Irregular Channel Polarization and Its Applications to Static Adversarial Wiretap Channel

Yizhi Zhao, Member, IEEE

Abstract

The problem of achieving the secrecy capacity of static adversarial wiretap channel with discrete memoryless channels is studied in this paper. To construct the explicit secure coding scheme, an irregular channel polarization operation is proposed which is the extension of Arikan’s channel polarization. As theoretically proofed, for \( N \) independent initial channels with different transition probabilities, channels generated by the operation \( G_N \) are also polarized into full noise channels and noiseless channels, same as the regular channel polarization. Then for the adversarial behaviors including directly reading and rewriting, equivalent channels are constructed by channel cascading with full noise or noiseless binary erase channels. Finally by applying the irregular channel polarization to the equivalent channels, a secure polar coding scheme is constructed which successfully achieves the secrecy capacity of static adversarial wiretap channel with discrete memoryless channels under the reliability and strong security criterions.

Index Terms

adversarial wiretap channel, irregular channel polarization, secrecy capacity, secure polar coding, strong security, reliability.

I. Introduction

The open problem of secrecy capacity achieving was introduced by Wyner in 1975 [1], along with his original wiretap channel (WTC) model in which eavesdropper can wiretapping the communication of legitimate parties through a degraded noisy wiretap channel. In his pioneering work, Wyner had shown the existence of channel noise based codes which can achieve the secrecy
capacity against the noisy channel type wiretapping approaches. Then in the follow-up work of Wyner and Ozarow\cite{2}, *wiretap channel type II* (WTC-II) was proposed with a direct type of wiretapping approach as that eavesdropper can directly read a certain part of the transmitted information from the noiseless main channel. Based on this directly reading, some channel level modification works were proposed, such as the noise extend WTC-II models\cite{3,4,5} and the multi-access extended WTC-II model\cite{6}. Then as an extension on the adversarial behavior,\cite{7} presented an active WTC-II in which eavesdropper not only directly read a certain part of the transmitted information, but also modify the bits observed. Later the *adversarial wiretap channel* (A-WTC) was proposed and studied by\cite{8}, in which eavesdropper can read and rewrite certain parts of the transmitted information directly and independently. Compared with the original WTC, secrecy capacities of WTC-II (including those channel level modified models) and A-WTC are much harder to achieve because of their directly adversarial approaches.

In the last decade, remarkable progress had been made for solving Wyner’s secrecy capacity achieving problem owing to the invention of Arıkan’s polar code\cite{9}. Secrecy capacities of original WTC\cite{10,11} and several extended WTCs\cite{12,13,14,15} had been achieved by explicitly constructed secure polar coding schemes in which variations of the polarization between the noisy main channel and the noisy wiretap channel is well designed for obtaining a secure and reliable transmission, which perfectly matches Wyner’s idea of noise based secure coding. However for WTC-II or A-WTC, achieving the secrecy capacity by secure polar coding scheme is much more complicated due to the following problems.

- For A-WTC (WTC-II included), adversarial approaches such as directly reading and rewriting are not channel based, thus secure polar coding is hard to implement directly.
- It is hard to design a passive secure coding scheme which can cover the initiative of the eavesdropper, since the information parts for reading and rewriting can be arbitrarily chosen.

In this paper, we focus on the solving the first problem by exploring an explicit secure polar coding scheme to against the directly reading and rewriting from the eavesdropper in A-WTC. Specifically, our work is set up on a *static A-WTC with noisy discrete memoryless channels* (sA-WTC with DMCs), which assumes that legitimate parties know the exact *eavesdropper behavior state* (EBS, similar as the channel state information, CSI) including the reading part, rewriting part and the transition probability of the main channel. This static assumption is set for removing the initiative of the eavesdropper in A-WTC.

The contributions of our work are as follow:
• We have presented an irregular channel polarization which is the extension of Arıkan’s channel polarization theory. As we proofed, for \( N = 2^n \) and DMCs \( W^{1:N} \) with different transition probabilities, by performing a similar channel combing and channel splitting \((G_N)\), the generated channels are also polarized into full-noise channels and noiseless channels respectively with probabilities \( 1 - A[I(W^{1:N})] \) and \( A[I(W^{1:N})] \) when \( N \to \infty \), similar as the original channel polarization;

• For the directly reading and rewriting in A-WTC, we have presented an equivalent model by replacing the reading and rewriting behaviors with noiseless BECs or full-noise BECs;

• For sA-WTC with DMCs, we have constructed a secure polar coding scheme by applying the irregular polarization to the equivalent model, and achieved the secrecy capacity under the reliability and strong security criterions.

The outline of this paper is as follow. Section 2 introduces the sA-WTC with DMCs and its secrecy capacity achieving problem. Section 3 presents the irregular channel polarization. Section IV presents the equivalent channel model for A-WTC and the construction of irregular secure polar coding scheme on the equivalent channel. Section V concludes the paper.

II. Problem Statement

**Notation:** We define the integer interval \([a,b]\) as the integer set between \(\lfloor a \rfloor\) and \(\lceil b \rceil\). For \(n \in \mathbb{N}\), define \( N \triangleq 2^n \). Denote \( X, Y, Z, \ldots \) random variables (RVs) taking values in alphabets \( \mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots \) and the sample values of these RVs are denoted by \( x, y, z, \ldots \) respectively. Then \( p_{XY} \) denotes the joint probability of \( X \) and \( Y \), and \( p_X, p_Y \) denotes the marginal probabilities. Especially for channel \( W \), the transition probability is defined as \( W_{Y|X} \) and \( W \) for simplicity. Also we denote a \( N \) size vector \( X^{1:N} \triangleq (X^1, X^2, \ldots, X^N) \). When the context makes clear that we are dealing with vectors, we write \( X^N \) in place of \( X^{1:N} \). And for any index set \( A \subseteq [1, N] \), we define \( X^A \triangleq \{X^i\}_{i \in A} \). For the polar codes, we denote \( G_N \) the generator matrix , \( R \) the bit reverse matrix, \( F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \) and \( \otimes \) the Kronecker product, and we have \( G_N = RF^\otimes n \). Denote \( A[\cdot] \) as the average and \( \mathbb{E}[\cdot] \) as the expectation.

Firstly, we introduce the sA-WTC with DMCs.

**Definition 1** The static adversarial wiretap channel with discrete memoryless channels (sA-WTC with DMCs) is defined as \((\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{V}, \mathcal{\tilde{V}}, W_{Y|X}, \tilde{W}_{V|Z}, \rho_r, \rho_w, S_r, S_w)\). The model contains
two symmetric discrete memoryless channels, the main channel $W^N$ and the wiretap channel $\tilde{W}^N$ with block length $N$ and transition probabilities $W_{V|X}, \tilde{W}_{V|\tilde{X}}$ respectively. $X$ is the input alphabet of main channel, $V$ is the output alphabet of main channel and $\tilde{V}$ is the output alphabet of wiretap channel. For all $(x^N, v^N, \tilde{v}^N) \in X \times V \times \tilde{V}$, have

$$W^N(v^{1:N}|x^{1:N}) = \prod_{i=1}^{N} W(v^i|x^i)$$

$$\tilde{W}^N(\tilde{v}^{1:N}|x^{1:N}) = \prod_{i=1}^{N} \tilde{W}(\tilde{v}^i|x^i)$$

(2)

Subset $S_r \subseteq [1, N]$ is the arbitrarily selected index set for reading, satisfies $|S_r| = N\rho_r$. Subset $S_w \subseteq [1, N]$ is the arbitrarily selected index set for rewriting, satisfies $|S_w| = N\rho_w$. According to the static assumption, both $(\rho_r, \rho_w)$ and $(S_r, S_w)$ are known by the legitimate parties when encoding and decoding. Then the rewriting operation is defined as

$$Y^i = \begin{cases} ? & \text{if } i \in S_w \\ V^i & \text{otherwise} \end{cases}$$

(3)

where "?" is the dump letter, $V^N$ is the input of the rewriting operation and $Y^N$ is the output for legitimate receiver with alphabet $Y$. The reading operation is defined as

$$Z^i = \begin{cases} \tilde{V}^i & \text{if } i \in S_r \\ ? & \text{otherwise} \end{cases}$$

(4)

where $Z^N$ is the output for eavesdropper with alphabet $Z$.

