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 Arikan. 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. Extension of the coding technique to the multiple-access channels with a degraded eavesdropper is discussed. Finally, 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. Wyner's degraded wiretap channel assumes that the eavesdropper channel is a degraded version of the one seen by the legitimate receiver. Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper, in terms the lower noise level, 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 as an elusive task.

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 of the Ohio State University. A summary of this technical report will appear in 21st Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Sept. 2010, Istanbul, Turkey.

In [5], the authors constructed LDPC based wiretap codes for certain binary erasure channel (BEC) and binary symmetric channel (BSC) scenarios. 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 considers secret communication over a binary-input degraded wiretap channel. Using the polar coding technique of Arikan [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 [1]. The results are also extended to the multiple-access setting, where the coding scheme is shown to achieve non-trivial secrecy rates for both users. Finally, we consider fading wiretap channels and propose a key agreement scheme where the users only assumed to have the statistical knowledge of the eavesdropper CSI. 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

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

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 probability of ML decision error on a single use of the channel.

[1] We acknowledge that the concurrent work [9] independently established the result that polar codes can achieve the secrecy capacity of the degraded wiretap channels, when both main and eavesdropper channels are binary-input and symmetric (Corollary 7 of this note).

Polar codes is recently introduced by Arikan [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], [10]). 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.

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

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

and

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

In order to derive the rate of the channel polarization, the random process Z_n is defined in [8] and in [10]. Basically,

$$\Pr\{Z_n \in (a,b)\} = \frac{|\{i \in \{1,\cdots,N\} : Z(W_{2^n}^{(i)}) \in (a,b)\}|}{N} \tag{5}$$

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

Theorem 2 (Theorem 1 of [10]): 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. Arikan'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 main result of [8] using the bound given in [10].

Theorem 3 (Theorem 2 of [10]): 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

$$P_e(N) = O(2^{-N^\beta}).$$

Sketch of the proof: For any given $\beta \in (0, \frac{1}{2})$ 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 block 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 [11].) ■

This result shows the existence of a polar code $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ achieving the symmetric capacity of W. We remark 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.

A. Polarization for degraded channels

In [11], the following lemma is proven

Lemma 4 (Lemma 4.7 of [11]): 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:

$$p(y_{m_i}, y_{e_i} | x_1^i, y_{m_1}^{i-1}, y_{e_1}^{i-1}) = W(y_{m_i}, y_{e_i} | x_i).$$

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: $f : m \rightarrow X_1^N$ 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.

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

The secrecy is measured by the mutual information leakage rate to the eavesdropper

$$\frac{1}{N} I\left(M; {Y_e}_1^N\right).$$

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

$$\begin{aligned} \frac{1}{N}\log(|\mathcal{M}|) &= R \\ P_e &\leq \epsilon \\ \frac{1}{N} I\left(M; {Y_e}_1^N\right) &\leq \epsilon \end{aligned} \tag{6}$$

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

$$W_m(y_m|x) \tag{7}$$

and the symmetric eavesdropper channel is

$$W_e(y_e|x) = \sum_{y_m \in \mathcal{Y}_m} W_m(y_m|x) W_d(y_e|y_m). \tag{8}$$

Here, the degradation is due to the channel $W_d(y_e|y_m)$.

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

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

and

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

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 $u_{\mathcal{F}_m}$. 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 $\bar{v}_m$ and $u_{\mathcal{F}_m}$, we define the vector $u_{\mathcal{F}_e}(\bar{v}_m)$ with $u_{\mathcal{F}_m}(\bar{v}_m) = u_{\mathcal{F}_m}$ and $u_{\mathcal{F}_e \backslash \mathcal{F}_m}(\bar{v}_m) = \bar{v}_m$. Then, the code $\mathcal{C}_e(\bar{v}_m) \triangleq \mathcal{C}(N, \mathcal{F}_e, u_{\mathcal{F}_e}(\bar{v}_m))$ will be a symmetric capacity achieving polar code for the eavesdropper channel W_e for any $\bar{v}_m$ if the eavesdropper channel is symmetric (as any frozen vector choice for symmetric channels will work [8]). 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, $I(W_m) - I(W_e)$, is achieved by polar coding.

