Polar Coding for Secure Transmission and Key Agreement

O. Ozan Koyluoglu and Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University
Columbus, OH 43210

***Abstract*—Wyner's work on wiretap channels and the recent works on information theoretic security are based on random codes. Achieving information theoretical security with practical coding schemes is of definite interest. In this note, the attempt is to overcome this elusive task by employing the polar coding technique of Arıkan. It is shown that polar codes achieve non-trivial perfect secrecy rates for binary-input degraded wiretap channels while enjoying their low encoding-decoding complexity. In the special case of symmetric main and eavesdropper channels, this coding technique achieves the secrecy capacity. Next, fading erasure wiretap channels are considered and a secret key agreement scheme is proposed, which requires only the statistical knowledge of the eavesdropper channel state information (CSI). The enabling factor is the creation of advantage over Eve, by blindly using the proposed scheme over each fading block, which is then exploited with privacy amplification techniques to generate secret keys.**

I. Introduction

The notion of information theoretic secrecy was introduced by Shannon to study secure communication over point-to-point noiseless channels [1]. This line of work was later extended by Wyner [2] to noisy channels assuming a degraded eavesdropper channel (compared to that of the legitimate receiver). Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper can be exploited to transmit secret bits using random codes. This *keyless secrecy* result was then extended to a more general (broadcast) model in [3] and to the Gaussian setting in [4]. Recently, there has been a renewed interest in wireless physical layer security (see, e.g., Special Issue on Information Theoretic Security, *IEEE Trans. Inf. Theory*, June 2008 and references therein). However, designing practical codes to achieve secrecy for any given main and eavesdropper channels remained open.

In [5], the authors constructed LDPC based wiretap codes for certain binary erasure channels (BECs) and binary symmetric channels (BSCs). In particular, when the main channel is noiseless and the eavesdropper channel is a BEC, [5] presented codes that approach secrecy capacity. For other scenarios, secrecy capacity achieving code design is stated as an open problem. Similarly, [6] considers the design of secure nested codes for the noiseless main channel setting (see also [7]).

This work is partially supported by Los Alamos National Labs (LANL) and by National Science Foundation (NSF). The first author is partially supported by the Presidential Fellowship award of the Ohio State University.

This work studies secret communication over a binary-input degraded wiretap channel. Using the polar coding technique of Arıkan [8], we show that non-trivial secrecy rates are achievable. According to our best knowledge, this coding technique is the first provable and practical (having low encoding and decoding complexity) secrecy encoding technique for this set of channels. In the special case of the symmetric main and eavesdropper channels, this technique achieves the secrecy capacity of the channel. We note that the parallel works [9], [10] independently established the result that polar coding achieves the secrecy capacity of the degraded wiretap channels, if both main and eavesdropper channels are binary-input and symmetric, i.e., Corollary 7 of this paper. (This result publicized for the first time in [9]. [10] includes the rate-equivocation analysis. An earlier version of our work can be found in [11].) Secondly, we consider fading wiretap channels and propose a key agreement scheme requiring only the statistical knowledge of the eavesdropper CSI at the users. The enabling observation is that by blindly using the scheme over many fading blocks, the users will eventually create an advantage over Eve, which can then be exploited to generate secret keys using privacy amplification techniques.

II. Notations

Throughout this paper, vectors are denoted by $x_1^N = \{x_1, \cdots, x_N\}$ or by $\bar{x}$ if we omit the indices. Random variables are denoted with capital letters X, which are defined over sets denoted by the calligraphic letters $\mathcal{X}$. For a given set $\mathcal{A} \subset \{1, \cdots, N\}$, we write $x_{\mathcal{A}}$ to denote the sub-vector $\{x_i : i \in \mathcal{A}\}$. Omitting the random variables, we use the following shorthand for probability distributions $p(x) \triangleq \Pr(X = x)$, $p(x|y) \triangleq \Pr(X = x|Y = y)$.

III. Polar Codes

Consider a binary-input DMC (B-DMC) given by $W(y|x)$, where $x \in \mathcal{X} = \{0, 1\}$ and $y \in \mathcal{Y}$ for some finite set $\mathcal{Y}$. The N uses of W is denoted by $W^N(y_1^N|x_1^N)$. The symmetric capacity of a B-DMC W is given by

$$I(W) \triangleq \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \frac{1}{2} W(y|x) \log_2 \left(\frac{W(y|x)}{\sum_{x' \in \mathcal{X}} \frac{1}{2} W(y|x')} \right), \quad (1)$$

which is the mutual information $I(X;Y)$ when the input X is uniformly distributed. The Bhattacharyya parameter of W is given by

$$Z(W) \triangleq \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}, \tag{2}$$

which measures the reliability of W as it is an upper bound on the ML decision error probability on a single channel use.