As illustrated in Fig. 1 for the sA-WTC with DMCs in Definition [1] have
• Alice: encodes the message $M$ into codewords $X^N$ and transmit it to Bob over the main channel $W^N$ with channel output $V^N$.
• Eve: rewrites the bits of $V^S_w$ into dump letter $? and outputs $Y^N$. Reads the bits of $\bar{V}^S_r$ form wiretap channel $\bar{W}^N$ and fills $\bar{V}^S_c$ with ? to form the observed information $Z^N$.
• Bob: finally receives the transmitted and modified codewords as $Y^N$ and decodes it into estimated information $\hat{M}$.

**Definition 2** For sA-WTC with DMCs, define a $(2^{NR}, N)$ secure code $C_N$, then the performance of $C_N$ can be measured as follow.
• Reliability is measured by error probability $P_e(C_N) = \Pr(M \neq \hat{M})$. And the reliability criterion is defined as $\lim_{N \to \infty} P_e(C_N) = 0$.
• Security is measured by information leakage $L(C_N) = I(Z^N; M)$. And the strong security criterion is defined as $\lim_{N \to \infty} L(C_N) = 0$.

**Theorem 1** (Secrecy capacity) For the A-WTC with DMCs, assuming a uniformly distributed input and $|U| = |X|$, then under the reliability and strong security criterions, the secrecy capacity $C_s$ is upper bounded by

$$C_s = \max_{U \to X \to Y, Z} \left[ (1 - \rho_w)I(U; V) - \rho_r I(U; \bar{V}) \right]$$

(5)

**Proof:** Generally from [16], since the Markov chain $M \to U \to X \to Y, Z$ holds, have

$$C_s = \max_{U \to X \to Y, Z} \left[ I(U; Y) - I(U; Z) \right]$$

(6)

According to [4, Theorem 1], in case $\rho_w = 0$ and $|U| \leq |X|$, the secrecy capacity satisfies

$$C_s = \max_{U \to X \to Y, Z} \left[ I(U; Y) - \rho_r I(U; \bar{V}) \right]$$

(7)

Thus by comparing the effects of the reading and rewriting operations to Eve and Bob, as the corollary for $\rho_w \neq 0$, we can have

$$C_s = \max_{U \to X \to Y, Z} \left[ (1 - \rho_w)I(U; V) - \rho_r I(U; \bar{V}) \right]$$

(8)

Note that this A-WTC with DMCs is a general model for the following particular cases.
• In case $\rho_w = 0$ and $\rho_r = 0$, it turns to the non-degraded WTC with secrecy capacity $\max [I(U; Y) - I(U; Z)]$. 
In case $\rho_w = 0$ with noiseless $W^N$ and $\tilde{W}^N$, it turns to the WTC-II [2] with secrecy capacity $1 - \rho_r$.

- In case $\rho_w = 0$ with noiseless $\tilde{W}^N$, it turns to the extended WTC-II studied in [3] with secrecy capacity $\max \left[ I(U; Y) - \rho_r I(U; \tilde{V}) \right]$.

- In case $\rho_w = 0$ and $W^N = \tilde{W}^N$, it turns to the extended WTC-II studied in [5] with secrecy capacity $\max \left[ I(U; V) (1 - \rho_r) \right]$.

- In case $W^N$ and $\tilde{W}^N$ are noiseless, it turns to the A-WTC studied in [8] with secrecy capacity $1 - \rho_r - \rho_w$ for perfect secrecy.

In this paper, we intend to construct an explicit secure polar coding scheme to achieve the secrecy capacity of the sA-WTC with DMCs under the reliability and strong security criterion, which is an universal secrecy capacity achieving solution for all the listed models under the static assumption.

III. IRREGULAR CHANNEL POLARIZATION

Channel polarization was first introduced by Arıkan in [9]. In his theory, $N = 2^n$ independent copies of channel $W$, the $W^N$, can be polarized into noiseless channels and full-noise channels respectively with probabilities $I(W)$ and $1 - I(W)$ by liner operation $G_N$ when $N$ goes infinity. In this section, we will discuss an irregular case of this channel polarization that replace the $W^N$ with $W^{1:N}$ where $W^i : \mathcal{X} \to \mathcal{Y}$ is independent from others with different $W^i|_X$. Theoretical results of this irregular polarization will be used for constructing the irregular polar coding scheme for sA-WTC with DMCs.

A. Recursive Structure of Irregular Channel Transformation

In the regular polarized channel transformation, the whole combining and splitting operation can be broken recursively into single step $2 \times 2$ kernel transformation, as $(W, W) \mapsto (W^-, W^+)$, where $W^- : \mathcal{X} \to \tilde{\mathcal{Y}}$, $W^+ : \mathcal{X} \to \tilde{\mathcal{Y}} \times \mathcal{X}$ and a one-to-one mapping $f : \mathcal{Y}^2 \to \tilde{\mathcal{Y}}$. Then for irregular channel transformation, we keep the original framework of channel combining and splitting of the polar channel transformation as $G_N$, but just replace the initial channels $W^N$ by $W^{1:N}$ where $W^i : \mathcal{X} \to \mathcal{Y}$ is independent from others with different $W^i|_X$.

**Definition 3** Define the irregular $2 \times 2$ kernel transformation illustrated in Fig. 2b as $(W^1, W^2) \mapsto (W^-, W^+)$ which contains a channel operation pair ($\boxminus$, $\boxplus$) that

$$W^- = W^1 \boxminus W^2 \text{ and } W^+ = W^1 \boxplus W^2$$

(9)
specifically as

\[ W^-(f(y^1, y^2)|u^1) = \sum_{u^2} \frac{1}{2} W^1(y^1|u^1 \oplus u^2) W^2(y^2|u^2) \]

\[ W^+(f(y^1, y^2), u^1|u^2) = \frac{1}{2} W^1(y^1|u^1 \oplus u^2) W^2(y^2|u^2) \]  

(11)

Then we perform the irregular 2 × 2 kernel transformation \((W^1, W^2) \leftrightarrow (W^-, W^+)\) to the \(N\) initial channels \(W^{1:N}\) recursively and describe the structure of the irregular transformation for generating the \(W^{(1:N)}_N\).

**Proposition 1** (Irregular the recursive structure) consider \(N\) independent initial B-DMC \(W^{1:N}\) with \(N = 2^n\), for all \(q \in [0, n - 1]\), \(Q = 2^q\), \(k \in [0, \frac{N}{2Q} - 1]\) and \(i \in [2kQ + 1, 2kQ + Q]\), by applying the irregular 2 × 2 kernel in Def. 3 we have the recursive channel transformation as

\[(W_Q^{(i)}, W_Q^{(i+Q)}) \leftrightarrow (W_{2Q}^{(2i-2kQ-1)}, W_{2Q}^{(2i-2kQ)})\]  

(12)

where

\[ W_{2Q}^{(2i-2kQ-1)} = W_Q^{(i)} \Box W_Q^{(i+Q)} \]

\[ W_{2Q}^{(2i-2kQ)} = W_Q^{(i)} \Box W_Q^{(i+Q)} \]  

(14)

specifically as

\[ W_{2Q}^{(2i-2kQ-1)}(y^{2kQ+1:2kQ+2Q}, u^{2kQ+1:2i-2kQ-2}|u^{2i-2kQ-1}) \]

\[ = \sum_{u^{2i-2kQ}} \frac{1}{2} W_Q^{(i)}(y^{2kQ+1:2kQ+Q}, u_e^{2kQ+1:2i-2kQ-2} \oplus u_e^{2kQ+1:2i-2kQ-2}|u^{2i-2kQ-1} \oplus u^{2i-2kQ}) \]  

(16)

\[ \cdot W_Q^{(i+Q)}(y^{2kQ+Q+1:2kQ+2Q}, u_e^{2kQ+1:2i-2kQ-2}|u^{2i-2kQ}) \]

and

\[ W_{2Q}^{(2i-2kQ)}(y^{2kQ+1:2kQ+2Q}, u^{2kQ+1:2i-2kQ-1}|u^{2i-2kQ}) \]

\[ = \frac{1}{2} W_Q^{(i)}(y^{2kQ+1:2kQ+Q}, u_e^{2kQ+1:2i-2kQ-2} \oplus u_e^{2kQ+1:2i-2kQ-2}|u^{2i-2kQ-1} \oplus u^{2i-2kQ}) \]  

(18)

\[ \cdot W_Q^{(i+Q)}(y^{2kQ+Q+1:2kQ+2Q}, u_e^{2kQ+1:2i-2kQ-2}|u^{2i-2kQ}) \]
where \( u_o \) refers to odd term and \( u_e \) refers to even term.