Proof:

Encoding: We map the secret message to be transmitted to $\bar{v}_m$ 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 is the frozen vector of the polar code $\mathcal{C}_m$, $u_{\mathcal{F}_e \backslash \mathcal{F}_m} = \bar{v}_m$, 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

$$H(\bar{V}_r | \bar{V}_m, U_{\mathcal{F}_m}, Y_{e1}^N) \leq H(P_e) + N \log(|\mathcal{X}|) P_e \leq N\epsilon(N), \tag{9}$$

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.

$$\begin{aligned}
I(M; Y_{e1}^N | U_{\mathcal{F}_m}) &= I(\bar{V}_m; Y_{e1}^N | U_{\mathcal{F}_m}) & (10)\\
&= I(\bar{V}_m, \bar{V}_r; Y_{e1}^N | U_{\mathcal{F}_m}) - I(\bar{V}_r; Y_{e1}^N | \bar{V}_m, U_{\mathcal{F}_m}) & (11)\\
&\overset{(a)}{=} I(U_1^N; Y_{e1}^N) - H(\bar{V}_r) + H(\bar{V}_r | \bar{V}_m, U_{\mathcal{F}_m}, Y_{e1}^N) & (12)\\
&\overset{(b)}{\leq} I(X_1^N; Y_{e1}^N) - H(\bar{V}_r) + H(\bar{V}_r | \bar{V}_m, U_{\mathcal{F}_m}, Y_{e1}^N) & (13)\\
&\overset{(c)}{\leq} NI(W_e) - |\mathcal{A}_e| + H(\bar{V}_r | \bar{V}_m, u_{\mathcal{F}_m}, Y_{e1}^N) & (14)\\
&\overset{(d)}{\leq} NI(W_e) - |\mathcal{A}_e| + N\epsilon(N), & (15)
\end{aligned}$$

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 $I(X_1^N; Y_{e1}^N) = \sum\limits_{i=1}^{N} I(X_1^N; Y_{ei} | Y_{e1}^{i-1}) \leq \sum\limits_{i=1}^{N} H(Y_{ei}) - H(Y_{ei} | X_i) = NI(X_i; Y_{ei})$ with a uniformly distributed X_i, and (d) follows from (9) 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

$$\frac{1}{N} I(\bar{V}_m; Y_{e1}^N | U_{\mathcal{F}_m}) \quad \leq \quad \epsilon \tag{16}$$

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, i.e., $C(W_m) - C(W_e)$, of the channel.

V. Secure Transmission over Multiple-Access Channel

A discrete memoryless two-user multiple access channel with an eavesdropper (MAC-E) is denoted by

$$(\mathcal{X}_1 \times \mathcal{X}_2, W(y_m, y_e|x_1, x_2), \mathcal{Y}_m \times \mathcal{Y}_e),$$

for some finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_m, \mathcal{Y}_e$. Here the symbols $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ 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:

$$p(y_{mi}, y_{ei}|x_{11}^i, x_{21}^i, y_{m1}^{i-1}, y_{e1}^{i-1}) = W(y_{mi}, y_{ei}|x_{1i}, x_{2i}).$$

We assume that each transmitter $k \in \{1, 2\}$ has a secret message M_k which is to be transmitted to the receiver in N channel uses and to be secured from the eavesdropper. In this setting, secret codebooks have the following components:

1) The secret message set $\mathcal{M}_k$; $k = 1, 2$. The transmitted messages are assumed to be uniformly distributed over these message sets.

2) A stochastic encoding function $f_k(.)$ at transmitter k which maps the secret messages to the transmitted symbols: $f_k : m_k \rightarrow {X_k}_1^N$ for each $m_k \in \mathcal{M}_k$; $k = 1, 2$.

3) Decoding function $\phi(.)$ at receiver which maps the received symbols to estimates of the messages: $\phi({Y_m}_1^N) = \{\hat{m}_1, \hat{m}_2\}$.

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

$$P_e = \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} \sum_{(m_1,m_2)\in\mathcal{M}_1\times\mathcal{M}_2} \text{Pr}\left\{\phi({Y_m}_1^N) \neq \{m_1, m_2\}|(m_1, m_2) \text{ is sent}\right\}$$

The secrecy is measured by the mutual information leakage rate to the eavesdropper

$$\frac{1}{N} I\left(M_1, M_2; {Y_e}_1^N\right).$$

We say that the rate tuple (R_1, R_2) is achievable for the channel, if, for any given $\epsilon > 0$, there exists a secret codebook such that,

$$\begin{aligned} \frac{1}{N}\log(|\mathcal{M}_1|) &= R_1 \\ \frac{1}{N}\log(|\mathcal{M}_2|) &= R_2, \\ P_e &\leq \epsilon, \end{aligned}$$

and

$$\frac{1}{N} I\left(M_1, M_2; {Y_e}_1^N\right) \leq \epsilon \tag{17}$$

for sufficiently large N.