Polar codes are recently introduced by Arıkan [8]. These codes can be encoded and decoded with complexity $O(N\log N)$, while achieving an overall block-error probability that is bounded as $O(2^{-N^\beta})$ for any fixed $\beta < \frac{1}{2}$ ([8], [12]). In [8], channel polarization is used to construct codes (polar codes) that can achieve the symmetric capacity, $I(W)$, of any given B-DMC W. Channel polarization consists of two operations: Channel combining and channel splitting. Let u_1^N be the vector to be transmitted. The combined channel is represented by W_N and is given by

$$W_N(y_1^N|u_1^N) = W^N(y_1^N|u_1^N B_N F^{\otimes n}), \tag{3}$$

where B_N is a bit-reversal permutation matrix, $N = 2^n$, and $F \triangleq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Note that the actual channel input here is given by $x_1^N = u_1^N B_N F^{\otimes n}$. The channel splitting constructs N binary input channels from W_N, where the transformation is given by

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) \triangleq \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N(y_1^N|u_1^N). \tag{4}$$

The polarization phenomenon is shown by the following.

Theorem 1 (Theorem 1 of [8]): For any B-DMC W, $N = 2^n$ for some n, and $\delta \in (0,1)$, we have

$$\lim_{N\to\infty} \frac{|\{i \in \{1,\cdots,N\} : I(W_N^{(i)}) \in (1-\delta, 1]\}|}{N} = I(W),$$

$$\lim_{N\to\infty} \frac{|\{i \in \{1,\cdots,N\} : I(W_N^{(i)}) \in [0, \delta)\}|}{N} = 1 - I(W).$$

In order to derive the rate of the channel polarization, the random process Z_n is defined in [8] and in [12]. Basically,

$$\Pr\{Z_n \in (a,b)\} = \frac{|\{i \in \{1,\cdots,N\} : Z(W_{2^n}^{(i)}) \in (a,b)\}|}{N}$$

The rate of the channel polarization is given by the following.

Theorem 2 (Theorem 1 of [12]): For any B-DMC W and for any given $\beta < \frac{1}{2}$,

$$\lim_{n\to\infty} \Pr\{Z_n < 2^{-2^{n\beta}}\} = I(W).$$

Now, the idea of polar coding is clear. The encoder-decoder pair, utilizing the polarization effect, will transmit data through the subchannels for which $Z(W_N^{(i)})$ is near 0. In [8], the polar code $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ for B-DMC W is defined by $x_1^N = u_1^N B_N F^{\otimes n}$, where $u_{\mathcal{A}^c}$ is a given frozen vector, and the information set $\mathcal{A}$ is chosen such that $|\mathcal{A}| = K$ and $Z(W_N^{(i)}) < Z(W_N^{(j)})$ for all $i \in \mathcal{A}$, $j \in \mathcal{A}^c$. The frozen vector $u_{\mathcal{A}^c}$ is given to the decoder. Arıkan's successive cancellation (SC) estimates the input as follows: For the frozen indices $\hat{u}_{\mathcal{A}^c} = u_{\mathcal{A}^c}$. For the remaining indices s.t. $i \in \mathcal{A}$; $\hat{u}_i = 0$, if $W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|0) \geq W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|1)$ and $\hat{u}_i = 1$, otherwise. With this decoder, it is shown in [8] that the average block error probability over the ensemble (consisting of all possible frozen vector choices) of polar codes is bounded by

$$P_e(N) \leq \sum_{i\in\mathcal{A}} Z(W_N^{(i)}).$$

We now state the result of [8] using the bound given in [12].

Theorem 3 (Theorem 2 of [12]): For any given B-DMC W with $I(W) > 0$, let $R < I(W)$ and $\beta \in (0, \frac{1}{2})$ be fixed. Block error probability for polar coding under SC decoding (averaged over possible choices of frozen vectors) satisfies $P_e(N) = O(2^{-N^\beta})$.

Note that, for any $\beta \in (0, \frac{1}{2})$ and $\epsilon > 0$, we can define the sequence of polar codes by choosing the information indices as $\mathcal{A}_N = \{i \in \{1,\cdots,N\} : Z(W_N^{(i)}) \leq \frac{1}{N} 2^{-N^\beta}\}$. Then, from the above theorems, for sufficiently large N, we can achieve the rate $R = \frac{|\mathcal{A}_N|}{N} \geq I(W) - \epsilon$ with average error probability (averaged over the possible choices of $u_{\mathcal{A}_N^c}$) $P_e(N) \leq \sum_{i\in\mathcal{A}_N} Z(W_N^{(i)}) \leq 2^{-N^\beta}$ under SC decoding. (See also [13].)

This result shows the existence of a polar code $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ achieving the symmetric capacity of W. We note that, any frozen vector choice of $u_{\mathcal{A}^c}$ will work for symmetric channels [8]. For our purposes, we will denote a polar code for B-DMC W with $\mathcal{C}(N, \mathcal{F}, u_{\mathcal{F}})$, where the frozen set is given by $\mathcal{F} \triangleq \mathcal{A}^c$. Note that, $\mathcal{A}$ denotes the indices of information transmission for the polar code, whereas $\mathcal{F}$ is the set of frozen indices.

We conclude this section by noting the following lemma (given in [13]) regarding polar coding over degraded channels.