The recursive relation of irregular transformation in Prop. 1 is illustrated in Fig. 3 with \( N = 8 \).

\[
\begin{align*}
W_8^{(1)} & \quad W_8^{(1)} & \quad W_8^{(1)} & \quad W_1^1 \\
W_8^{(2)} & \quad W_8^{(3)} & \quad W_2^2 & \\
W_8^{(5)} & \quad W_3^3 & \quad W_5^5 & \\
W_8^{(6)} & \quad W_6^6 & \quad W_6^6 & \\
W_8^{(7)} & \quad W_7^7 & \quad W_7^7 & \\
W_8^{(8)} & \quad W_8^{(8)} & \quad W_8^{(8)} & \\
\end{align*}
\]

Fig. 3. The irregular channel transformation process with \( W^{1:N}, N = 8 \)

Since \( G_N \) remains unchanged for irregular channel transformation, for all \( y^{1:N} \in \mathcal{Y}^N, u^{1:N} \in \mathcal{X}^N \), the relations of transition probabilities between \( W_N \) and \( W^{1:N} \) is

\[
W_N(y^{1:N}|u^{1:N}) = W^{1:N}(y^{1:N}|u^{1:N}G_N)
\]

which is the same formation as the regular channel polarization.

**Definition 4** ([9]) For any given B-DMC \( W : \mathcal{X} \rightarrow \mathcal{Y} \), the Bhattacharyya parameter is defined as

\[
Z(W) \triangleq \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}
\]

which satisfies

\[
\log \frac{2}{1 + Z(W)} \leq I(W) \leq \sqrt{1 - Z(W)^2}
\]

where \( I(W) \) refers to the capacity of the channel \( W \). Specially for BEC, have \( I(W) = 1 - Z(W) \).

**Proposition 2** For irregular \( 2 \times 2 \) kernel transformation \((W^1, W^2) \mapsto (W^-, W^+)\), have

\[
I(W^-) + I(W^+) = I(W^1) + I(W^2)
\]
Proof: Note that $I(W^-) = I(U^1; Y^1 Y^2)$ and $I(W^+) = I(U^2; Y^1 Y^2 U^1)$, thus have

$$I(W^-) + I(W^+) = I(U^1; Y^1 Y^2) + I(U^2; Y^1 Y^2 U^1)$$

$\overset{(a)}{=} I(U^1; Y^1 Y^2) + I(U^2; Y^1 Y^2 | U^1)$

$$= I(U^1 U^2; Y^1 Y^2)$$

$$= I(U^1; Y^1) + I(U^2; Y^2)$$

$$= I(W^1) + I(W^2)$$

where $(a)$ is due to $U^1$ and $U^2$ are independent.

Proposition 3 For irregular $2 \times 2$ kernel transformation $(W^1, W^2) \mapsto (W^-, W^+)$, have

$$Z(W^+) = Z(W^1) Z(W^2)$$

$$Z(W^-) \leq Z(W^1) + Z(W^2) - Z(W^1) Z(W^2)$$

And the second equal holds when $W^1$, $W^2$ are BEC.

Proof: See Appendix A

B. Irregular Channels Polarization

As a corollary to Prop. 3, for BEC case, since $I(W) = 1 - Z(W)$, have

$$I(W^-) = I(W^1) I(W^2)$$

$$I(W^+) = I(W^1) + I(W^2) - I(W^1) I(W^2)$$

By extending this recursion to BECs $W^{1:N}$, for all $q \in [0, n - 1]$, $Q = 2^q$, $k \in [0, \frac{N}{2Q} - 1]$ and $i \in [2kQ + 1, 2kQ + Q]$, have

$$I(W_{2Q}^{(2i-2kQ-1)}) = I(W_Q^{(i)}) I(W_Q^{(i+Q)})$$

$$I(W_{2Q}^{(2i-2kQ)}) = I(W_Q^{(i)}) + I(W_Q^{(i+Q)}) - I(W_Q^{(i)}) I(W_Q^{(i+Q)})$$

From (31), for BEC case, we can recursively compute the $I(W_{N}^{(1:N)})$ from the initial $I(W_{1:N}^{1})$ for the irregular channel transformation with operation $G_N$. As illustrated in Fig. 4 for the result of irregular channel transformation of $I(W_{N}^{(1:N)})$ with $N = 2^{10}$, the $I(W_{N}^{(1:N)})$ recursively computed form $I(W_{1:N}^{1})$ have a similar polarization effect as the regular polarized channel transformation by using the operation $G_N$ on $W^N$. For original channel polarization of the $N$ independent copy of any B-DMC $W$ in [9], have

$$I_{\infty} = \begin{cases} 1 & \text{w.p. } I(W) \\ 0 & \text{w.p. } 1 - I(W) \end{cases}$$
so there may be a similar polarization formation for irregular channel transformation of any
B-DMCs $W^{1:N}$. Now we discuss the polarization of the irregular channel transformation.

**Proposition 4** *(Irregular channel polarization)* for any B-DMC $W^{1:N}$ with different transition
probabilities, the generated channels $W_i^N$ form irregular channel transformation $G_N$ are polar-
ized in the sense that, for any fixed $\delta \in (0, 1)$, as $N \rightarrow \infty$, the fraction of indices $i \in [1, N]$ for
which $I(W_i^N) \in (1 - \delta, 1]$ goes to $\mathbb{A}[I(W^{1:N})]$ and the fraction for which $I(W_i^N) \in [0, \delta)$ goes
to $1 - \mathbb{A}[I(W^{1:N})]$. Also can be write as

$$I_\infty = \begin{cases} 1 & \text{w.p. } \mathbb{A}[I(W^{1:N})] \\ 0 & \text{w.p. } 1 - \mathbb{A}[I(W^{1:N})] \end{cases}$$  \hspace{1cm} (33)

where $\mathbb{A}[I(W^{1:N})]$ is the average of the initial $I(W^i)$ for all the $i \in [1, N]$.

Now we proof the Prop. 4 by extending the proof work of [9, Section IV]. Consider a multi-
channel stochastic process of the irregular channel transformation as in Fig. 5, with $N = 2^n,
q \in [0, n - 1]$, $Q = 2^q$ and $k \in [0, \frac{N}{2Q} - 1]$. Assume that $n \rightarrow \infty$ in case of $q \rightarrow \infty$. For the
random channel process from level $q$ to $q + 1$, 0 refers the move to the upper node at level
$q + 1$ and 1 refers the move to the lower node both with probability $1/2$. Initially at level 0,
we have $W^{1:N}$. Define a sequence $b_1b_2...b_\theta$ as the random path for $W^{1:N}$ all together from level

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig4}
\caption{Polarization of $I(W_i^N)$ with $N = 2^{10}$ for irregular channel transformation. $W_N^{(1:N)}$ are transformed from $N$ independent BECs $W^{1:N}$ with random and different erase probabilities.}
\end{figure}
0 to level \( q \), which means all the channels take the same random moves. Also note that for \( i \in [2kQ + 1, 2kQ + 2Q] \), all the \( W^i \) will move to a same node under a same \( q \)-steps random path. For example, in Fig. 5, with the path 000, every channel of \( W^{1:8} \) will moves to \( W_{8}^{(1)} \). Also, we write \( W_{b_1b_2...b_q}^{1:N} \) as the locate of the channels move by the path \( b_1b_2...b_q \).

Consider the probability space \((\Omega, \mathbb{F}, P)\), where \( \Omega \) is the space for \((b_1, b_2, ...) \in \{0, 1\}^\infty \), \( \mathbb{F} \) is the Borel field (BF) generated by \( S(b_1, ..., b^q) \equiv \{ \omega \in \Omega : \omega^1 = b_1, ..., \omega^q = b^q \} \), and \( P \) is the probability measure defined on \( \mathbb{F} \) that \( P(S(b_1, ..., b^q)) = 1/2^q \). Then have \( \mathbb{F}^0 \subset \mathbb{F}^1 \subset ... \subset \mathbb{F}^q \). Further, denote \( K_q^{1:N} = W_{b_1b_2...b_q}^{1:N} \) as the value of the multi channel stochastic process that \( K_q^{1:N} = W_{b_1b_2...b_q}^{1:N} \). Denote i.i.d. RVs \( \{B_q; q = 1, 2, ...\} \) that \( B^{1:q} \) takes on the sample value \( b_1, ..., b^q \). Thus formally the multi channel stochastic process can be defined as follow. For \( \omega = (\omega^1, \omega^2, ...) \in \Omega \) and \( q \geq 1 \), define \( B^q(\omega) = \omega^q, K_q^{1:N}(\omega) = W_{\omega^1...\omega^q}^{1:N}, A[I_q^{1:N}(\omega)] = A[I^{1:N}(K_q^{1:N}(\omega))] \), \( A[Z_q^{1:N}(\omega)] = A[Z^{1:N}(K_q^{1:N}(\omega))] \). For \( q = 0 \), define \( K_0^{1:N} = W^{1:N}, A[I_0^{1:N}] = A[I(W^{1:N})] \), \( A[Z_0^{1:N}] = A[Z(W^{1:N})] \). For any fixed \( q \geq 0 \), \( B^q, K_q^{1:N}, A[I_q^{1:N}] \) and \( A[Z_q^{1:N}] \) are measurable with respect to the BF \( \mathbb{F} \).

