Fifty-second Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 1 - 3, 2014

Coding for Secure Write-Efficient Memories

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

***Abstract*—Endurance and security are two serious challenges for non-volatile memories such as flash memories. Write-Efficient Memory (WEM) is an important rewriting code model to solve the endurance problem.**

Aiming at jointly solving the endurance and the security issues in non-volatile memories, this work focuses on rewriting code with a security constraint. To that end, a novel coding model, secure WEM, is proposed here. We explore its rewriting-rate-equivocation region and its secrecy rewriting capacity in this paper.

I. Introduction

Flash memories are becoming ubiquitous due to the advantages such as higher data density, scaling size and non-volatility. The two most conspicuous challenges of flash memories are its limited lifetime, i.e., the so called *endurance* problem, and the difficulty of secure deletion, i.e., the so called *insecure deletion*. 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 here, secure write-efficient memory (WEM), to address the two challenges jointly, and focus on information theoretical results, i.e., rewriting-rate-equivocation region and its secrecy rewriting capacity.

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

Flash memories are significant non-volatile memory techniques. The unit of flash memory is a cell. Each flash chip is composed of blocks, each block consists of pages, and each page is made up of cells. There are three operations on flash cells, read, write/program and erase. The granularity of read/write and erase is a page and a block, respectively.

The first challenge in flash memories is *endurance*. Endurance means flash memory can only experience a limited number of program/erase cycles, beyond which the cell quality degradation can no longer be accommodated by the memory system fault tolerance capacity.

Rewriting code is a powerful coding technology to solve the endurance problem from information theory and coding theory perspective. Fig.1 presents us 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 the predefined constraint between x_0^{N-1} and y_0^{N-1} is satisfied.

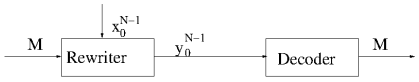

Fig. 1. Rewriting code model, where M is the message to rewrite, x_0^{N-1} is the current cell state, and y_0^{N-1} is the rewrite codeword.

Based on various constraints, different rewriting code models such as write-once memory (WOM) codes [14] and WEM codes [1] have been proposed, and optimal code constructions [4], [11] have been constructed for them, respectively. 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}.

Let $\mathcal{D} \subseteq \mathbb{N}$. We use $\mathcal{D}$ to 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 $\mathbf{R} : \mathcal{X}^N \times \mathcal{D} \to \mathcal{X}^N$, which changes the N cells' levels to represent the new input data. (Note that the rewriting function can be either deterministic or stochastic.)

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

- $\mathcal{D} = \{0, 1, \cdots, M-1\}$ and $\bigcup_{i=0}^{M-1} \mathcal{C}_i$, 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 $\mathbf{D}(\mathbf{R}(x_0^{N-1}, i)) = i$ for any $i \in \mathcal{D}$.

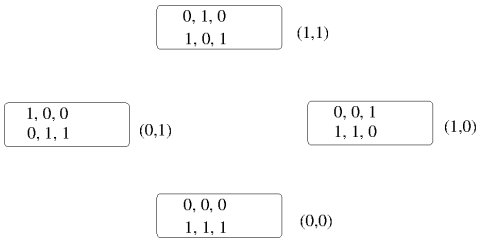

Fig. 2. An example of (3, 4, 1) WEM, where two sequences of numbers inside a box are codewords, the number outside a box is the data represented by the codewords inside the box, e.g., both codewords $(0,0,0)$ and $(1,1,1)$ represent data $(0,0)$, the rewriting cost metric is the Hamming distance, that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

That is, the constraint is for each rewrite the rewriting cost between the current cell state x_0^{N-1} and the rewrite codeword y_0^{N-1} has to be less than a predefined constraint. Note, another WEM model with the average rewrite cost constraint is also present in [1]. We present a concrete example of WEM in Fig.2.

Although WEM is a reasonable model for solving endurance in phase-change memory [9], it is worth noting that WEM can also be used in flash memories, such as rank modulation [10]. On the other hand, as pointed out by Fu et al [7], "the binary WOM and the generalized WOM are special cases of deterministic WEM", for which the example presented in Fig. 2 is a good example as it is exactly the classical WOM code example used by Rivest et al. in [14]. Therefore, in this work we focus on the WEM as our main tool for rewriting codes.