Lemma 4 (Lemma 4.7 of [13]): Let $W : \mathcal{X} \to \mathcal{Y}$ and $W' : \mathcal{X} \to \mathcal{Y}'$ be two B-DMCs such that W is degraded w.r.t. W', i.e., there exists a channel $W'' : \mathcal{Y}' \to \mathcal{Y}$ such that

$$W(y|x) = \sum_{y'\in\mathcal{Y}'} W'(y'|x) W''(y|y').$$

Then, $W_N^{(i)}$ is degraded w.r.t. $W'^{(i)}_N$ and $Z(W_N^{(i)}) \geq Z(W'^{(i)}_N)$.

IV. Secure Transmission over Wiretap Channel

A discrete memoryless wiretap channel with is denoted by

$$(\mathcal{X}, W(y_m, y_e|x), \mathcal{Y}_m \times \mathcal{Y}_e),$$

for some finite sets $\mathcal{X}, \mathcal{Y}_m, \mathcal{Y}_e$. Here the symbols $x \in \mathcal{X}$ are the channel inputs and the symbols $(y_m, y_e) \in \mathcal{Y}_m \times \mathcal{Y}_e$ are the channel outputs observed at the main decoder and at the eavesdropper, respectively. The channel is memoryless and time-invariant: $p(y_{mi}, y_{ei}|x_1^i, y_m{}_1^{i-1}, y_{e1}^{i-1}) = W(y_{mi}, y_{ei}|x_i)$. We assume that the transmitter has a secret message M which is to be transmitted to the receiver in N channel uses and to be secured from the eavesdropper. In this setting, a secret codebook has the following components:

1) The secret message set $\mathcal{M}$. The transmitted messages are assumed to be uniformly distributed over these message sets.

2) A stochastic encoding function $f(.)$ at the transmitter which maps the secret messages to the transmitted symbols: $f : m \to X_1^N$ for each $m \in \mathcal{M}$.

3) Decoding function $\phi(.)$ at receiver which maps the received symbols to estimate of the message: $\phi({Y_m}_1^N) = \{\hat{m}\}$.

The reliability of transmission is measured by the following probability of error.

$$P_e = \frac{1}{|\mathcal{M}|} \sum_{(m)\in\mathcal{M}} \Pr\left\{\phi({Y_m}_1^N) \neq (m) | (m) \text{ is sent}\right\}$$

We say that the rate R is an achievable secrecy rate, if, for any given $\epsilon > 0$, there exists a secret codebook such that,

$$\begin{aligned} \frac{1}{N}\log(|\mathcal{M}|) &= R \\ P_e &\leq \epsilon \\ \frac{1}{N} I\left(M; {Y_e}_1^N\right) &\leq \epsilon \end{aligned} \quad (5)$$

for sufficiently large N.

Consider a degraded binary-input wiretap channel, where, for the input set $\mathcal{X} = \{0, 1\}$, the main channel is given by

$$W_m(y_m|x) \quad (6)$$

and the eavesdropper channel is

$$W_e(y_e|x) = \sum_{y_m \in \mathcal{Y}_m} W_m(y_m|x) W_d(y_e|y_m). \quad (7)$$

Note that, due to degradation, polar codes designed for the eavesdropper channel can be used for the main channel. For a given sufficiently large N and $\beta \in (0, \frac{1}{2})$, let

$$\mathcal{A}_m = \{i \in \{1, \cdots, N\} : Z({W_m}_N^{(i)}) \leq \frac{1}{N} 2^{-N^\beta}\},$$

$$\mathcal{A}_e = \{i \in \{1, \cdots, N\} : Z({W_e}_N^{(i)}) \leq \frac{1}{N} 2^{-N^\beta}\}.$$

Now, consider a polar code $\mathcal{C}_m \triangleq \mathcal{C}(N, \mathcal{F}_m, u_{\mathcal{F}_m})$ for the main channel with some $u_{\mathcal{F}_m}$ (the frozen vector for the main channel). Due to Lemma 4, we have $\mathcal{A}_e \subset \mathcal{A}_m$ and hence $\mathcal{F}_m \subset \mathcal{F}_e$. Now, for any given length $|\mathcal{F}_e| - |\mathcal{F}_m|$ vector $\bar{v}_m$ (to be called as message vector) and $u_{\mathcal{F}_m}$, we define the frozen vector for the eavesdropper, denoted by $u_{\mathcal{F}_e}(\bar{v}_m)$, by choosing $(u_{\mathcal{F}_e}(\bar{v}_m))_{\mathcal{F}_m} = u_{\mathcal{F}_m}$ and $(u_{\mathcal{F}_e}(\bar{v}_m))_{\mathcal{F}_e \setminus \mathcal{F}_m} = \bar{v}_m$. Note that, denoting $\mathcal{C}_e(\bar{v}_m) \triangleq \mathcal{C}(N, \mathcal{F}_e, u_{\mathcal{F}_e}(\bar{v}_m))$, the ensemble $\cup_{\bar{v}_m, u_{\mathcal{F}_m}} \mathcal{C}_e(\bar{v}_m)$ is a symmetric capacity achieving polar code ensemble for the eavesdropper channel W_e (if the eavesdropper channel is symmetric, any frozen vector choice will work [8], and hence the code achieves the capacity of the eavesdropper channel for any $\bar{v}_m, u_{\mathcal{F}_m}$). This implies that the code for the main channel can be partitioned as $\mathcal{C}_m = \cup_{\bar{v}_m} \mathcal{C}_e(\bar{v}_m)$. This observation, when considered over the ensemble of codes, enables us to construct secrecy achieving polar coding schemes, even if the eavesdropper channel is not symmetric, as characterized by the following theorem.