Note that in the multi channel stochastic process, all the channels \( W^{1:N} \) are taking a same path, thus at level \( n \), all the \( W^{1:N} \) will move to a same node. So we have

\[
A[I_\infty^{1:N}] = I_\infty \quad \text{and} \quad A[Z_\infty^{1:N}] = Z_\infty
\]  

(34)
Consider the following expectation

\[ E \left[ A\left[I_{q+1}^{1:N}\right]|S(b^1, \ldots, b^q) \right] = \frac{1}{N} \sum_{i=1}^{N} \left[ \frac{1}{2} I(W_{b_i}^{i}, \ldots, b^q) + \frac{1}{2} I(W_{b_i}^{i}, \ldots, b^q) \right] \]

\[ = \frac{(a)}{N} \sum_{i=1}^{N} I(W_{b_i}^{i}, \ldots, b^q) \]

\[ = A[I_{q}^{1:N}] \quad (36) \]

where \((a)\) is due to Prop. 2 and all the \(W_i\) take the same path. Thus we have martingale \(\{A[I_{q}^{1:N}], \mathcal{F}^q; q \geq 0\}\) as

\[ \mathcal{F}^q \subset \mathcal{F}^{q+1} \text{ and } A[I_{q}^{1:N}] \text{ is } \mathcal{F}^q\text{-measurable} \]

\[ E \left[ |A[I_{q}^{1:N}]| \right] < \infty \quad (38) \]

\[ A[I_{q}^{1:N}] = E \left[ A[I_{q+1}^{1:N}]|\mathcal{F}^q \right] \]

So have

\[ E[I_\infty] = E \left[ A[I_\infty] \right] = A[I_0^{1:N}] \quad (39) \]

Similarly for expectation

\[ E \left[ A[Z_{q+1}^{1:N}]|S(b^1, \ldots, b^q) \right] = \frac{1}{N} \sum_{i=1}^{N} \left[ \frac{1}{2} Z(W_{b_i}^{i}, \ldots, b^q) + \frac{1}{2} Z(W_{b_i}^{i}, \ldots, b^q) \right] \]

\[ \leq \frac{(a)}{N} \sum_{i=1}^{N} Z(W_{b_i}^{i}, \ldots, b^q) \]

\[ = A[Z_{q}^{1:N}] \quad (41) \]

where \((a)\) is due to Prop. 3 and all the \(W_i\) take the same path. Thus we have supermartingale \(\{A[Z_{q}^{1:N}], \mathcal{F}^q; q \geq 0\}\) as

\[ \mathcal{F}^q \subset \mathcal{F}^{q+1} \text{ and } A[Z_{q}^{1:N}] \text{ is } \mathcal{F}^q\text{-measurable} \]

\[ E \left[ |A[Z_{q}^{1:N}]| \right] < \infty \quad (43) \]

\[ A[Z_{q}^{1:N}] \geq E \left[ A[Z_{q+1}^{1:N}]|\mathcal{F}^q \right] \]

So it converges a.e. and in \(L^1\) to a RV \(A[Z_\infty^{1:N}]\) such that

\[ E \left[ |A[Z_{q}^{1:N}] - A[Z_\infty^{1:N}]| \right] \rightarrow \infty \quad (44) \]
followed with $\mathbb{E} \left[ |\mathbb{A}[Z_{q+1}^{1:N}] - \mathbb{A}[Z_q^{1:N}]| \right] \rightarrow \infty$. From Prop. 3 have that for connected $i, j \in [1, N]$, exists $i' \in [1, N]$ that $Z_{q+1}^j = Z_q^i Z_q^{i'}$ with probability $1/2$ in the multi channel stochastic process. Besides, note that

$$
\mathbb{A}[Z_q^{1:N} Z_q^{1:N'}] = \frac{1}{N} \sum_{i=1}^{N} Z_q^i Z_q^{i'}
$$

\begin{equation}
\leq \sqrt{\frac{1}{N} \sum_{i=1}^{N} (Z_q^i)^2 \cdot \frac{1}{N} \sum_{i'=1}^{N} (Z_q^{i'})^2}
\end{equation}

\begin{equation}
= \mathbb{A}[(Z_q^{1:N})^2]
\end{equation}

\begin{equation}
\leq \mathbb{A}[Z_q^{1:N}]^2
\end{equation}

where $(a)$ is due to Cauchy’s inequality, and $(b)$ is due to $i$ are symmetric with $i'$ and $Z_q^i, Z_q^{i'} \in Z_q^{1:N}$. Thus have

$$
\mathbb{E} \left[ |\mathbb{A}[Z_{q+1}^{1:N}] - \mathbb{A}[Z_q^{1:N}]| \right] = \mathbb{E} \left[ \frac{1}{N} \sum_{i=1}^{N} Z_{q+1}^i - \sum_{i=1}^{N} Z_q^i \right]
$$

$$
= \mathbb{E} \left[ \frac{1}{N} \sum_{i=1}^{N} |Z_{q+1}^i - Z_q^i| \right]
$$

$$
\geq \frac{1}{2} \mathbb{E} \left[ \frac{1}{N} \sum_{i=1}^{N} |Z_q^i Z_q^{i'} - Z_q^i| \right]
$$

$$
= \frac{1}{2} \mathbb{E} \left[ \mathbb{A}[Z_q^{1:N}] - \mathbb{A}[Z_q^{1:N} Z_q^{1:N'}] \right]
$$

$$
\geq \frac{1}{2} \mathbb{E} \left[ \mathbb{A}[Z_q^{1:N}] - \mathbb{A}[Z_q^{1:N}]^2 \right]
$$

$$
= \frac{1}{2} \mathbb{E} \left[ \mathbb{A}[Z_q^{1:N}](1 - \mathbb{A}[Z_q^{1:N}]) \right] \geq 0
$$

where $(a)$ is due (46). Since when $q \rightarrow \infty$, $Z_q^{1:N} \rightarrow Z_\infty$, have $\mathbb{E} \left[ (1 - Z_\infty) Z_\infty \right] = 0$, which means that $Z_\infty$ equals 0 or 1. Form Def. 4 have $I_\infty = 1 - Z_\infty$. Therefore, form $I_\infty = \mathbb{E}[I_\infty] = \mathbb{A}[I_0^{1:N}]$, easy to have

$$
I_\infty = \begin{cases} 
1, \text{ w.p. } \mathbb{A}[I_0^{1:N}] \\
0, \text{ w.p. } 1 - \mathbb{A}[I_0^{1:N}] 
\end{cases}
$$

which completes the proof of Prop. 4.
C. Rate of Irregular Polarization

**Proposition 5** For any B-DMC $W^{1:N}$ with $I(W^i) > 0$, and any fixed $R < A[I(W^{1:N})]$ and constant $\beta \leq 1/2$, there exists index set $A_N \subset [1, N]$, $|A_N| \leq NR$ that

$$\sum_{i \in A_N} Z(W_N^{(i)}) = o(2^{-N\beta}) \quad (50)$$

and

$$P_e(N, R) = o(2^{-N\beta}) \quad (51)$$

For regular channel polarization, its bounded rate has been rigorously proofed in [17]. Fortunately, this piner work can also be adapted for proofing the Prop. 5 by making a few modifications based on the multi channel stochastic process. Note that from Def. 4, we can have

$$I(W)^2 + Z(W)^2 \leq 1$$

and

$$I(W) + Z(W) \geq 1 \quad (52)$$

Thus from Prop. 4, we have

$$Z_\infty = \begin{cases} 0 & \text{w.p. } A[I_0^{1:N}] \\ 1 & \text{w.p. } 1 - A[I_0^{1:N}] \end{cases} \quad (53)$$

