y_1Z_1}(x,y,z) = P_{X_1}(x)P_{Y_1|X_1}(y|x)P_{Z|Y}(z|y)$. Similarly, let $(R_2, R_{e2}) \in \mathcal{R}(P_{X_2Y_2})$ for some random variables X_2, Y_2 and Z_2 whose joint distribution is such that $\forall(x,y,z) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$, $P_{X_2Y_2Z_2}(x,y,z) = P_{X_2}(x)P_{Y_2|X_2}(y|x)P_{Z|Y}(z|y)$.

Let

$$\theta = \begin{cases} 1 & \text{with probability } \lambda, \\ 2 & \text{with probability } 1-\lambda, \end{cases}$$

thus we know that $\theta \to X_\theta \to Y_\theta \to Z_\theta$ forms a Markov chain and the joint distribution of X_θ, Y_θ and Z_θ satisfies $\forall(x,y,z) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$, $P_{X_\theta Y_\theta Z_\theta}(x,y,z) = P_{X_\theta}(x)P_{Y_\theta|X_\theta}(y|x)P_{Z|Y}(z|y)$ and $P_{X_\theta Y_\theta} \in \mathcal{P}(D)$. Let $X = X_\theta$, $Y = Y_\theta$ and $Z = Z_\theta$. Then

$$H(Y|X) = H(Y_\theta|X_\theta),$$
$$\geq H(Y_\theta|X_\theta, \theta),$$
$$= \lambda H(Y_1|X_1) + (1-\lambda)H(Y_2|X_2),$$
$$= \lambda R_1 + (1-\lambda)R_2, .$$

Similarly, we can prove that $H(Y|Z) \geq \lambda R_{e1} + (1-\lambda)R_{e2}$. Hence, for any $\lambda \in [0,1]$, there exist X, Y such that $(\lambda R_1 + (1-\lambda)R_2, \lambda R_{e1} + (1-\lambda)R_{e2}) \in \mathcal{R}(P_{XY}) \subseteq \mathcal{R}^{swemn}$, which finishes the proof.

D. Sketch Proof of Achieving the Entire Region $\mathcal{R}(P_{XY})$ for Type Two Region

In this case, we rewrite equation (23) as follows: I

$$= I(M; z_0^{N-1}),$$
$$= I(y_0^{N-1}; z_0^{N-1}) - I(y_0^{N-1}; x_0^{N-1}) - H(M_1)$$
$$- H(M_2) - H(x_0^{N-1}|y_0^{N-1})$$
$$+ H(M_1M_2|Mz_0^{N-1}) + H(x_0^{N-1}|M_1M_2Mz_0^{N-1}),$$
$$\leq NI(Y;Z) - NI(X;Y) + H(M_1M_2|Mz_0^{N-1})$$
$$+ H(x_0^{N-1}|M_1M_2Mz_0^{N-1}) - H(x_0^{N-1}|y_0^{N-1}),$$
$$\leq NI(Y;Z) - NI(X;Y) + H(M_1)$$
$$+ H(M_2|MM_1z_0^{N-1})$$
$$+ H(x_0^{N-1}|MM_1M_2z_0^{N-1}) - H(x_0^{N-1}|y_0^{N-1}),$$

where some repeated steps of equation (23) are skipped.

Therefore, if $\frac{1}{N}H(M_1) = I(Y;X) - I(Y;Z) + \sigma_1$, $\frac{1}{N}H(M_2|z_0^{N-1}MM_1) \leq \sigma_2$, and $H(x_0^{N-1}|M_1M_2\ Mz_0^{N-1}) - H(x_0^{N-1}|y_0^{N-1}) \leq \sigma_3$ for $\sigma_i \geq 0$ for $i = 1,2,3$, the full secrecy is possible.

This motivates us to redefine the enhanced secure WEM (shown in Fig. 12) as follows:

Definition 18: An $(N, 2^{NR}, 2^{NR_1}, 2^{NR_2}, D)$ code for type two enhanced secure WEM with wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Y|Z})$ and the rewriting cost function $\varphi(\cdot)$ consists of:

- A *primary* message set $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$, an *auxiliary* random message set $\mathcal{R}_1 = \{0, 1, \cdots, 2^{NR_1} - 1\}$ and a *primary* random message set $\mathcal{R}_2 = \{0, 1, \cdots, 2^{NR_2} - 1\}$;
- A *stochastic* rewriting function for Alice: $\mathbf{R}_A : \mathcal{D} \times \mathcal{X}^N \to \mathcal{Y}^N$ such that $\varphi(x_0^{N-1}, \mathbf{R}_A(M, x_0^{N-1})) \leq D$ for all $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
- An *auxiliary* function for Alice to determine the random argument in $\mathbf{R}_A$, $f : \mathcal{Y}^N \to \mathcal{R}_1 \times \mathcal{R}_2$. And a *deterministic* rewriting function for Alice: $\mathbf{R}'_A : \mathcal{R}_1 \times \mathcal{R}_2 \times \mathcal{D} \times \mathcal{X}^N \to \mathcal{Y}^N$ such that $\mathbf{R}'_A(f(\mathbf{R}_A(x_0^{N-1}, M)), M, x_0^{N-1}) = \mathbf{R}_A(x_0^{N-1}, M)$ for all $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;