Theorem 5: For a binary-input degraded wiretap channel, the perfect secrecy rate of $I(W_m) - I(W_e)$ is achieved by polar coding.

Proof:

Encoding: We map the secret message to be transmitted to the message vector, $\bar{v}_m$, and generate a random vector $\bar{v}_r$, according to uniform distribution over $\mathcal{X}$, of length $|\mathcal{A}_e|$. Then, the channel input is constructed with $x_1^N = u_1^N B_N F^{\otimes n}$, where $u_{\mathcal{F}_m}$ is the frozen vector of the polar code $\mathcal{C}_m$, $u_{\mathcal{F}_e \setminus \mathcal{F}_m} = \bar{v}_m$, and $u_{\mathcal{A}_e} = \bar{v}_r$. The polar code ensemble is constructed over all different choices of frozen vectors, i.e., $u_{\mathcal{F}_m}$.

Decoding: The vectors $\bar{v}_m$ and $\bar{v}_r$ can be decoded with the SC decoder described above with error probability $P_e = O(2^{-N^\beta})$ (averaged over the ensemble) achieving a rate $R = \frac{|\bar{v}_m|}{N} = I(W_m) - I(W_e)$ for sufficiently large N.

Security: Lets assume that the vector $\bar{v}_m$ is given to the eavesdropper along with $u_{\mathcal{F}_m}$. Then, employing the SC decoding, the eavesdropper can decode the random vector $\bar{v}_r$ with $P_e = O(2^{-N^\beta})$ averaged over the ensemble. Utilizing the Fano's inequality and average it over the code ensemble seen by the Eve, i.e. over $\bar{V}_m$ and $U_{\mathcal{F}_m}$, we obtain

$$H(\bar{V}_r|\bar{V}_m, U_{\mathcal{F}_m}, {Y_e}_1^N) \leq H(P_e) + N\log(|\mathcal{X}|)P_e \leq N\epsilon(N), \quad (8)$$

where $\epsilon(N) \to 0$ as $N \to \infty$.

Then, the mutual information leakage to the eavesdropper averaged over the ensemble can be bounded as follows.

$$\begin{aligned} I(M; {Y_e}_1^N | U_{\mathcal{F}_m}) &= I(\bar{V}_m; {Y_e}_1^N | U_{\mathcal{F}_m}) \\ &= I(\bar{V}_m, \bar{V}_r; {Y_e}_1^N | U_{\mathcal{F}_m}) - I(\bar{V}_r; {Y_e}_1^N | \bar{V}_m, U_{\mathcal{F}_m}) \quad (9) \\ &\overset{(a)}{=} I(U_1^N; {Y_e}_1^N) - H(\bar{V}_r) + H(\bar{V}_r|\bar{V}_m, U_{\mathcal{F}_m}, {Y_e}_1^N) \quad (10) \\ &\overset{(b)}{\leq} I(X_1^N; {Y_e}_1^N) - H(\bar{V}_r) + H(\bar{V}_r|\bar{V}_m, U_{\mathcal{F}_m}, {Y_e}_1^N) \quad (11) \\ &\overset{(c)}{\leq} NI(W_e) - |\mathcal{A}_e| + H(\bar{V}_r|\bar{V}_m, u_{\mathcal{F}_m}, {Y_e}_1^N) \quad (12) \\ &\overset{(d)}{\leq} NI(W_e) - |\mathcal{A}_e| + N\epsilon(N), \quad (13) \end{aligned}$$

where in (a) we have U_1^N each entry with i.i.d. uniformly distributed, (b) follows from data processing inequality, (c) is due to $I(X_1^N; {Y_e}_1^N) = \sum_{i=1}^N I(X_1^N; Y_{ei}|{Y_e}_1^{i-1}) \leq \sum_{i=1}^N H(Y_{ei}) - H(Y_{ei}|X_i) = NI(X_i; Y_{ei})$ with a uniformly distributed X_i, and (d) follows from (8) with $\epsilon(N) \to 0$ as $N \to \infty$. As $\frac{|\mathcal{A}_e|}{N} \to I(W_e)$ as N gets large, we obtain

$$\frac{1}{N} I(\bar{V}_m; {Y_e}_1^N | U_{\mathcal{F}_m}) \leq \epsilon \quad (14)$$

for a given $\epsilon > 0$ for sufficiently large N. As the reliability and secrecy constraints are satisfied averaged over the ensemble, there exist a polar code with some fixed $u_{\mathcal{F}_m}$ achieving the secure rate $I(W_m) - I(W_e)$. ■

Note that in the above result, the code satisfying the reliability and the secrecy constraints can be found from the ensemble by an exhaustive search. However, as block length increases, almost all the codes in the ensemble will do equally well. If the eavesdropper channel is symmetric, then the secrecy

constraint is satisfied for any given frozen vector $u_{\mathcal{F}_m}$ and the code search is only for the reliability constraint. If the eavesdropper channel is not symmetric, a prefix channel can be utilized to have this property.