For [17], Section II, Def. 1, we redefine $\tilde{\mathcal{Z}}_{z_0}$ as the class of random process \{A[Z_q^{1:N}] : q = 0, 1, ...\} with $A[Z_0^{1:N}] = z_0 \in (0, 1)$. $A[Z_q^{1:N}]$ is measurable with respect to $\mathcal{F}_q$ and satisfies

$$A[Z_{q+1}^{1:N}] = A[Z_q^{1:N} Z_{q'}^{1:N'}] \text{ if } B_{q+1} = 1$$

$$A[Z_{q+1}^{1:N}] \in \left[ A[Z_q^{1:N}], 2A[Z_q^{1:N}] - A[Z_q^{1:N} Z_{q'}^{1:N'}] \right] \text{ if } B_{q+1} = 0 \quad (55)$$

by noting that $0 < A[Z_q^{1:N}] = A[Z_q^{1:N'}] < 1$ with $z_0 \in (0, 1)$. Let $\tilde{\mathcal{Z}} := \bigcup_{z_0 \in (0, 1)} \tilde{\mathcal{Z}}_{z_0}$. Since $A[Z_q^{1:N}] \leq 2A[Z_q^{1:N}] - A[Z_q^{1:N} Z_{q'}^{1:N'}]$, combining with (41), we have that \{A[Z_q^{1:N}], $\mathcal{F}_q$, $q \geq 0$\} of (55) is a bounded supermartingale and it converges a. e. and $L^1$ to RV $A[Z_\infty^{1:N}]$.

For [17], Section IV, Def. 3, we redefine the extremal process \{A[Z_q^{1:N}]\} in $\tilde{\mathcal{Z}}$ as

$$A[Z_{q+1}^{1:N}] = \begin{cases} A[Z_q^{1:N} Z_{q'}^{1:N'}] & \text{if } B_{q+1} = 1 \\ 2A[Z_q^{1:N}] - A[Z_q^{1:N} Z_{q'}^{1:N'}] & \text{if } B_{q+1} = 0 \end{cases} \quad (56)$$

Note that $A[Z_q^{1:N} Z_{q'}^{1:N'}] \leq A[Z_q^{1:N} Z]^2$ from (46) and $2A[Z_q^{1:N}] - A[Z_q^{1:N} Z_{q'}^{1:N'}] \geq 2A[Z_q^{1:N}] - A[Z_q^{1:N} Z]^2$. Thus extremal process \{A[Z_q^{1:N}]\} also satisfies

- Extremal \{A[Z_q^{1:N}]\} is a Markov process;
- Extremal \{A[Z_q^{1:N}]\} is a bounded martingale according to (41);
\[ P(Z_\infty = 0) = A[Z_0^{1:N}] \text{ and } P(Z_\infty = 1) = 1 - A[Z_0^{1:N}]; \]

\[ \{A[Z_q^{1:N}]\} \in \tilde{Z}_{\alpha_0} \text{ is dominated by } \{A[Z_q^{1:N}]\{z_0\}\}, \{A[Z_q^{1:N}]\{\alpha\}\} \text{ is dominated by } \{A[Z_q^{1:N}]\{\beta\}\} \]

for all \( 0 < \alpha \leq \beta < 1. \)

Note that \( \{A[Z_q^{1:N}]\{z_0\}\} \) refers to the extremal \( \{A[Z_q^{1:N}]\} \) process, and the dominating relationship, including the asymptotically dominating (a.d.), universally dominating (u.d.) and the sequence \( \{f_q\} \subset [0, 1] \), all follow the definition in [17, Section IV, Def. 2]. Thus we can have that

\[ \liminf_{q \to \infty} P(A[Z_q^{1:N}] \leq f_q) \geq P(Z_\infty = 0) \tag{57} \]

form [17, Section IV, Prop. 1].

For [17, Section IV-C], consider a modified construction of \( \tilde{Q}_q \). Fix an extremal \( \{A[Z_q^{1:N}]\} \) process with \( A[Z_0^{1:N}] = z_0 \) for \( z_0 \in (0, 1) \). It is easy to proof that \( \{A[Z_q^{1:N}]\} \in (0, 1) \). Then let \( \tilde{Q}_q := A[Z_q^{1:N}](1 - A[Z_q^{1:N}]) \), then have \( \tilde{Q}_q \in (0, 1/4] \). Thus from (56), have

\[ \tilde{Q}_{q+1} = \begin{cases} A[Z_q^{1:N}Z_q^{1:N'}](1 - A[Z_q^{1:N}Z_q^{1:N'}]) & \text{if } B_{q+1} = 1 \\ (2A[Z_q^{1:N}] - A[Z_q^{1:N}Z_q^{1:N'}])(1 - 2A[Z_q^{1:N}] + A[Z_q^{1:N}Z_q^{1:N'}]) & \text{if } B_{q+1} = 0 \end{cases} \tag{58} \]

Let

\[ \zeta = \frac{\sqrt{(\tilde{Q}_{q+1}|B_{q+1} = 1 \tilde{Q}_q)}}{\sqrt{\tilde{Q}_q}} + \frac{\sqrt{(\tilde{Q}_{q+1}|B_{q+1} = 0 \tilde{Q}_q)}}{\sqrt{\tilde{Q}_q}} \tag{59} \]

and \( a = A[Z_q^{1:N}], b = A[Z_q^{1:N}Z_q^{1:N'}], \) thus

\[ \zeta = \sqrt{\frac{b(1-b)}{a(1-a)}} + \sqrt{\frac{(2a-b)(1-2a+b)}{a(1-a)}} \]

\[ \leq \sqrt{\left[ \sqrt{b(1-b)^2} + \sqrt{(2a-b)(1-2a+b)} \right]^2} \cdot \left[ \sqrt{\frac{1}{a(1-a)}} + \sqrt{\frac{1}{a(1-a)}} \right] \tag{61} \]

\[ = 2 \sqrt{1 - \frac{(a-b)^2}{a(1-a)}} \]

where \( (a) \) is due to Cauchy’s inequality. It is easy to proof that \( A[Z_q^{1:N}] = A[Z_q^{1:N}Z_q^{1:N'}] \) only when they equal to 0 or 1. Hence from \( \{A[Z_q^{1:N}]\} \in (0, 1) \), have \( \zeta < 2 \). Thus we obtain

\[ \mathbb{E}[\tilde{Q}_q^{1/2}] \leq \frac{1}{2} \left( \frac{\zeta^2}{4^q} \right)^{1/2} \]

and then

\[ P(\tilde{Q}_q \geq \rho^q) \leq \frac{1}{2} \left( \frac{\zeta^2}{4^q} \right)^{1/2} \tag{62} \]

by Markov’s inequality. Therefore, we can have that for any \( \rho \in \left( \frac{\zeta^2}{4^q}, 1 \right) \), sequence \( \{\rho^q\} \) is a.d. over the class of extremal \( \{A[Z_q^{1:N}]\} \) process, according to [17, Section IV, Prop. 2].
For [17, Section IV-D], fix an extremal \( \{A[Z_1^N]\} \) process and another process \( \{A[\bar{Z}_i^1:N]\} \) with \( m \in [0, q] \) that
\[
A[\bar{Z}_i^1] = A[Z_i^1], \quad \text{for } i \in [0, m]
\]
and
\[
A[\bar{Z}_{i+1}^1] = \begin{cases} 
A[\bar{Z}_i^1:Z_{i+1}^N] & \text{if } B_{i+1} = 1 \\
2A[\bar{Z}_i^1] & \text{if } B_{i+1} = 0 
\end{cases} \quad \text{for } i \geq m
\]
(63)
Note that it also satisfies \( A[\bar{Z}_i^1:N] \geq A[Z_i^1:N] \). Thus from [17, Section IV, Prop. 3], by combining all the modifications presented above, we can finally have that for any \( \beta < 1/2 \), the sequence \( \{2^{-2n\beta}\} \) is u.d. over the class of extremal \( \{A[Z_q^1:N]\} \) process. Hence,
\[
\liminf_{q \to \infty} P(A[Z_q^1:N] \leq 2^{-2n\beta}) = \liminf_{n \to \infty} P(Z_n \leq 2^{-N\beta}) = A[I_0^1:N]
\]
(65)
and \( P_e(N, R) = o(2^{-N\beta}) \), which completes the proof of Prop. 5.

IV. Irregular Polar Coding for sA-WTC with DMC

In this section, we continue on the work of achieving the secrecy capacity of sA-WTC with DMCs explicitly by applying the results of irregular polarization.

A. Equivalent Models for sA-WTC with DMC

The aim of building the equivalent models is to find a channel-form expression for the directly reading the rewriting operation of eavesdropper, so that we can perform the polar codes for constructing the secure coding schemes. For both directly reading or writing on a single transmitted bit, the effects of these adversarial operations are the same as single bit BEC with \( \epsilon = 0 \) or \( \epsilon = 1 \).