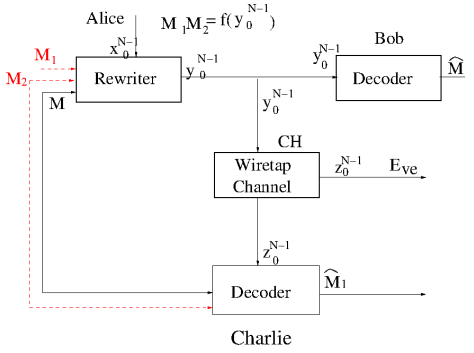

Fig. 12. Type two enhanced secure WEM model. CH is the wiretap channel. M is a message to rewrite, x_0^{N-1} is the current cell states, y_0^{N-1} is the rewrite codeword, M_1 and M_2 are two random variables determined by $f(y_0^{N-1})$, z_0^{N-1} is the wiretap channel's output, $\hat{M}_1$ and $\hat{M}$ are estimated messages corresponding to M_1 and M, respectively.

- A decoding function for Bob: $\mathbf{D}_B : \mathcal{Y}^N \to \mathcal{D}$ such that $\mathbf{D}_B(\mathbf{R}_A(M, x_0^{N-1})) = M$ for all $M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
- A *virtual* decoding function for Charlie: $\mathbf{D}_C : \mathcal{Z}^N \times \mathcal{D} \to \mathcal{R}_2 \times \mathcal{R}_1$.

That is, compared with type one enhanced secure WEM, we let M_1 be the random variable instead of auxiliary message variable. Again, the role of Charlie is motivated by the inequation in the above, i.e., $\frac{1}{N}H(M_2|z_0^{N-1}MM_1) \le \sigma_2$, and it leads to decoding M_2 with z_0^{N-1}, M and M_2 available. The reliability for Charlie is measured by $P_e = Pr(M_1 \neq \hat{M}_1)$.

The remaining proof details are similar to those of previous subsections, and we omit them.

E. Proof of the Converse Part

The proof for R is the same as that of [1], and for completeness, we present it here. We first digress to prove the following conclusion:

$$NR = H(y_0^{N-1}|x_0^{N-1}). \tag{30}$$

$$\begin{aligned} NR &= H(M), && (31)\\ &= H(M|x_0^{N-1}), && (32)\\ &= H(Mx_0^{N-1}|x_0^{N-1}), && (33)\\ &\ge H(y_0^{N-1}|x_0^{N-1}), && (34)\\ &\ge H(M|x_0^{N-1}), && (35)\\ &= NR, \end{aligned}$$

where

(31) follows from the assumption that M is uniformly distributed among $\mathcal{D}$;
(32) follows from the fact that M is independent of x_0^{N-1};
(34) follows from $y_0^{N-1} = \mathbf{R}(M, x_0^{N-1})$ and the fact that function never increases entropy;
(35) follows from $M = \mathbf{D}(y_0^{N-1})$.

Next, we proceed the proof as follows: $R = \frac{1}{N}H(y_0^{N-1}|x_0^{N-1}) \le \frac{1}{N}\sum_{i=0}^{N-1} H(y_i|x_i) \le H(Y|X)$.

Then, we consider the rewriting cost, $\varphi(x_0^{N-1}, y_0^{N-1}) = \frac{1}{N}\sum_{i=0}^{N-1}\varphi(x_i, y_i) = E(\varphi(X, Y)) \le D$, thus $P_{XY} \in \mathcal{P}(D) = \{P_{XY} : P_X = P_Y, E(\varphi(X, Y)) \le D\}$, where the fact that $P_X = P_Y$ follows from the assumption that stationary distribution of x_0^{N-1} exists. Therefore, $R \le H(Y|X)$ for $P_{XY} \in \mathcal{P}(D)$.

Let us consider $R_e \le \frac{1}{N}H(M|z_0^{N-1}) \le \frac{1}{N}H(y_0^{N-1}|z_0^{N-1}) \le \frac{1}{N}\sum_{i=0}^{N-1} H(y_i|z_i) \le H(Y|Z)$.

Meanwhile, we know that $R_e \le \frac{1}{N}H(M|z_0^{N-1}) \le \frac{1}{N}H(M) = R$. Therefore, $R_e \le \min\{R, H(Y|Z)\}$.