Corollary 6: For non-symmetric eavesdropper channels, the channel can be prefixed with some $p(x|x')$ such that the resulting eavesdropper channel

$$W'_e(y_e|x') = \sum_{y_m \in \mathcal{Y}_m} p(x|x') W_m(y_m|x) W_d(y_e|y_m)$$

is symmetric. Then, using the scheme above, the secret rate

$$R = I(W'_m) - I(W'_e)$$

is achievable, where $W'_m(y_m|x') = p(x|x')W_m(y_m|x)$.
Finally, we note that the scheme achieves the secrecy capacity and any code in the ensemble, i.e., any fixed $u_{\mathcal{F}_m}$, will satisfy both the reliability and secrecy constraints, if the main and eavesdropper channels are symmetric.

Corollary 7: For a binary-input degraded wiretap channel with symmetric main and eavesdropper channels, polar coding achieves the secrecy capacity of the channel, i.e., $C(W_m) - C(W_e)$.

We note that the stated results are achievable by encoders and decoders with complexity of $O(N \log N)$ for each. In addition, if the channels are binary erasure channels (BECs), then there exists algorithms with complexity $O(N)$ for the code construction [8].

V. Secret Key Agreement over Fading Wiretap Channels

In this section, we focus on the following key agreement problem: Alice, over (slow) fading wiretap channel, would like to agree on a secret key with Bob in the presence of passive eavesdropper Eve. We focus on the special case of binary erasure main and eavesdropper channels, for which the code construction is shown to be simple [8].

Fading blocks are represented by $i = 1, \cdots, LM$, each block has N channel uses, and there are L super blocks each with M fading blocks. Random variables over blocks are represented with the following bar notation. $\bar{Y}_e^{(l;m)}$ denotes the observations of Eve over the fading block m of the super block l, the observations of Eve over super block $l \in [1, \cdots, L]$ is denoted by $\bar{\bar{Y}}_e^{(l)} = \bar{Y}_e^{(l;1\cdots M)} \triangleq \{\bar{Y}_e^{(l;1)}, \cdots, \bar{Y}_e^{(l;M)}\}$, and Eve's total observation over all super blocks is denoted by $Y_e^* = \bar{\bar{Y}}_e^{(1\cdots L)} = \{\bar{\bar{Y}}_e^{(1)}, \cdots, \bar{\bar{Y}}_e^{(L)}\}$.

Main and eavesdropper channels are binary erasure channels and are denoted by $W_m^{(i)}$ and $W_e^{(i)}$, respectively. Here, the channels W_m and W_e are random, outcome of which result in the channels of each block. Instantaneous eavesdropper CSI is not known at the users, only the statistical knowledge of it is assumed. The channels are assumed to be physically degraded w.r.t. *some* order at each block. [1] Note that, in this setup, eavesdropper channel can be better than the main channel on the average.

We utilize the proposed secrecy encoding scheme for the wiretap channel at each fading block. Omitting the block indices, frozen and information bits are denoted as $u_{\mathcal{F}_m}$ and $u_{\mathcal{A}_m}$, respectively. Information bits are uniformly distributed binary random variables and are mapped to $u_{\mathcal{A}_m}$. Secure message and randomization bits among these information bits are denoted by $\bar{V}_m$ and $\bar{V}_r$, respectively. Frozen bits are provided both to main receiver and eavesdropper at each block. (We omitted writing this side information below as all zero vector can be chosen as the frozen vector for the erasure channel [8].) Note that Alice and Bob do not know the length of $\bar{V}_m^{(i)}$ at fading block i. In particular, there may not be any secured bits at a given fading block.