**Definition 5** Define \( \otimes \) as the channel cascading operation, for instance \( W^1 = W^2 \otimes W^3 \). Define two single bit BECs \( W_{\epsilon 0} \) and \( W_{\epsilon 1} \) with same input alphabet \( \{0, 1\} \) and same output alphabet \( \{0, 1, ?\} \), satisfying that erase probability \( \epsilon = 0 \) for \( W_{\epsilon 0} \) and \( \epsilon = 1 \) for \( W_{\epsilon 1} \).

Then the equivalent channels can be constructed as follow.

- Denote DMCs \( W_i^{1:N} : \mathcal{X}^N \to \mathcal{V}^N \to \mathcal{Y}^N \) as the equivalent main channels for directly rewriting, for \( i \in [1, N] \), have
\[
W_i^w = \begin{cases} 
W \otimes W_{\epsilon 1} : W_i^w(y|x) = \sum_{v \in \mathcal{Y}} W(v|x)W_{\epsilon 1}(y|v) & \text{if } i \in S_w \\
W \otimes W_{\epsilon 0} : W_i^w(y|x) = \sum_{v \in \mathcal{Y}} W(v|x)W_{\epsilon 0}(y|v) & \text{otherwise}
\end{cases}
\]
(66)
and \( C(W_{\text{w}}^{1:N}) = (1 - \rho_{\text{w}})NC(W) \).

- Denote DMCs \( W_{\text{r}}^{1:N} : X^{N} \rightarrow Y^{N} \rightarrow Z^{N} \) as the equivalent wiretap channels of directly reading, for \( i \in [1, N] \), have
  \[
  W_{i}^{\text{r}} = \begin{cases} 
  \tilde{W}[W_{i}^{0}(z|x) = \sum_{\tilde{v} \in \tilde{V}} \tilde{W}(\tilde{v}|x)W_{i}^{0}(z|\tilde{v}) & \text{if } i \in S_{\text{r}} \\
  \tilde{W}[W_{i}^{1}(z|x) = \sum_{\tilde{v} \in \tilde{V}} \tilde{W}(\tilde{v}|x)W_{i}^{1}(z|\tilde{v}) & \text{otherwise}
  \end{cases}
  \tag{67}
  \]
  and \( C(W_{\text{r}}^{1:N}) = \rho_{\text{r}}NC(\tilde{W}) \).

- For special case that \( W_{\text{w}}^{N} \) and \( \tilde{W}_{\text{w}}^{N} \) are noiseless, \( i \in [1, N] \), have
  \[
  W_{i}^{\text{w}} = \begin{cases} 
  W_{i}^{0} : W_{i}^{0}(y|x) = 1 & \text{if } i \in S_{\text{w}} \\
  W_{i}^{1} : W_{i}^{1}(y|x) = 0 & \text{otherwise}
  \end{cases}
  \tag{68}
  \]
  \[
  W_{i}^{r} = \begin{cases} 
  W_{i}^{0} : W_{i}^{0}(z|x) = 1 & \text{if } i \in S_{\text{r}} \\
  W_{i}^{1} : W_{i}^{1}(z|x) = 0 & \text{otherwise}
  \end{cases}
  \tag{69}
  \]
  Since \( W_{\text{w}}^{N} \), \( \tilde{W}_{\text{w}}^{N} \), \( W_{\text{w}}^{0} \) and \( W_{\text{w}}^{1} \) are symmetric, the constructed equivalent channels \( W_{\text{w}}^{1:N} \) and \( W_{\text{r}}^{1:N} \) are also symmetric.

B. Irregular Polarization of Equivalent Channels

Now apply the irregular polarization to the constructed equivalent channels.

For \( W_{\text{w}}^{1:N} \), \( \rho_{\text{w}} \) fraction of channels equal to \( W_{\text{w}}^{0} \), and \( 1 - \rho_{\text{w}} \) fraction of channels equal to \( W_{\text{w}}^{1} \). For \( \beta < 1/2 \), \( \delta_{N} = 2^{-N^{3/2}} \), the irregularly polarized index sets of \([1, N]\) are
  \[
  \mathcal{H}_{W_{\text{w}}} = \{i \in [1, N] : Z(W_{\text{w}}^{(i)}) \geq 1 - \delta_{N}\}
  \]
  \[
  \mathcal{L}_{W_{\text{w}}} = \{i \in [1, N] : Z(W_{\text{w}}^{(i)}) \leq \delta_{N}\}
  \tag{71}
  \]
  where \( \mathcal{H}_{W_{\text{w}}} \) is the polarized full-noise index set for Bob, and \( \mathcal{L}_{W_{\text{w}}} \) is the polarized noiseless index set for Bob.

Similarly for \( W_{\text{r}}^{1:N} \), \( \rho_{\text{r}} \) fraction of channels equal to \( \tilde{W} \), and \( 1 - \rho_{\text{r}} \) fraction of channels equal to \( W_{\text{r}}^{1} \). By applying the irregular channel polarization, for \( \beta < 1/2 \), \( \delta_{N} = 2^{-N^{3/2}} \), the polarized index sets of \([1, N]\) are
  \[
  \mathcal{H}_{W_{\text{r}}} = \{i \in [1, N] : Z(W_{\text{r}}^{(i)}) \geq 1 - \delta_{N}\}
  \]
  \[
  \mathcal{L}_{W_{\text{r}}} = \{i \in [1, N] : Z(W_{\text{r}}^{(i)}) \leq \delta_{N}\}
  \tag{73}
  \]
where $H_W$ is the polarized full-noise index set for Eve, and $L_W$ is the polarized noiseless index set for Eve.

Note for the case that $W^N$ and $\tilde{W}^N$ are noiseless (the basic A-WTC), $Z(W^i_w)$ is either 0 with fraction $1 - \rho_w$ or 1 with fraction $\rho_w$, and $Z(W^i_r)$ is either 0 with fraction $\rho_r$ or 1 with fraction $1 - \rho_r$, so for the recursion process of $Z(W^i_w)$ and $Z(W^i_r)$, there are only three possible cases $(1,1) \mapsto (1,1)$, $(1,0) \mapsto (1,0)$ and $(0,0) \mapsto (0,0)$. Thus for the generated $W^{(1:N)}_w$ and $W^{(1:N)}_r$, the proportion of $Z(W^{(i)}_{wN}) = 1$ remains $\rho_w$ and $Z(W^{(i)}_{rN}) = 0$ remains $1 - \rho_w$, the proportion of $Z(W^{(i)}_{rN}) = 1$ remains $1 - \rho_r$ and $Z(W^{(i)}_{rN}) = 0$ remains $\rho_r$. Thus for irregular channel polarization, the polarized index sets of $[1:N]$ are

$$H_{W_w} = \{i \in [1,N] : Z(W^{(i)}_{wN}) = 1\}$$

$$L_{W_w} = \{i \in [1,N] : Z(W^{(i)}_{wN}) = 0\}$$

and

$$H_{W_r} = \{i \in [1,N] : Z(W^{(i)}_{rN}) = 1\}$$

$$L_{W_r} = \{i \in [1,N] : Z(W^{(i)}_{rN}) = 0\}$$

C. Secure Polar Coding Scheme

Owing to the irregularly polarized index sets of equivalent channels, now we can directly apply the structure of strong security achieving coding in [11] (the multi-block chaining structure) to the sA-WTC with DMCs.

Let $(I, R, F, B)$ be a subsets partition of index $[1,N]$, satisfies

$$I = L_{W_w} \cap H_{W_r}$$

$$F = (L_{W_w})^c \cap H_{W_r}$$

$$R = L_{W_w} \cap (H_{W_r})^c$$

$$B = (L_{W_w})^c \cap (H_{W_r})^c$$

(79)

Then considering a $T$ times $N$-length block transmission over the sA-WTC with DMC, for each $t \in [1,T]$, eavesdropper Eve can arbitrarily choose the reading set $S^t_r$ and the rewriting set $S^t_w$ under the constrains of fixed $\rho_r$ and $\rho_w$. Because of the static assumption, we assume that legitimate parties know both $S^t_r$ and $S^t_w$ at the beginning of first transmission. Thus, based on the differently chosen $S^t_r$ and $S^t_w$, legitimate parties can have $(I^t, R^t, F^t, B^t)$ for each $t$. Further, sperate an $E^t$ from $I^t$ that $E^t \subset I^t$ and satisfies $|E^t| = |B^{t+1}|$. Then we can have the encoding
and decoding process of strong security achieving coding scheme for sA-WTC with DMC as follow.