Finally, we note that the secrecy requirement imposed on the full message set implies the secrecy of individual messages. In other words, $\frac{1}{n}I(M_1, M_2; {Y_e}_1^N) \leq \epsilon$ implies $\frac{1}{n}I(M_k; {Y_e}_1^N) \leq \epsilon$ for $k = 1, 2$.

We focus on a binary-input degraded MAC-E, where the main channel is given by

$$W_m(y_m|x_1, x_2) \tag{18}$$

and the eavesdropper channel is

$$W_e(y_e|x_1, x_2) = \sum_{y_m\in\mathcal{Y}_m} W_m(y_m|x_1, x_2)W_d(y_e|y_m). \tag{19}$$

Here, the degradation is due to the channel $W_d(y_e|y_m)$. Utilizing the scheme given in the previous section together with a successive cancelation scheme for decoding messages, we obtain the following result.

Corollary 8: For a binary-input degraded MAC-E, we define

$$\begin{aligned} W_{1m}(y_m|x_1) &\triangleq \sum_{x_2} p(x_2)W_m(y_m|x_1, x_2) \\ W_{1e}(y_e|x_1) &\triangleq \sum_{x_2,y_m} p(x_2)W_m(y_m|x_1, x_2)W_d(y_e|y_m) \\ W_{2m}(y_m, x_1|x_2) &\triangleq p(x_1)W_m(y_m|x_1, x_2) \\ W_{2e}(y_e, x_1|x_2) &\triangleq \sum_{y_m} p(x_1)W_m(y_m|x_1, x_2)W_d(y_e|y_m) \end{aligned}$$

for uniform input distributions $p(x_1)$ and $p(x_2)$. Then, the secret rate pair

$$R_1 = I(W_{1m}) - I(W_{1e}) \tag{20}$$

$$R_2 = I(W_{2m}) - I(W_{2e}) \tag{21}$$

is achieved by polar coding.

Proof: Please refer to Appendix B. ■

Note that another rate pair that is obtained by reversing the indices above is achievable. The overall region can be stated as the time sharing of the two rate pairs. Here, as noted in the previous section, the secrecy constraint is satisfied w.h.p. for any code pair in the ensembles of users as block length gets large (if an exhaustive search over the ensembles is not possible). But, if the channels W_{1e} and W_{2e} defined in the theorem are symmetric, and sum of the capacity of these channels is equal to the sum capacity of Eve, i.e., $\left\{ \max\limits_{p(x_1)p(x_2)} I(X_1, X_2; Y_e) \right\} = I(W_{1e}) + I(W_{2e})$, then (using this at step (a) of (55)) we can show that any code pair in the ensembles satisfy the reliability and secrecy constraints.

VI. Secret Key Agreement over Fading Wiretap Channels

In this section, we focus on the following key agreement problem: Alice, over fading wiretap channel, would like to agree on a secret key with Bob in the presence of passive eavesdropper Eve. For simplicity, we focus on the special case of binary erasure main and eavesdropper channels, and the results can be extended to arbitrary binary-input channels using the result of Section IV.

Fading blocks are represented by $i = 1, \cdots, ML$ and each block has N channel uses. 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 $l \in [1, L]$ 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 [2]. 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 $u_{\mathcal{A}_M}$. Secret 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

[2] Remarkable, a random walk model with packet erasures can be covered with this model. Also, parallel channel model is equivalent to this scenario.

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.

At this point, if the eavesdropper is degraded, we have

$$\begin{aligned} \frac{1}{N}H(\bar{V}_m^{(i)}) &= C(W_m^{(i)}) - C(W_e^{(i)}) && (22)\\ \frac{1}{N}H(\bar{V}_r^{(i)}) &= C(W_e^{(i)}) && (23)\\ \frac{1}{N}H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}, \bar{V}_m^{(i)}) &\leq \epsilon, && (24) \end{aligned}$$

where the last inequality follows from Fano's inequality, if $\bar{V}_m^{(i)}$ is given to Eve by an oracle, for sufficiently large N. Otherwise, if the main receiver is degraded, we have

$$\begin{aligned} H(\bar{V}_m^{(i)}) &= 0 && (25)\\ \frac{1}{N}H(\bar{V}_r^{(i)}) &= C(W_m^{(i)}) && (26)\\ \frac{1}{N}H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}) &\leq \epsilon, && (27) \end{aligned}$$

for sufficiently large N.