B. Insecure deletion and wiretap codes

Flash memory is commonly accessed through a Flash Translation Layer (FTL) [8], which is used in USB sticks, solid state drives, etc. One core function of FTL is to maintain a physical-to-logical mapping table. FTLs access the raw flash memory directly by a Physical Address (PA), and the PA is mapped to a Logical Address (LA) that computer system uses to access data. The writes on flash memory are made on *out-of-place* fashion, i.e., to update data in a LA, the original LA-PA mapping is marked as invalid, the data is written to a free page and a new LA-PA mapping is established. Other functions of FTL are wear leveling and garbage collection, etc.

The second challenge in flash memories is *insecure deletion* (or *insecure erasure*) ([15]). Insecure deletion is the phenomenon that FTL produces multiple copies of data that can not be deleted completely as it is either impossible or costly, however, a sophisticated attacker can recover and obtain information about the data.

We illustrate insecure deletion using Fig. 3 in detail. Let $\mathcal{X}, \mathcal{Z}$ be two alphabets of the symbol stored in a cell. Let M be the sensitive data (personal, finance information, etc) stored in a logical address LA_0. Let

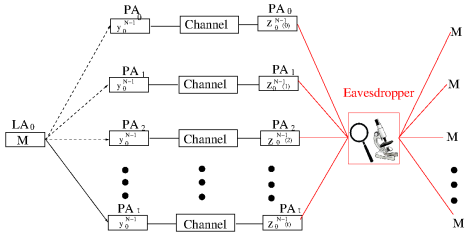

Fig. 3. Illustration of insecure deletion in flash memories

$y_0^{N-1} \in \mathcal{X}^N$ be its codeword (which may not be a rewriting codeword) initially stored in PA_0. Due to flash operations, pages are disturbed and interfered [12] so much that the noise can not be tolerated by the underlying error-correcting codes and other protection mechanisms, and data is copied to PA_1. (Note that PA_1 may also be the updated version of PA_0 due to data updating.) Similarly, copies of y_0^{N-1} may be storied in $\mathrm{PA}_2, \cdots, \mathrm{PA}_t$ gradually, only one of which is mapped to the 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} in $\mathrm{PA}_0, \cdots, \mathrm{PA}_t$, respectively. Besides noise, another reason to produce identical copies of codewords is wear leveling and garbage collection, that is, when a page is selected for garbage collection, its valid data is copied to other free pages and the mapping is reestablished. When M is deleted by current methods such as overwriting (i.e., update LA_0 to some random number), some of $z_0^{N-1}(0), \cdots, z_0^{N-1}(t)$ remain in raw flash memory [15] due to the out-of-place update. Note that, it is possible to block erase all copies of $z_0^{N-1}(0), z_0^{N-1}(1), \cdots, z_0^{N-1}(t)$, however, such operations incur a great many of block erasures and it is bad for flash memory endurance. Therefore, perfect deleting data is either not possible or very costly. When the flash is attacked by an eavesdropper, who is able to trace any one of $z_0^{N-1}(0), \cdots, z_0^{N-1}(t)$, and is aware of all encoding and decoding algorithms, the sensitive information of M can be leaked. As pointed out by Cassuto [5], " the challenge of removing the data from the device is both due to the imperfections of the physical erasure processes and, at a higher level, due to address-translation layers that may make it non-trivial to track all traces of sensitive data for erasure ".

Wiretap codes [16] provide unconditional information-theoretic security under the sole assumption that the channel from a sender to an eavesdropper is "noisier" than the channel from a sender to a receiver. More precisely, in the wiretap codes 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

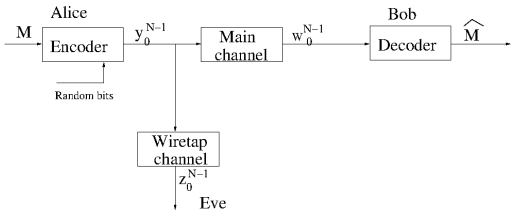

Fig. 4. Wiretap codes model. M is the message to send to Bob, y_0^{N-1} is the encoded codeword, w_0^{N-1} and z_0^{N-1} are noisy codewords of y_0^{N-1} passing through the main channel and the wiretap channel, respectively, and $\hat{M}$ is the estimate of M given by Bob.