- **Encoding:**
  - Assigning the $u^N$: $\mathcal{T} \setminus \mathcal{E}^t$ is assigned with information bits (uniform message bits); $\mathcal{F}^t$ is assigned with frozen bits; $\mathcal{R}^t$ and $\mathcal{E}^t$ are assigned with uniformly distributed random bits; $\mathcal{B}^t$ is assigned with pre-shared bits for $t = 1$ or with bits of $\mathcal{E}^{t-1}$ for $t > 1$.
  - Encode $u^{1:N}$ to channel input $x^{1:N}$ by irregular polar coding $x^{1:N} = u^{1:N}G_N$ and transmitted to Bob over the main channel $W^N$.

- **Decoding:**
  - Bob receives $y^{1:N}$ as the rewritten channel output from main channel.
  - For $i \in \mathcal{T} \cup \mathcal{R}^t$, $\hat{u}^i$ is decoded by the SC decoding as
    $$\hat{u}^i = \arg \max_{u \in \{0, 1\}} W^{(i)}_{u^{1:N}}(u|\hat{u}^{1:i-1}, y^{1:N})$$
  - For $i \in \mathcal{F}^t$, $\hat{u}^i$ is decoded as frozen bit.
  - For $i \in \mathcal{B}^t$, $\hat{u}^i$ is decoded as the pre-shared bit in case $t = 1$ or as the correspondent bit of $\hat{u}^{\mathcal{E}^{t-1}}$ of the $(t-1)$-th time in case $t > 1$.

  Note that for eavesdropper Eve, she directly reads $\tilde{v}^S$ from the wiretap channel $\tilde{W}^N$, and directly rewrites $v^S$ into $\tilde{v}$.

**D. Performance**

Now we discuss the performance of the irregular secure polar coding scheme by reliability, security and achievable secrecy rate.

1) **Reliability:** For each $t \in [1, T]$, information bits and random bits are transmitted by the irregularly polarized subset $\mathcal{R}^t \cup \mathcal{I}^t = \mathcal{L}_{W_w}^t$. Note that $|\mathcal{L}_{W_w}^t| = NP(Z(W^{(i)}_{w^N}) \leq \delta_N)$ by (71). From Prop. 4, have $P(Z(W^{(i)}_{w^N}) \leq \delta_N) \leq A[I(W^{(1:N)}_w)]$. Thus based on Prop. 5, the error probability of $T$ times transmission is

$$P_e(T) = \sum_{t=1}^{T} \sum_{\mathcal{R}^t \cup \mathcal{I}^t} Z(W^{(i)}_{w^N}) + \sum_{t=2}^{T} \sum_{\mathcal{E}^{t-1}} Z(W^{(i)}_{w^N})$$

$$\leq (2T - 1)o(2^{-N^\beta})$$

Thus $\lim_{N \to \infty} P_e(T) = 0$ which achieves the reliability criterion in Def. 2.
2) **Strong security:** For strong security, we analyze the information leakage of $T$ tomes transmission. Let $L(T) = I(M^{1:T}; Z^{1:T})$ be the information leakage to Eve, where $M^t = U^{T \setminus t}$, $Z^t = Z^N$ and additionally $E^t = U^t$, $F^t = U^F$ for $t$-th block transmission. Thus from [11, Section IV-B], for the adapted multi-block chaining structure, have

$$L(T) \leq \sum_{t=1}^{T} I(M^t, E^t, F^t; Z^t) + I(E^0; Z^0)$$

(83)

with frozen bits $F^t$ fixed to 0. Note that Eve do not know the pre-shared information, so $I(E^0; Z^0) = 0$.

For any subset $\mathcal{A}$ of index $N$, denote $a^1 < a^2 < \ldots < a^{|\mathcal{A}|}$ as the correspondent indices of the elements $U^A$, that $U^A \triangleq U^{a^1:a^{|\mathcal{A}|}} = U^{a^1}, \ldots, U^{a^{|\mathcal{A}|}}$. According to [10, Lemma 15], the subsets $\mathcal{I}^t \cup \mathcal{F}^t$ and $\mathcal{R}^t$ of irregular polarization match the construction of the induced channel, thus satisfies

$$I(M^t, E^t, F^t; Z^t) = I(U^{\mathcal{I}^t \cup \mathcal{F}^t}; Z^N) = \sum_{i=1}^{[\mathcal{I}^t \cup \mathcal{F}^t]} I(U^{a^i}; Z^N | U^{a^1:a^{i-1}})$$

(85)

$$= \sum_{i=1}^{[\mathcal{I}^t \cup \mathcal{F}^t]} I(U^{a^i}; U^{a^1:a^{i-1}}, Z^N)$$

$$\leq \sum_{i=1}^{[\mathcal{I}^t \cup \mathcal{F}^t]} I(U^{a^i}; U^{1:a^{i-1}}, Z^N)$$

where $(a)$ is because $U^{a^i}$ are independent from each other.

According to (79), $\mathcal{I}^t \cup \mathcal{F}^t = \mathcal{H}^t_{W_r}$. Then from (73), have $Z(W_{rN}^{(i)}) \geq 1 - 2^{-N^\beta}$ for $i \in \mathcal{H}^t_{W_r}$. Note that $I(W) \leq \sqrt{1 - Z(W)^2}$, thus $I(W_{rN}^{(i)}) \leq o(2^{-N^\beta})$ for $i \in \mathcal{H}^t_{W_r}$. Hence $I(M^t, E^t, F^t; Z^t) \leq o(N2^{-N^\beta})$, which indicates $L(T) \leq o(TN2^{-N^\beta})$.

For case that $\tilde{W}^N$ is noiseless (such as the basic A-WTC), have $Z(W_{rN}^{(i)}) = 1$ for $i \in \mathcal{H}^t_{W_r}$, which indicates that $I(W_{rN}^{(i)}) = 0$. Thus $I(M^t, E^t, F^t; Z^t) = 0$ and $L(T) = 0$.

Therefore have $\lim_{N \to \infty} L(T) = 0$ for a fixed $T$, which achieves the strong security criterion in Def. 2.

3) **Achievable secrecy rate:** As proofed previously, reliability and strong security criterions are achieved by the proposed irregular secure polar coding. Now we discuss the achievable secrecy rate of our scheme for sA-WTC with DMCs.
Let $R_s$ be the secrecy rate, then have $R_s = \frac{1}{TN} \sum_{t=1}^T |\mathcal{I}^t \setminus \mathcal{E}^t|$. Since $\mathcal{E}^T$ can be set to $\emptyset$, have
\[
\lim_{N \to \infty} R_s \geq \lim_{N \to \infty} \frac{1}{T} \sum_{t=1}^T \frac{1}{N} (|\mathcal{I}^t| - |\mathcal{B}^t|)
= \lim_{N \to \infty} \frac{1}{T} \sum_{t=1}^T \frac{1}{N} (|\mathcal{I}^t \cup \mathcal{R}^t| - |\mathcal{B}^t \cup \mathcal{R}^t|)
= \lim_{N \to \infty} \frac{1}{T} \sum_{t=1}^T \frac{1}{N} (|\mathcal{L}^t_{w_t}| - |(\mathcal{H}^t_{w_t})^c|)
\]
\[= (a) \frac{1}{T} \sum_{t=1}^T [A[I(W_{1:N}^{1:N})] - A[I(W_{r}^{1:N})]]t\]
\[= (b) (1 - \rho_w)I(U; V) - \rho_r I(U; V)
\]
where $(a)$ is due to Prop. 4 and Prop. 5, $(b)$ is due to $A[I(W_{1:N}^{1:N})] = (1 - \rho_w)I(U; V)$, $A[I(W_{r}^{1:N})] = \rho_r I(U; V)$. Thus the secrecy capacity of sA-WTC with DMCs can be achieved when $N \to \infty$.