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

$$\frac{1}{N}H(\bar{V}_m^{(i)}) = [C(W_m^{(i)}) - C(W_e^{(i)})]^+, \tag{28}$$

and

$$\frac{1}{N}H(\bar{V}_r^{(i)}) = \min\{C(W_m^{(i)}), C(W_e^{(i)})\}, \tag{29}$$

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 [12]). 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, $H(W^*) \to LMN\, E\,[C(W_m)]$, 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 [13]. 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 [13]. We first state the following definitions and lemma regarding universal hashing, and then formalize the main result of this section in the following theorem.

Definition 9: 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.

There are efficient universal classes, e.g., to map n bits to r bits, class of linear functions given by $r \times n$ matrices needs rn bits to describe [14]. Note that hash function should have complexity as 1) it will be revealed to each user, and 2) Alice and Bob will compute $g(W^*)$. There are more efficient classes with polynomial time evaluation complexity and $O(n)$ description complexity [14].

Generalized privacy amplification, proposed in [13], is based on the following property of universal hashing.

Lemma 10 (Theorem 3, [13]): Let $X \in \mathcal{X}$ be a random variable with distribution P_X and Rényi entropy $R(X) = -\log_2 E[P_X(X)]$. 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

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

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

Theorem 11: For any $\epsilon, \epsilon^* > 0$, let

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

and

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

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, where 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

$$\frac{1}{N} H(\bar{V}_m^{(i)}) - \epsilon_1 \leq \frac{1}{N} H(\bar{V}_m^{(i)}|\bar{Y}_e^{(i)}) \leq \frac{1}{N} H(\bar{V}_m^{(i)}), \tag{30}$$

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 the information carried in $\bar{V}_m$), and

$$\frac{1}{N} H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}, \bar{V}_m^{(i)}) \leq \epsilon_2, \tag{31}$$

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 $M \geq M_1$

$$H(W^*) \geq LMN\left(E\left[C(W_m)\right] - \epsilon^*\right), \tag{32}$$

and

$$\Pr\{W^* \neq \hat{W}^*\} \leq LM2^{-N^{\beta}}, \tag{33}$$

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

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

$$H(W^*|Y_e^*) \;=\; \sum_{l=1}^{L} H(\bar{\bar{W}}^{(l)}|\bar{\bar{Y}}_e^{(l)}) = \sum_{i=1}^{LM} H(\bar{V}_m^{(i)}|\bar{Y}_e^{(i)}) + H(\bar{V}_r^{(i)}|\bar{Y}_e^{(i)}, \bar{V}_m^{(i)}) \tag{34}$$

Focusing on a particular super block, omitting the index (l) in $(\bar{\bar{W}}^{(l)}, \bar{\bar{Y}}_e^{(l)})$, and using (30) and (31) in (34), we obtain

$$\begin{aligned} MN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon_4\right) &\leq H(\bar{\bar{W}}|\bar{\bar{Y}}_e) && (35)\\ &\leq MN\left(E\left[[C(W_m) - C(W_e)]^+\right] + \epsilon_5\right), && (36) \end{aligned}$$

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 10 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 [15]: 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 [15], as $L \to \infty$

$$L\delta_0 \to 0 \text{ and } L\delta \to 0, \tag{37}$$

and

$$R(\bar{\bar{W}}^{(1\cdots L)}|\bar{\bar{Y}}_e^{(1\cdots L)} = \bar{\bar{y}}_e^{(1\cdots L)}, T = 1) \geq L(H(\bar{\bar{W}}|\bar{\bar{Y}}_e) - 2\delta) + \log(1-\delta). \tag{38}$$

We continue as follows.

$$\begin{aligned} R(\bar{\bar{W}}^{(1\cdots L)}|\bar{\bar{Y}}_e^{(1\cdots L)} = \bar{\bar{y}}_e^{(1\cdots L)}, T = 1) &\geq L(H(\bar{\bar{W}}|\bar{\bar{Y}}_e) - 2\delta) + \log(1-\delta)\\ &\geq LMN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \epsilon_4 - \frac{2\delta}{MN} + \frac{\log(1-\delta)}{LMN}\right)\\ &= LMN\left(E\left[[C(W_m) - C(W_e)]^+\right] - \delta^*\right), && (39) \end{aligned}$$

where $\delta^* \to 0$ as $M, N \to \infty$.