Considering the resulting information accumulation over a block, we obtain the followings.

$$\begin{aligned} \frac{1}{N} H(\bar{V}_m^{(i)}) &= [C(W_m^{(i)}) - C(W_e^{(i)})]^+ \\ \frac{1}{N} H(\bar{V}_r^{(i)}) &= \min\{C(W_m^{(i)}), C(W_e^{(i)})\}, \end{aligned}$$

where the former denotes the amount of secure information generated at block i (here the secrecy level is the bound on the mutual information leakage rate), and the latter denotes the remaining information. Note that these entropies are random variables as channels are random over the blocks. Remarkable, this scheme converts the fading phenomenon to the advantage of Alice and Bob (similar to the enabling observation utilized in [14]). Exploiting this observation and coding over LM fading blocks, the proposed scheme below creates advantage for the main users: As L, M, N get large, information bits, denoted by W^*, are w.h.p. reliably decoded at the Bob, $H(W^*) \to LMN\,[C(W_m)]$, and $H(W^*|Y_e^*) \to LMN\,E\,[[C(W_m) - C(W_e)]^+]$. This accomplishes *both* advantage distillation and information reconciliation phases of a key agreement protocol [15], [16]. Now, a third phase (called as *privacy amplification*) is needed to distill a shorter string K from W^*, about which Eve has only a negligible amount of information. The privacy amplification step can be done with universal hashing as considered in [15]. We first state the following definition and lemma regarding universal hashing, and then formalize the main result of this section in the following theorem.

Definition 8: A class $\mathcal{G}$ of functions $\mathcal{A} \to \mathcal{B}$ is universal if, for any $x_1 \neq x_2$ in $\mathcal{A}$, the probability that $g(x_1) = g(x_2)$ is at most $\frac{1}{|\mathcal{B}|}$ when g is chosen as random from $\mathcal{G}$ according to the uniform distribution.

Note that the hash function should have complexity as 1) it will be revealed to each user, and 2) Alice and Bob will compute $g(W^*)$; and efficient universal classes exist, see, for example, [17]. Generalized privacy amplification, proposed in [15], is based on the following property of universal hashing.

Lemma 9 (Theorem 3, [15]): Let $X \in \mathcal{X}$ be a random variable with distribution P_X and Rényi entropy (of second

[1] We remark that a random walk model with packet erasures can be covered with this model. Also, parallel channel model can be adapted into this framework.

order) $R(X) = -\log_2 E[P_X(X)]$. Let G be a random choice (according to uniform distribution) of a member of universal class of hash functions $\mathcal{X} \to \{0,1\}^r$, and let $Q = G(X)$. Then, we have

$$H(Q|G) \geq R(Q|G) \geq r - \log_2\left(1 + 2^{r-R(X)}\right) \geq r - \frac{2^{r-R(X)}}{\ln 2}.$$

Exploiting the proposed coding scheme, which creates advantage in favor of Bob over the fading channel, we use the hash functions described above and obtain the following result.

Theorem 10: For any $\epsilon, \epsilon^* > 0$, let

$$n = L\,M\,N\,\left(E\left[C(W_m)\right] - \epsilon^*\right),$$
$$r = L\,M\,N\,\left(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon^*\right).$$

Then, for sufficiently large L, M and N, Alice and Bob can w.h.p. agree on the random variable $W^* \triangleq \bar{\bar{W}}^{(1\cdots L)}$ of length n over LM fading blocks (i.e., $\Pr\{W^* \neq \hat{W}^*\} \leq \epsilon$, where $\hat{W}^*$ denotes the estimate at Bob); and choose $K = G(W^*)$ as their secret key (here G is chosen uniformly random from universal class of hash functions $\{0,1\}^n \to \{0,1\}^r$) satisfying

$$I(K; Y_e^*, G) \leq \epsilon,$$

where $Y_e^* \triangleq \bar{\bar{Y}}_e^{(1\cdots L)}$ denotes the Eve's total received symbols.

Proof:

We repeat the described scheme over LM fading blocks. Due to the construction above, we have

$$\frac{1}{N}H(\bar{V}_m^{(i)}) - \epsilon_1 \leq \frac{1}{N}H(\bar{V}_m^{(i)}|\bar{Y}_e^{(i)}) \leq \frac{1}{N}H(\bar{V}_m^{(i)}), \quad (15)$$

where $\frac{1}{N}H(\bar{V}_m^{(i)}) = [C(W_m^{(i)}) - C(W_e^{(i)})]^+$ and $\epsilon_1 \to 0$ as N gets large (follows from the fact that conditioning does not increase entropy and the security of $\bar{V}_m^{(i)}$), and

$$\frac{1}{N}H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}, \bar{V}_m^{(i)}) \leq \epsilon_2, \quad (16)$$

where $\epsilon_2 \to 0$ as $N \to \infty$ (follows from Fano's inequality).

We now consider the total information accumulation and leakage. Let $W^* = \bar{\bar{W}}^{(1\cdots L)} \triangleq \{\bar{V}_m^{(l;m)}, \bar{V}_r^{(l;m)}, \forall l \in [1, L], \forall m \in [1, M]\}$ and denote the estimate of it at Bob as $\hat{W}^*$. We obtain that, there exist N_1, M_1, s.t. for any $N \geq N_1$ and $M \geq M_1$, we have

$$H(W^*) \geq LMN\left(E\left[C(W_m)\right] - \epsilon^*\right) \quad (17)$$

$$\Pr\{W^* \neq \hat{W}^*\} \leq LM2^{-N^\beta}, \quad (18)$$

for some $\beta \in (0, \frac{1}{2})$ due to polar coding and the union bound.