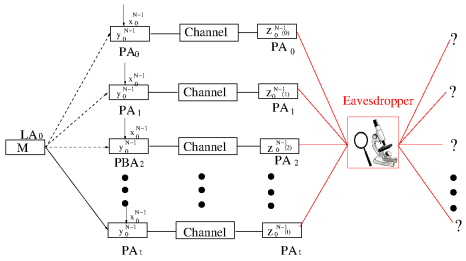

Fig. 5. Illustration of rewriting codes with security constraint in flash memories

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 is to design a *reliabe* and *secure* communication scheme, that is, Bob can reliably recover the message, while the information leaked to Eve is negligible.

Wiretap codes have been gaining escalating practical interest due to its two striking benefits over conventional cryptography. One is no computational assumption, which provides long-term security even facing with the incoming quantum computing era, and the other is no keys distribution, which is attractive for vulnerable and low-power devices. Popular as wiretap code is for secure wireless communication [13], there is barely no research work [5] considering its application to non-volatile memory storage.

C. Contribution of this paper

In this paper, we first propose a novel coding model here – secure write efficient memory– which has both properties of rewriting codes as well as wiretap channel codes to jointly solve the endurance and the insecure deletion problem. Fig. 5 presents us the big picture of this setting, where the sensitive data M is encoded using *rewriting code* 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*. Rigorous definition of the codes is deferred to a later section. To the best knowledge of authors, this is the first work to study rewriting code with security concern under the wiretap channel setting. To that end, in this work we mainly explore the fundamental information theoretical results, i.e., achievable rate region and its capacity.

II. Problem Definitions and Main Results

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

A. Terms and 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. By assuming the stationary distribution of cell levels x_0^{N-1} is $\pi(x_0^{N-1})$, $\bar{D} = \sum_{x_0^{N-1}} \pi(x_0^{N-1}) \sum_{j\in\mathcal{D}} \bar{D}_j(x_0^{N-1})$, where $\bar{D}_j(x_0^{N-1})$ is the average rewriting cost of updating cell levels x_0^{N-1} to a codeword representing $j \in \mathcal{D}$. (Note that the $\bar{D}_j(x_0^{N-1})$ may not be deterministic as the $\mathbf{R}(\cdot)$ can be stochastic.)

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

B. Secure WEM with a maximal rewriting cost constraint

The secure WEM model is illustrated in Fig. 6. Here 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}. The 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, such that the rewriting cost between x_0^{N-1} and y_0^{N-1} satisfies a predefined cost constraint for each rewrite. The codeword y_0^{N-1} passes through a noisy main memoryless channel CH_1 $\mathbb{W} = (\mathcal{X}, \mathcal{W}, W_{W|X})$, and the noisy codeword $w_0^{N-1} \in \mathcal{W}^N$ is its output. The decoder can reliably decode w_0^{N-1} to recover the message M. The codeword y_0^{N-1} also passes through a even noisier and memoryless wiretap channel CH_2, $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|Y})$, $Y \in \mathcal{X}$. (The assumption that CH_2 is more noisier than CH_1 is due to the fact that the decoding of w_0^{N-1} at a legitimate decoder always happens prior to the deletion of w_0^{N-1}, thus z_0^{N-1} suffers from more disturb/interference than w_0^{N-1} [12]). The equivocation rate at the eavesdropper $\frac{1}{N}H(M|z_0^{N-1})$ [16], which is the uncertainty of the eavesdropper about

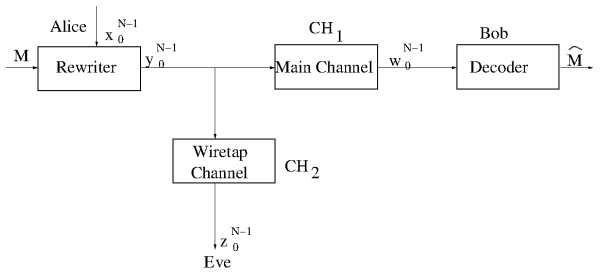

Fig. 6. The secure WEM model. CH_1, CH_2 are the main channel and the wiretap channel, respectively. $M, x_0^{N-1}, y_0^{N-1}, z_0^{N-1}, w_0^{N-1}$ and $\hat{M}$ are the message to rewrite, the current cell states, the rewrite codeword, the wiretap channel's output, the main channel's output and the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

the message M after observing the wiretap channel output z_0^{N-1}, also satisfies a predefined constraint such that at most a certain mount of information leaks.