REFERENCES

[1] R. Ahlswede and Z. Zhang, "Coding for write-efficient memory," *Inf. Comput.*, vol. 83, no. 1, pp. 80–97, Oct. 1989.
[2] M. Andersson, "Coding for the wiretap channal," Ph.D. dissertation, Dept. School Electr. Eng., Royal Inst. Technol., Stockholm, Sweden, 2011.
[3] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
[4] M. Barlas, "Characterization of metal oxide RRAM memory cells," Ph.D. dissertation, Dept. School Electr. Eng., École Polytech. Fédérale de Lausanne, Lausanne, Switzerland, 2014.
[5] P. S. S. Basu, K. Srinivasan, and K. Vorouganti, "An empirical study of file systems on NVM," in *Proc. IEEE 31st Symp. Mass Storage Syst. Technol. (MSST)*, Santa Clara, CA, USA, May 2015, pp. 1–14.
[6] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, 2012, pp. 294–311.
[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[8] D. Burshtein and A. Strugatski, "Polar write once memory codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 5088–5101, Aug. 2013.
[9] Y. Cai, E. F. Haratsch, O. Mutlu, and K. Mai, "Error patterns in MLC NAND flash memory: Measurement, characterization, and analysis," in *Proc. Conf. Design, Autom. Test Europe*, Dresden, Germany, Mar. 2012, pp. 521–526.
[10] Y. Cassuto, "Not just for errors: Codes for fast and secure flash storage," in *Proc. Globecom*, Dec. 2010, pp. 1871–1875.
[11] Y. Cassuto and E. Yaakobi, "Short Q-ary fixed-rate WOM codes for guaranteed rewrites and with hot/cold write differentiation," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3942–3958, Jun. 2014.
[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.
[13] E. Sasoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1117–1121.
[14] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Orlando, FL, USA: Academic, 1982.
[15] P. Desnoyers, "Analytic modeling of SSD write performance," in *Proc. Int. Syst. Storage Conf. (SYSTOR)*, Jun. 2012, Art. no. 12.
[16] F.-W. Fu and A. J. H. Vinck, "On the capacity of generalized write-once memory with state transitions described by an arbitrary directed acyclic graph," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 308–313, Jan. 1999.
[17] R. Gabrys, E. Yaakobi, L. Dolecek, A. Vardy, J. K. Wolf, and P. H. Siegel, "Non-binary WOM-codes for multilevel flash memories," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2011, pp. 40–44.
[18] E. Hof and S. Shamai. (2010). "Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels." [Online]. Available: https://arxiv.org/abs/1005.2759
[19] D. Ielmini, S. Lavizzari, D. Sharma, and A. Lacaita, "Physical interpretation, modeling and impact on phase change memory (PCM) reliability of resistance drift due to chalcogenide structural relaxation," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, Dec. 2007, pp. 939–942.
[20] A. N. Jacobvitz, R. Calderbank, and D. J. Sorin, "Writing cosets of a convolutional code to increase the lifetime of flash memory," in *Proc. 50th Annu. Allerton Conf. Commun., Control Comput. (Allerton)*, Monticello, IL, USA, Oct. 2012, pp. 308–318.
[21] A. N. Jacobvitz, R. Calderbank, and D. J. Sorin, "Coset coding to extend the lifetime of memory," in *Proc. IEEE 19th Int. Symp. High Perform. Comput. Archit. (HPCA)*, Feb. 2013, pp. 222–233.