Considering $Y_e^* \triangleq \bar{\bar{Y}}_e^{(1\cdots L)}$ at Eve, we write

$$H(W^*|Y_e^*) = \sum_{l=1}^{L} H(\bar{\bar{W}}^{(l)}|\bar{\bar{Y}}_e^{(l)})$$
$$= \sum_{i=1}^{LM} H(\bar{V}_m^{(i)}|\bar{Y}_e^{(i)}) + H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}, \bar{V}_m^{(i)}). \quad (19)$$

Focusing on a particular super block, omitting the index (l) in $(\bar{\bar{W}}^{(l)}, \bar{\bar{Y}}_e^{(l)})$, and using (15) and (16) in (19), we obtain

$$MN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon_4\right) \leq H(\bar{\bar{W}}|\bar{\bar{Y}}_e)$$
$$\leq MN\left(E\left[[C(W_m) - C(W_e)]^+\right] + \epsilon_5\right), \quad (20)$$

where ϵ_4 and ϵ_5 vanishes as M, N get large.

In order to translate $H(W^*|Y_e^*)$ to Rényi entropy, to use Lemma 9 in our problem, we resort to typical sequences, as for a uniform random variable both measures are the same. Considering $(\bar{\bar{W}}^{(1)}, \cdots, \bar{\bar{W}}^{(L)}, \bar{\bar{Y}}_e^{(1)}, \cdots, \bar{\bar{Y}}_e^{(L)})$ as L repetitions of the experiment of super block random variables $(\bar{\bar{W}}, \bar{\bar{Y}}_e)$, we define the event T based on typical sets as follows [18]: Let $\delta > 0$. $T = 1$, if the sequences $\bar{\bar{w}}^{(1\cdots L)}$ and $(\bar{\bar{w}}^{(1\cdots L)}, \bar{\bar{y}}_e^{(1\cdots L)})$ are δ-typical; and $\bar{\bar{y}}_e^{(1\cdots L)}$ is such that the probability that $(\bar{\bar{w}}'^{(1\cdots L)}, \bar{\bar{y}}_e^{(1\cdots L)})$ is δ-typical is at least $1-\delta$, which is taken over $\bar{\bar{w}}'^{(1\cdots L)}$ according to $p(\bar{\bar{W}}'^{(1\cdots L)}|\bar{\bar{y}}_e^{(1\cdots L)})$. Otherwise, we set $T = 0$ and denote $\delta_0 \triangleq \Pr\{T = 0\}$. Then, by Lemma 6 of [18], as $L \to \infty$

$$L\delta_0 \to 0, L\delta \to 0, \text{ and} \quad (21)$$

$$R(\bar{\bar{W}}^{(1\cdots L)}|\bar{\bar{Y}}_e^{(1\cdots L)} = \bar{\bar{y}}_e^{(1\cdots L)}, T = 1)$$
$$\geq L(H(\bar{\bar{W}}|\bar{\bar{Y}}_e) - 2\delta) + \log(1-\delta). \quad (22)$$

We continue as follows.

$$\begin{aligned} R(\bar{\bar{W}}^{(1\cdots L)}|\bar{\bar{Y}}_e^{(1\cdots L)} = \bar{\bar{y}}_e^{(1\cdots L)}, T = 1) & \\ \geq\ & L(H(\bar{\bar{W}}|\bar{\bar{Y}}_e) - 2\delta) + \log(1-\delta) \\ \geq\ & LMN\Bigg(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon_4 \\ & - \frac{2\delta}{MN} + \frac{\log(1-\delta)}{LMN}\Bigg) \\ =\ & LMN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \delta^*\right), \end{aligned} \quad (23)$$

where $\delta^* \to 0$ as $M, N \to \infty$. Thus, for the given ϵ^*, there exists M_2, N_2 s.t. for $M \geq M_2$ and $N \geq N_2$, $\frac{\epsilon^*}{2} \geq \delta^*$. We let $r = LMN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon^*\right)$ and consider the following bound.

$$\begin{aligned} H(K|Y_e^*, G) \geq H(K|Y_e^*, G, T) & \\ \overset{(a)}{\geq}\ & (1-\delta_0)\sum_{y_e^* \in \mathcal{Y}_e^*}\Bigg(H(K|Y_e^* = y_e^*, G, T = 1) \\ & P(Y_e^* = y_e^*|T = 1)\Bigg) \\ \overset{(b)}{\geq}\ & (1-\delta_0)\left(r - \frac{2^{-LMN(\epsilon^* - \delta^*)}}{\ln 2}\right), \end{aligned} \quad (24)$$

where in (a) δ_0 is s.t. $L\delta_0 \to 0$ as $L \to \infty$, (b) is due to Lemma 9 given above and due to (23) and the choice of r. Here, for the given $\epsilon > 0$, there exists M_3, N_3 s.t. for $M \geq M_3$ and $N \geq N_3$, $\frac{2^{-LMN(\frac{\epsilon^*}{2})}}{\ln 2} \leq \frac{\epsilon}{2}$. Hence, we obtain

$$\begin{aligned} I(K; Y_e^*, G) &= H(K) - H(K|Y_e^*, G) && (25) \\ &\leq \delta_0 r + \frac{2^{-LMN(\epsilon^* - \delta^*)}}{\ln 2} && (26) \\ &\overset{(a)}{\leq} \delta_0 LMN + \frac{2^{-LMN(\frac{\epsilon^*}{2})}}{\ln 2} && (27) \\ &\overset{(b)}{\leq} \delta_0 LMN + \frac{\epsilon}{2}, && (28) \end{aligned}$$

where (a) holds if $M \geq M_2$ and $N \geq N_2$ and (b) holds if $M \geq M_3$ and $N \geq N_3$.