Thus, for the given $\epsilon^* > 0$, 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 continue as follows.

$$\begin{aligned}
H(K|Y_e^*,G) &\geq H(K|Y_e^*,G,T)\\
&= \text{Pr}\{T=1\}H(K|Y_e^*,G,T=1)+\text{Pr}\{T=0\}H(K|Y_e^*,G,T=0)\\
&\overset{(a)}{\geq} (1-\delta_0)\sum_{y_e^*\in\mathcal{Y}_e^*} H(K|Y_e^*=y_e^*,G,T=1)P(Y_e^*=y_e^*|T=1)\\
&\overset{(b)}{\geq} (1-\delta_0)\left(r-\sum_{y_e^*\in\mathcal{Y}_e^*}\frac{2^{r-R(W^*|Y_e^*=y_e^*,T=1)}}{\ln 2}P(Y_e^*=y_e^*|T=1)\right)\\
&\overset{(c)}{\geq} (1-\delta_0)\left(r-\frac{2^{-LMN(\epsilon^*-\delta^*)}}{\ln 2}\right) \qquad (40)
\end{aligned}$$

where in (a) δ_0 is s.t. $L\delta_0\to 0$ as $L\to\infty$, (b) is due to Lemma 10 given above, (c) is due to (39) 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

$$\begin{aligned}
I(K;Y_e^*,G) &= H(K)-H(K|Y_e^*,G) &(41)\\
&\leq \delta_0 r+\frac{2^{-LMN(\epsilon^*-\delta^*)}}{\ln 2} &(42)\\
&\leq \delta_0 LMN+\frac{2^{-LMN(\epsilon^*-\delta^*)}}{\ln 2} &(43)\\
&\overset{(a)}{\leq} \delta_0 LMN+\frac{2^{-LMN(\frac{\epsilon^*}{2})}}{\ln 2} &(44)\\
&\overset{(b)}{\leq} \delta_0 LMN+\frac{\epsilon}{2}, &(45)
\end{aligned}$$

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

$$\begin{aligned}
\delta_0 LMN &\leq \frac{\epsilon}{2} &(46)\\
LM2^{-N^\beta} &\leq \epsilon, &(47)
\end{aligned}$$

which holds as $\delta_0 L\to 0$ as $L\to\infty$ in (37). (In fact, due to [15, 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 (32), (33), (45), due to (46) and (47):

$$\begin{aligned}
H(W^*) &\geq LMN\left(E\left[C(W_m)\right]-\epsilon^*\right) &(48)\\
\text{Pr}\{W^*\neq\hat{W}^*\} &\leq \epsilon &(49)\\
I(K;Y_e^*,G) &\leq \epsilon &(50)
\end{aligned}$$

In addition, for this choice of L, M, N, we bound $H(K)\geq r-\epsilon$ due to (40), which shows that the key is approximately uniform. ■

Few remarks are now in order.

1) The results do not depend on random coding arguments. Coding is low complex: a) Any code in the ensemble will work (frozen bits can be set to all zero vector), b) Overall encoding and decoding complexity is $O(LMN\log(N))$ for a total number of LMN channel uses, c) Code construction has $O(N)$ complexity for each block, as the main channel is erasure channel [8].

2) Existing code designs in the literature and also the previous sections 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.

3) In the above scheme, instead of hash function and Rényi entropy, extractor functions and min-entropy can be used [15]. Similar to above, we can obtain

$$H_\infty(W^*|Y_e^* = y_e^*, T = 1) \geq LMN(E[[C(W_m) - C(W_e)]^+] - \delta^*),$$

as min-entropy and entropy are same if the random variable is uniformly distributed. Now by Lemma 9 of [15], for any $\Delta > 0$ and sufficiently large L, there exist an extractor $g : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^r$ with $d \leq \Delta n$ s.t., if V is uniformly distributed over $\{0,1\}^d$ then

$$H(K = E(W^*, V)|Y_e^* = y_e^*, g, V, T = 1) \geq r - 2^{-n^{1/2-o(1)}}.$$

Note that extractors can be efficient compared to universal hashing. For example, while the randomly chosen hash function may require n bits to describe, the extractor can be described with $d \leq \Delta n$ bits with small Δ. If the chosen (hash or extractor) function has to be communicated through the same channel, this property can be exploited to increase the key renewal rate.