Note that the wiretap channel $\mathbb{P}$ above not only models the disturb/interference mentioned in [12], but also models methods proposed in [15] such as *scrubbing*, that is re-program the page to turn all the remaining cell states to some specific state.

For simplicity, we assume that CH_1 is noiseless, and the leave the opposite case as the future work. For this reason, we omit the rigorous definition of the notion more noisier, and interested readers are referred to [3].

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 $\frac{1}{N} H(M|z_0^{N-1}) \geq R_e - \epsilon$ for any $M \in \mathcal{D}, z_0^{N-1} \in \mathcal{Z}^n$ and $\epsilon > 0$.
- 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 $x_0^{N-1} \in \mathcal{X}^N$.

Note that in the above definition, the first requirement of rewriting function is the same as that of WEM [1], and the second requirement of rewriting function is added here to consider the uncertainty of the message at the eavesdropper, therefore $(N, 2^{NR}, R_e, D)$ codes are actually a subset of write-efficient memory codes [1], and we term the code as secure WEM.

Also note that in the above the security measure is the weak security condition. Besides it, other security measures, such as the strong security condition [3] and the recently proposed semantic security measure [2], also exist, and we leave them as future work.

Fixed D, the rewriting cost function $\varphi(\cdot)$ and the wiretap channel $\mathbb{P} = (\mathcal{X}, \mathcal{Z}, P_{Z|X})$, a tuple $(R, R_e) \in \mathbb{R}^2$ is said to be *achievable* if there exists an $(N, 2^{NR}, R_e, D)$ 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. 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 $M \in \mathcal{D}, z_0^{N-1} \in \mathcal{Z}^N$ and $\epsilon > 0$.
- 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.

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

D. Main results of this paper

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

1) Characterizing the achievable region for $\mathcal{R}^{swem}$:

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

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

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

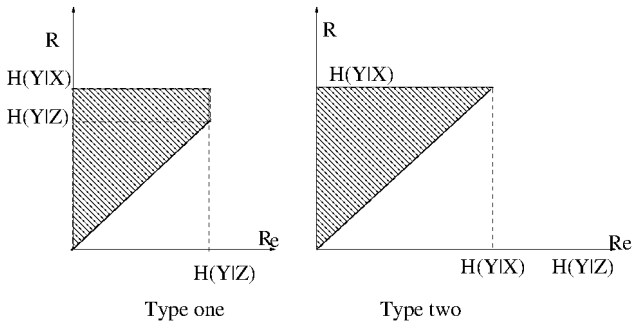

Fig. 7. Typical shape of the achievable region in Theorem 4.

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 in Theorem 4 is the same as the rewriting rate for write-efficient memories [1, Theorem 2], which is an immediate result as secure WEM is an especial case of WEM. The second inequality is the mayor contribution of this paper.

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

2) Characterizing the achievable region for $\mathcal{R}_{ave}^{swem}$:

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., $\mathcal{R}_{ave}^{swem} = \mathcal{R}^{swem}$.

III. Achievable regions for secure WEM

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 to that of Theorem 4. For further simplicity, we only present details of type one region of Fig. 7, skip the details for type two region of Fig. 7 as it is similar to the previous one, and the sketch can be found in the full version of this paper.

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 and show that the existence of a sequence $(N, 2^{NR}, R_e, D)$ code such that $\frac{1}{N}L \overset{def}{=} \frac{1}{N}H(M) - \frac{1}{N}H(M|z_0^{N-1}) \leq \epsilon$ for some $\epsilon > 0$ and $R \leq H(Y|Z)$. This shows that the following sub-region of type one region is achievable: $\mathcal{R}'(P_{XY}) \overset{def}{=} \{(R, R_e) : \begin{matrix} R & \leq H(Y|Z) \\ R_e & \leq R \end{matrix} \}$, 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) 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.