Now, we choose some $M \geq \max\{M_1, M_2, M_3\}$. For this choice of M, we choose sufficiently large L and sufficiently large N such that $N \geq \max\{N_1, N_2, N_3\}$ and

$$\delta_0 LMN \leq \frac{\epsilon}{2} \quad (29)$$

$$LM2^{-N^\beta} \leq \epsilon, \quad (30)$$

which holds as $\delta_0 L \to 0$ as $L \to \infty$ in (21). (In fact, due to [18, Lemma 4 and Lemma 6], for any $\epsilon' > 0$, we can take $\delta_0 L \leq \frac{\epsilon'}{L}$ as L gets large.) Therefore, for this choice of L, M, N, we obtain the desired result from (17), (18), (28), due to (29) and (30):

$$H(W^*) \geq LMN\left(E\left[C(W_m)\right] - \epsilon^*\right) \quad (31)$$

$$\Pr\{W^* \neq \hat{W}^*\} \leq \epsilon \quad (32)$$

$$I(K; Y_e^*, G) \leq \epsilon \quad (33)$$

In addition, for this choice of L, M, N, we bound $H(K) \geq r - \epsilon$ due to (24), which shows that the key is approximately uniform. ∎

Few remarks are now in order.

1) Existing code designs in the literature and the previous section of this work assume that Eve's channel is known at Alice and Bob. In the above scheme, Alice and Bob only need the statistical knowledge of eavesdropper CSI. Also, the main channel is not necessarily stronger than the eavesdropper channel, which is not the case for degraded wiretap settings.

2) The above scheme can be used for the wiretap channel of Section IV by setting $M = 0$ to achieve strong secrecy (assuring arbitrarily small information leakage) instead of the weak notion (making the leakage rate small). See also [18].

3) The results can be extended to arbitrary binary-input channels along the same lines, using the result of Section IV. In such a setting, the above theorem would be reformulated with $n = LMN(E[I(W_m)] - \epsilon^*)$ and $r = LMN(E[[I(W_m) - I(W_e)]^+] - \epsilon^*)$. However, the code construction complexity of such channels may not scale as good as that of the erasure channels [8].

VI. Discussion

In this work, we considered polar coding for binary-input DMCs with a degraded eavesdropper. We showed that polar coding can be utilized to achieve non-trivial secrecy rates for this set of channels. If both receiver and eavesdropper have binary-input symmetric channels in addition to the degradedness assumption, this coding technique achieves the secrecy capacity. The results might be extended to arbitrary discrete memoryless channels using the techniques given in [19]. The second focus of this work was the secret key agreement over fading channels, where we showed that Alice and Bob can create advantage over Eve by using the polar coding scheme at each fading block, which is then exploited with privacy amplification techniques to generate keys. This result is interesting in the sense that part of the key agreement protocol is established information theoretically over fading channels by only requiring the statistical knowledge of eavesdropper CSI at the users.

Acknowledgement

The authors are grateful to Erdal Arıkan of Bilkent University for providing comments on an earlier version of this work.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[5] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[6] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. 2007 IEEE Information Theory Workshop (ITW'07)*, Sep. 2007.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2008.

[8] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[9] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. 2010 IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, Jun. 2010, also in CoRR, abs/1001.0210, Jan. 2010. [Online]. Available: http://arxiv.org/abs/1001.0210

[10] E. Hof and S. Shamai, "Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels," submitted for publication, also in CoRR, abs/1005.2759, May 2010. [Online]. Available: http://arxiv.org/abs/1005.2759

[11] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *Technical Report, The Ohio State University*, Feb. 2010, also in CoRR, abs/1003.1422, Mar. 2010. [Online]. Available: http://hdl.handle.net/1811/44969, http://arxiv.org/abs/1003.1422

[12] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. 2009 IEEE International Symposium on Information Theory (ISIT 2009)*, Seoul, Korea, Jun. 2009.

[13] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, EPFL, Lausanne, Switzerland, 2009.

[14] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[15] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[16] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[17] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, 1979.

[18] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Computer Science 1807, Springer*, 2000, pp. 351–368.

[19] E. Sasoglu, E. Arıkan, and E. Telatar, "Polarization for arbitrary discrete memoryless channels," in *Proc. 2009 IEEE Information Theory Workshop (ITW 2009)*, Taormina, Sicily, Italy, Oct. 2009.