V. Conclusion

In this paper, we have studied the irregular channel transformation which is a modified $G_N$ operation of Arıkan’s channel polarization by replacing the initial channels $W^{N}$ with $W^{1:N}$ with different transition probabilities. As we proofed, this irregular channel transformation has a similar polarization effect for the initial $W^{1:N}$, named irregular channel polarization. Theoretical results show that for any fixed $\delta \in (0, 1)$, as $N \to \infty$, the fraction of indices $i \in [1, N]$ for which $I(W_{N}^{i}) \in (1 - \delta, 1]$ goes to $A[I(W^{1:N})]$ and the fraction for which $I(W_{N}^{i}) \in [0, \delta)$ goes to $1 - A[I(W^{1:N})]$. Also, for any B-DMC $W^{1:N}$ with $I(W^{i}) > 0$, and any fixed $R < A[I(W^{1:N})]$ and constant $\beta < 1/2$, there exists index set $\mathcal{A}_N \subset [1, N], |\mathcal{A}_N| \leq NR$ that $P_e(N, R) = \sum_{i \in \mathcal{A}_N} Z(W_{N}^{(i)}) = o(2^{-N^\beta})$.

For the secrecy capacity achieving problem of sA-WTC with DMCs, we have constructed equivalent channels $W_{w_t}^{1:N}$ and $W_{r_t}^{1:N}$ by respectively connecting the $W$ and $\tilde{W}$ with full noise erase bit channel or noiseless erase bit channel to obtain the same effect of reading and rewriting operation. By applying the irregular channel polarization to the constructed equivalent channels, we successfully implement the strong security achieving polar coding scheme to the sA-WTC with DMCs. As proofed, secrecy capacity has been achieved by this irregular secure polar coding scheme under the reliability and strong security criterions.
However, there are till some open problems. For the irregular polarization, we only have studied its basic polarization characters and the polarization rate, thus a more comprehensive study on whether it shares more commons with the original channel polarization is needed. Moreover, for A-WTC with DMCs, our irregular secure polar coding is only constructed under the static assumption which removes the initiative of eavesdropper. So the problem of constructing a secure scheme against a active eavesdropper over A-WTC with DMC is still need for further research.

**APPENDIX A**

Here we proof the Prop. For channel transformation of (12), similarly as [9, Appendix E], we have

\[
Z(W^+) = \sum_{y^1y^2u^1} \sqrt{W^+(f(y^1, y^2), u^1|0)W^+(f(y^1, y^2), u^1|0)} \\
= \sum_{y^1y^2u^1} \frac{1}{2} \sqrt{W^1(y^1|u^1)W^2(y^2|0)} \cdot \sqrt{W^2(y^1|u^1 \oplus 1)W^2(y^2|1)} \\
= \sum_{y^2} \sqrt{W^2(y^2|0)W^2(y^2|1)} \cdot \sum_{u^1} \frac{1}{2} \sum_{y^1} \sqrt{W^1(y^1|u^1)W^1(y^1|u^1 \oplus 1)} \\
= Z(W^2)Z(W^1) 
\]

\[
Z(W^-) = \sum_{y^1y^2} \sqrt{W^-(f(y^1, y^2)|0)W^-(f(y^1, y^2|1))} \\
= \sum_{y^1y^2} \frac{1}{2} \sqrt{W^1(y^1|0)W^2(y^2|0) + W^1(y^1|1)W^2(y^2|1)} \\
\cdot \sqrt{W^1(y^1|0)W^2(y^2|1) + W^1(y^1|1)W^2(y^2|0)} \\
\overset{(a)}{\leq} \sum_{y^1y^2} \frac{1}{2} \left[ \sqrt{W^1(y^1|0)W^2(y^2|0)} + \sqrt{W^1(y^1|1)W^2(y^2|1)} \right] \\
\cdot \left[ \sqrt{W^1(y^1|0)W^2(y^2|1) + W^1(y^1|1)W^2(y^2|0)} \right] \\
- \sum_{y^1y^2} \sqrt{W^1(y^1|0)W^2(y^2|0)W^1(y^1|1)W^2(y^2|1)} \\
\overset{(b)}{=} Z(W^1) + Z(W^2) - Z(W^1)Z(W^2) 
\]

where \((a)\) is due to

\[
\left[ (\sqrt{a} + \sqrt{c})(\sqrt{a}d + \sqrt{c}b) - 2\sqrt{abcd} \right]^2 \\
= \left[ (\sqrt{ab} + \sqrt{cd})(ad + cb) \right]^2 + 2(\sqrt{a} - \sqrt{c})^2(\sqrt{b} - \sqrt{a})^2\sqrt{abcd} 
\]

(93)
Note that the equal of (a) holds when \( a = c \) or \( b = d \) or \( abcd = 0 \), which is satisfied when \( W^1 \) and \( W^2 \) are BECs. (b) is due to

\[
\sum_{y^1,y^2} \frac{1}{2} \left[ \sqrt{W^1(y^1|0)W^2(y^2|0)} + \sqrt{W^1(y^1|1)W^2(y^2|1)} \right] \\
\cdot \left[ \sqrt{W^1(y^1|0)W^2(y^2|1)} + \sqrt{W^1(y^1|1)W^2(y^2|0)} \right] \\
= \frac{1}{2} \sum_{y^1} W^1(y^1|0) \sum_{y^2} \sqrt{W^2(y^2|0)W^2(y^2|1)} + \frac{1}{2} \sum_{y^1} W^1(y^1|1) \sum_{y^2} \sqrt{W^2(y^2|0)W^2(y^2|1)} \\
+ \frac{1}{2} \sum_{y^2} W^2(y^2|0) \sum_{y^1} \sqrt{W^1(y^1|0)W^2(y^1|1)} + \frac{1}{2} \sum_{y^2} W^2(y^2|1) \sum_{y^1} \sqrt{W^1(y^1|0)W^2(y^1|1)} \\
= Z(W^1) + Z(W^2)
\]

(95)

and

\[
\sum_{y^1,y^2} \sqrt{W^1(y^1|0)W^2(y^2|0)W^1(y^1|1)W^2(y^2|1)} \\
= \sum_{y^1} \sqrt{W^1(y^1|0)W^1(y^1|1)} \cdot \sum_{y^2} \sqrt{W^2(y^2|0)W^2(y^2|1)} \\
= Z(W^1)Z(W^2)
\]

(97)

ACKNOWLEDGMENT

This work is supported in part by the Natural Science Foundation of Hubei Province (Grant No.2017CFB398) and the Fundamental Research Funds for the Central Universities (Grant No.2662017QD042).

REFERENCES

[1] A. D. Wyner, “The wire-tap channel”, *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
[2] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II, AT&T Bell Laboratories technical journal”, vol. 63, no. 10, pp. 2135-2157, 1984.
[3] M. Nafea and A. Yener, “Wiretap channel II with a noisy main channel”, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1159-1163, Jun. 2015.
[4] D. He, W. Guo and Y. Luo, “Secrecy capacity of the extended wiretap channel II with noise”, *Entropy*, vol. 18, no. 12, pp.377, 2016.
[5] D. He, Y. Luo and N. Cai, “Strong secrecy capacity of the wiretap channel II with DMC main channel”, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 505-509, Jul. 2016.
[6] M. Nafea and A. Yener, “The multiple access wiretap channel II with a noisy main channel”, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2983-2987, Jul. 2016.
[7] V. Aggarwal, L. Lai, A. R. Calderbank, et al. “Wiretap Channel Type II with an Active Eavesdropper”, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1944-1948, Jul. 2009.

[8] P. Wang and R. Safavi-Naini, “A model for adversarial wiretap channels”, *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 970-983, Nov. 2015.

[9] E. Arikan, “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.

[10] 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.

[11] E. Şaşoğlu and A. Vardy, “A new polar coding scheme for strong security on wiretap channels”, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1117-1121, Jul. 2013.

[12] Y.-P. Wei and S. Ulukus, “Polar coding for the general wiretap channel”, in *Proc. Information Theory Workshop*, pp. 1-5, Apr. 26/May 1 2015.

[13] Y.-P. Wei and S. Ulukus, “Polar coding for the general wiretap channel with extensions to multiuser scenarios”, *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 2, pp. 278-291, Feb. 2016.

[14] T. C. Gulcu and A. Barg, “Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component”, in *Proc. IEEE Inf. Theory Workshop*, pp. 1-5, Apr. 26/May 1 2015.

[15] M. Zheng, M. Tao, W. Chen, and C. Ling, “Secure polar coding for the two-way wiretap channel,” *IEEE Access*, pp. 1-1, Mar. 2018.

[16] I. Csiszár, J. Körner, “Broadcast channels with confidential messages”, *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[17] E. Arikan and E. Telatar, “On the rate of channel polarization”, in *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1493-1495, Jul. 2009.

**Yizhi Zhao** received the Ph.D. degree in the school of Optical and Electronic Information from the Huazhong University of Science and Technology, Wuhan, China, in 2017.

He is currently an Assistant Professor with the College of Informatics, Huazhong Agricultural University. His research interests include physical layer coding, information theory and machine learning.