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}, 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 M_1 and M_2 should be random, and how to determine their random values.

In the following, we bound L using M, M_1, M_2 as follows, L

$$
\begin{aligned}
&= I(M; z_0^{N-1}),\\
&= I(M x_0^{N-1} M_1 M_2; z_0^{N-1})\\
&- I(M_1 M_2 x_0^{N-1}; z_0^{N-1}|M),\\
&= I(y_0^{N-1}; z_0^{N-1}) - I(M_1 M_2 x_0^{N-1}; z_0^{N-1} M),\\
&= I(y_0^{N-1}; z_0^{N-1}) - H(M_1 M_2 x_0^{N-1})\\
&+ H(M_1 M_2 x_0^{N-1}|z_0^{N-1} M),\\
&= I(y_0^{N-1}; z_0^{N-1}) - H(M_1 M_2) - H(x_0^{N-1})\\
&+ H(M_1 M_2 x_0^{N-1}|z_0^{N-1} M),\\
&= I(y_0^{N-1}; z_0^{N-1}) - I(y_0^{N-1}; x_0^{N-1}) - H(M_1)\\
&- H(M_2) - H(x_0^{N-1}|y_0^{N-1})\\
&+ H(M_1 M_2|M z_0^{N-1}) + H(x_0^{N-1}|M_1 M_2 M z_0^{N-1}),\\
&= NI(Y;Z) - NI(Y;X) - H(M_1)\\
&- H(M_2) - H(x_0^{N-1}|y_0^{N-1})\\
&+ H(M_1 M_2|M z_0^{N-1}) + H(x_0^{N-1}|M_1 M_2 M z_0^{N-1}),\\
&\leq NI(Y;Z) - NI(Y;X) - H(M_1)\\
&- H(x_0^{N-1}|y_0^{N-1}) + H(x_0^{N-1}|M_1 M_2 M z_0^{N-1})\\
&+ H(M_1 M_2|M z_0^{N-1}),
\end{aligned}
$$

where the third equation 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; the last equation is due to (y_0^{N-1}, x_0^{N-1}) is i.i.d according to $P_{XY} \in \mathcal{P}(D)$, and the wiretap channel is memoryless.

Therefore, if

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

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

$$\frac{1}{N}H(M_1 M_2|z_0^{N-1} M) \leq \sigma_2, \tag{2}$$

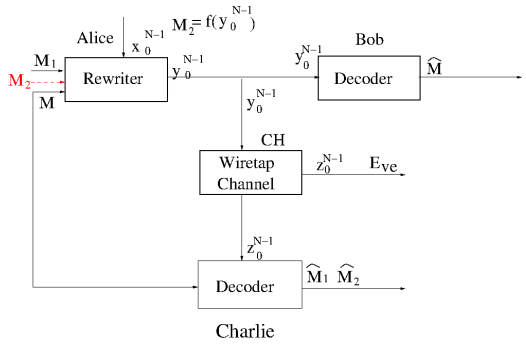

Fig. 8. Type one enhanced secure WEM model. CH is the wiretap channel. M, M_1 are messages to rewrite, where M is the primary message, M_1 is the auxiliary message and may not carry information, x_0^{N-1} is the current cell states, y_0^{N-1} is the rewrite codeword, M_2 is the random factor determined 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.

and

$$H(x_0^{N-1}|M_1M_2Mz_0^{N-1}) - H(x_0^{N-1}|y_0^{N-1}) \leq \sigma_3 \quad (3)$$

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

2) 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 (1), and inequations (2) and (3) hold.