[22] A. Jiang, V. Bohossian, and J. Bruck, "Rewriting codes for joint information storage in flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5300–5313, Oct. 2010.
[23] H. Kim, S. Seshadri, C. L. Dickey, and L. Chiu, "Evaluating phase change memory for enterprise storage systems: A study of caching and tiering approaches," in *Proc. 12th USENIX Conf. File Storage Technol. (FAST)*, Santa Clara, CA, USA, 2014, pp. 33–45.
[24] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.
[25] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, Dept. School Electr. Eng., École Polytech. Fédérale de Lausanne, Lausanne, Switzerland, 2010.
[26] L. A. Lastras-Montano, M. Franceschini, T. Mittelholzer, J. Karidis, and M. Wegman, "On the lifetime of multilevel memories," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Coex, Seoul, South Korea, Jun. 2009, pp. 1224–1228.
[27] L. A. Lastras-Montaño, M. M. Franceschini, T. Mittelholzer, and M. Sharma, "On the capacity of memoryless rewritable storage channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3178–3195, Jun. 2014.
[28] B. C. Lee, E. Ipek, O. Mutlu, and D. Burger, "Phase change memory architecture and the quest for scalability," *Commun. ACM*, vol. 53, no. 7, pp. 99–106, Jul. 2010.
[29] Q. Li and A. Jiang, "Polar codes are optimal for write-efficient memories," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 660–667.
[30] Q. Li, A. Jiang, and E. F. Haratsch, "Noise modeling and capacity analysis for NAND flash memories," in *Proc. IEEE Int. Symp. Inf. Theory(ISIT)*, Honolulu, HI, USA, Jun. 2014, pp. 2262–2266.
[31] Q. Li, H. Chang, A. Jiang, and E. F. Haratsch, "Joint decoder of content-replication codes for NAND flash memories," in *Proc. Non-Volatile Memory Workshop*, San Diego, CA, USA, Mar. 2015, pp. 2262–2266.
[32] Y. Li, P. P. C. Lee, and J. C. S. Lui, "Stochastic modeling of large-scale solid-state storage systems: Analysis, design tradeoffs and optimization," in *Proc. ACM SIGMETRICS/Int. Conf. Meas. Modeling Comput. System (SIGMETRICS)*, 2013, pp. 179–190.
[33] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.
[34] 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, Oct. 2011.
[35] J. Reardon, S. Capkun, and D. Basin, "Data node encrypted file system: Efficient secure deletion for flash memory," in *Proc. 21st USENIX Conf. Security Symp.*, Berkeley, CA, USA, 2012, pp. 333–348.
[36] J. Reardon, C. Marforio, S. Capkun, and D. Basin, "User-level secure deletion on log-structured file systems," in *Proc. 7th ACM Symp. Inf., Comput. Commun. Security*, 2012, pp. 63–64.
[37] J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, "Secure data deletion from persistent media," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 271–284.
[38] R. L. Rivest and A. Shamir, "How to reuse a 'write-once' memory," *Inf. Control*, vol. 55, nos. 1–3, pp. 1–19, 1982.
[39] M. Rosenblum and J. K. Ousterhout, "The design and implementation of a log-structured file system," *ACM Trans. Comput. Syst.*, vol. 10, no. 1, pp. 26–52, 1992.
[40] S. Russell and R. Ramakrishnan, "bLSM: A general purpose log structured merge tree," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2012, pp. 217–228.
[41] K. Santhosh, V. Avinash, N. Krishna, and P. Henry, "Spatially-coupled codes for write-once memories," in *Proc. 53rd Annu. Allerton Conf. Commun., Control Comput. (Allerton)*, Monticello, IL, USA, Oct. 2015, pp. 125–131.
[42] A. Shpilka, "Capacity-achieving multiwrite WOM codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1481–1487, Mar. 2014.
[43] A. Vardy and E. Yaakobi, "Codes for RAID solutions based upon SSDs," in *Proc. Inf. Theory Workshop*, Jerusalem, Isreal, Apr. 2015, pp. 1–5.
[44] D. Vučinić *et al.*, "DC Express: Shortest latency protocol for reading phase change memory over PCI express," in *Proc. 12th USENIX Conf. File Storate Technol. (FAST)*, Feb. 2014, pp. 309–315.
[45] M. Wei, L. M. Grupp, F. E. Spada, and S. Swanson, "Reliably erasing data from flash-based solid state drives," in *Proc. 9th USENIX Conf. File Stroage Technol. (FAST)*, San Jose, CA, USA, 2011, p. 8.
[46] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[47] Y. Yang and J. Zhu, "Algebraic modeling of write amplification in hotness-aware SSD," in *Proc. Int. Syst. Storage Conf. (SYSTOR)*, May 2015, Art. no. 4.

Qing Li (S') received the B.Sc. degree in information security from University of Science and Technology of China, Hefei, Anhui, China, in 2010, and the Ph.D. degree in computer science from Texas A&M University in College Station, Texas in 2015.

He is now working with ScaleFlux Inc. on big data storage.

Anxiao (Andrew) Jiang (SM') received the B.Sc. degree in electronic engineering from Tsinghua University, Beijing, China in 1999, and the M.Sc. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, California in 2000 and 2004, respectively.

He is currently an Associate Professor in the Computer Science and Engineering Department and the Electrical and Computer Engineering Department at Texas A&M University in College Station, Texas. He has been a visiting professor or associate at California Institute of Technology, University of California in San Diego and Ecole Polytechnique Federale de Lausanne (EPFL), and a consulting researcher at HP Labs, EMC and Microsoft Research. His research interests include information theory, data storage, networks and algorithm design.

Prof. Jiang is a recipient of the NSF CAREER Award in 2008 for his research on information theory for flash memories and a recipient of the 2009 IEEE Communications Society Data Storage Technical Committee (DSTC) Best Paper Award in Signal Processing and Coding for Data Storage.