We define the enhanced secure WEM (as shown in Fig. 8) as follows:

Definition 6. $(N, 2^{NR}, 2^{NR_1}, 2^{NR_2}, D)$ code for type one enhanced secure WEM with the wiretap channel $\mathbb{P} = (\mathcal{Y}, \mathcal{Z}, \mathcal{P}_{Y|Z})$ and the rewriting cost function $\varphi(\cdot)$ consists of:

- A *primary* message set $\mathcal{D} = \{0, 1, \cdots, 2^{NR} - 1\}$, an *auxiliary* message set $\mathcal{R}_1 = \{0, 1, \cdots, 2^{N\tilde{R}_1} - 1\}$ and a *random* message set $\mathcal{R}_2 = \{0, 1, \cdots, 2^{NR_2} - 1\}$;
- A *stochastic* rewriting function for Alice: $\mathbf{R}_A : \mathcal{R}_1 \times \mathcal{D} \times \mathcal{X}^N \to \mathcal{Y}^N$ such that $\varphi(x_0^{N-1}, \mathbf{R}_A(M_1, M, x_0^{N-1})) \leq D$ 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 factor in $\mathbf{R}_A$, $f : \mathcal{Y}^N \to \mathcal{R}_2$. And a *deterministic* rewriting function for Alice: $\mathbf{R}'_A : \mathcal{R}_1 \times \mathcal{R}_2 \times \mathcal{D} \times \mathcal{X}^N \to \mathcal{Y}^N$ 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 $M_1 \in \mathcal{R}_1, M \in \mathcal{D}$ and $x_0^{N-1} \in \mathcal{X}^N$;
- A decoding function for Bob: $\mathbf{D}_B : \mathcal{Y}^N \to \mathcal{D}$ 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). 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 reliability of Charlie is measured by $P_e = Pr((M_1, M_2) \neq (\hat{M}_1, \hat{M}_2))$.

3) Random code construction based on typical sequence for type one enhanced secure WEM :

- Codebook generation: Random 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}, random 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_2;
- $\mathbf{D}_C$: given M, z_0^{N-1}, output a unique $\hat{M}_1, \hat{M}_2$ such that $y_0^{N-1} = \mathcal{B}(M, \hat{M}_1, \hat{M}_2) \in \mathcal{T}_{P_{Y|Z}}^N(z_0^{N-1})$.

4) Analysis of the random code construction: Clearly, $\mathbf{D}_B$ 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(no $y_0^{N-1} \in \mathcal{B}(M, M_1)$ such that $y_0^{N-1} \in \mathcal{T}_{P_{Y|X}}^N(x_0^{N-1}))$

$$\begin{aligned} &= (1 - \frac{1}{2^{N(R+R_1)}})^{|\mathcal{T}_{P_{Y|X}}^N(x_0^{N-1})|}, \\ &= (1 - \frac{1}{2^{N(R+R_1)}})^{2^{N(R+R_1)}|\mathcal{T}_{P_{Y|X}}^N(x_0^{N-1})|2^{-N(R+R_1)}}, \\ &\leq e^{-(2^{NH(Y|X)-N(R+R_1)})}, \end{aligned} \quad (4)$$

where inequation (4) is based on the typical sequence property. Therefore, if $R + R_1 \leq H(Y|X)$, the above probability tends to be 0 and we have a desired y_0^{N-1}. We further know that $R_2 \geq I(X;Y)$ since $R_2 = H(X) - R - R_1$.

Finally, we analyze the condition under which the average error probability $E(P_e) = E(Pr(M_1, M_2) \neq (\hat{M}_1, \hat{M}_2)) = Pr((M_1, M_2) = (j,k))E(Pr((\hat{M}_1, \hat{M}_2) \neq (j,k)|(M_1, M_2) = (j,k)))$

tends to be 0 as $N \to 0$. If $P_e \to 0$ holds, we know that $\frac{1}{N}H(M_1M_2|z_0^{N-1}M) \leq \sigma_2$ 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: $\mathcal{E}_{1,1} \stackrel{def}{=} \{(y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ) \text{ and } y_0^{N-1} = \mathcal{B}(1,1,1)\}$, and $\mathcal{F}_{j,k} \stackrel{def}{=} \{(y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ) \text{ and } y_0^{N-1} \in \mathcal{B}(1,j,k)\}$. By the union bound, $E(Pr((\hat{M}_1, \hat{M}_2) \neq (1,1)|(M_1, M_2) = (1,1)))$

$$\begin{aligned} &\leq Pr(\mathcal{E}_{1,1}^c) + \bigcup_{(j,k)\neq(1,1)} Pr(\mathcal{F}_{j,k}), \\ &\leq \sum_{j,k} Pr((y_0^{N-1}, z_0^{N-1}) \in \mathcal{T}_\epsilon^N(YZ)|y_0^{N-1} \\ &= \mathcal{B}(1,j,k)) + \epsilon', \quad (5) \\ &\leq 2^{N(R_1+R_2-I(Y;Z)+\lambda)} + \epsilon', \quad (6) \end{aligned}$$

where inequation (5) and inequation (6) are based on properties of typical sequences.

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 [6, 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, $\frac{1}{N}L \leq \sigma_1 + \sigma_2 + \sigma_3$ based on inequation (**??**). 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:

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

With similar techniques to 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

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

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. 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:

$$NR = H(y_0^{N-1}|x_0^{N-1}). \quad (7)$$

$$\begin{aligned} NR &= H(M), \quad (8) \\ &= H(M|x_0^{N-1}), \quad (9) \\ &= H(Mx_0^{N-1}|x_0^{N-1}), \quad (10) \\ &\geq H(y_0^{N-1}|x_0^{N-1}), \quad (11) \\ &\geq H(M|x_0^{N-1}), \quad (12) \\ &= NR, \end{aligned}$$

where

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

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

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

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

Meanwhile, we know that $R_e \leq \frac{1}{N}H(M|z_0^{N-1}) \leq \frac{1}{N}H(M) = R$, where the last inequality is based on the conclusion just obtained for $H(M)$. Therefore, $R_e \leq \min\{R, H(Y|Z)\}$.

IV. Secrecy rewriting capacity

In this section, we study secrecy rewriting capacities by utilizing Theorem 4 and Theorem 5. We mainly present the results for $C^{swem}(D)$ as $C^{swem}_{ave}(D)$ 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 7. 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, clearly no confidential messages can be securely transmitted. From the above theorem, we know that $Y = Z$, 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 be coinciding 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 8. The WEM is *more capable* than wiretap channel $\mathbb{P} = (\mathcal{Z}, \mathcal{Y}, P_{\mathcal{Z}|\mathcal{Y}})$ if $I(X;Y) \geq I(Y;Z)$ 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 $I(X;Y) \leq I(Y;Z)$ for every $P_{XY} \in \mathcal{P}(D)$.

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

Corollary 9. 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.

V. Acknowledgment

This work was supported in part by the NSF Grant CCF-1217944.

References

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

[2] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *International Cryptology Conference (CRYPTO)*, 2012, pp. 294–311.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

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

[5] Y. Cassuto, "Not just for errors: codes for fast and secure flash storage," in *Globecom 2010, Workshop on the Application of Communication Theory to Emerging Memory Technologies*, 2010, pp. 1871–1875.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[7] F. Fu and R. W. Yeung, "On the capacity and error-correcting codes of write-efficient memories," *IEEE Trans on Inf Theory*, vol. 46, no. 7, pp. 2299–2314, Nov 2000.

[8] E. Gal and S. Toledo, "Algorithms and data structures for flash memories," *ACM Computing Surveys*, vol. 37, pp. 138–163, 2005.

[9] L. A. Lastras-Montano, M. Franceschini, T. Mittelholzer, J. Karidis, and M. Wegman, "On the lifetime of multilevel memories," in *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory (ISIT'09)*, Coex, Seoul, Korea, 2009, pp. 1224–1228.

[10] Q. Li, "Compressed Rank Modulation," in *Proc. 50th Annual Allerton Conference on Communication, Control and Computing (Allerton)*, Monticello, IL, October 2012.

[11] Q. Li and A. Jiang, "Polar codes are optimal for Write-efficient Memories," in *proc 51th Annual Allerton Conference on Communication, Control and Computing (Allerton)*, Monticello, IL, October 2013.

[12] Q. Li, A. Jiang, and E. F. Haratsch, "Noise Modeling and Capacity Analysis for NAND Flash Memories," in *Proc. IEEE International Symposium on Information Theory(ISIT)*, Honolulu, HI, June 2014.

[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4, pp. 355–580, 2009.

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

[15] M. Wei, L. M. Grupp, F. E. Spada, and S. Swanson, "Reliably erasing data from flash-based solid state drives," in *Proceedings of the 9th USENIX conference on File and stroage technologies (FAST'11)*, San Jose, California, 2011.

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