4) If the inverse of the hash (or extractor) functions can be computed easily, then this scheme can be used for secure message transmission. The enabling idea is to randomly select the transmitted input (here, information bits of the polar code) among the set $g^{-1}(K)$, where K here denotes the message that we would like to transmit. Then, Bob can recover the message that is secured from the Eve with the above scheme.

5) The result can be extended to the multi-eavesdropper scenario. If the eavesdroppers do not collude, we can use the worst average leakage, i.e., $r = \min_{W_e} LMN(E[[C(W_m) - C(W_e)]^+] - \epsilon^*)$, for the key. If they collude, assuming that there exist a physical degradation order among them, we can use the best eavesdropper channel for each fading block in the expression, i.e., $r = LMN(E[[C(W_m) - C(W_e^*)]^+] - \epsilon^*)$ where the expectation is over the statistics of the best eavesdropper denoted by W_e^*.

6) 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 [15].

7) 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].

VII. Discussion

In this work, we consider polar coding for binary-input point-to-point and multiple-access channels with a degraded eavesdropper. It is shown that polar coding can be utilized to achieve non-trivial secrecy rates for both channels. The results might be extended to arbitrary discrete memoryless channels using the techniques given in [16] (see Appendix A). In addition, results for the multiple-access channels might be enhanced using the rate-splitting technique proposed in [17]. We note that, polar coding for multiple-access channels is recently considered in [18], where the authors show that MAC can be polarized into five different extremal channels. This observation is used to achieve rate pairs on the dominant face of the rate region obtained by uniform inputs in [18]. This technique can be utilized in the secrecy setting by taking advantage of the extremal channels of the main channel over the eavesdropper channel. The second focus of this work is the secret key agreement over wireless 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 statistical knowledge of eavesdropper CSI at the users.

Appendix A
Other Polar Code Results

A. Polarization for an arbitrary DMC

Recently, the channel polarization result of [8] has extended to arbitrary discrete memoryless channels in [16]. These extended result shows polar codes achieving the symmetric capacity of the q-ary DMC W given by

$$I(W) \triangleq \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \frac{1}{q} W(y|x) \log_q \left(\frac{W(y|x)}{\sum\limits_{x'\in\mathcal{X}} \frac{1}{q} W(y|x')} \right), \tag{51}$$

where $|\mathcal{X}| = q$.

B. Polar codes with non-uniform input distributions

The following method, given in [19], is used in [11] and [16] to construct polar codes with non-uniform input distributions. Let $\mathcal{X}$ and $\mathcal{X}'$ be two finite sets with $|\mathcal{X}'| = m$. Then, any distribution $p(x)$ for $x \in \mathcal{X}$ for which $mp(x)$ is an integer $\forall x$ can be implemented by a uniform distribution on $\mathcal{X}'$ and a deterministic map $f : \mathcal{X}' \to \mathcal{X}$. Using this map, we define the augmented channel $W'(y|x') = W(y|f(x'))$. Then, the symmetric capacity of W', $I(W')$, is equal to $I(X;Y)$ with input distribution $p(x)$. This technique can be used to approach the true capacity of any DMC by approximating the capacity achieving input distribution by a rational $p(x)$ and using the above channel augmentation technique ([16]).

Appendix B
Proof of Theorem 8

We define W_{1m}, W_{1e}, W_{2m}, and W_{2e} as given in the theorem.

For a given sufficiently large N and $\beta \in (0, \frac{1}{2})$, let

$$\mathcal{A}_{1m} = \{i \in \{1, \cdots, N\} : Z({W_{1m}}_N^{(i)}) \le \frac{1}{N} 2^{-N^\beta}\},$$

and

$$\mathcal{A}_{1e} = \{i \in \{1, \cdots, N\} : Z({W_{1e}}_N^{(i)}) \le \frac{1}{N} 2^{-N^\beta}\}.$$

Now, consider a polar code $\mathcal{C}_{1m} \triangleq \mathcal{C}(N, \mathcal{F}_{1m}, u_{1\mathcal{F}_{1m}})$ for the channel W_{1m} with some $u_{1\mathcal{F}_{1m}}$, where $\mathcal{F}_{1m} = \mathcal{A}_{1m}^c$. Due to Lemma 4, we have $\mathcal{A}_{1e} \subset \mathcal{A}_{1m}$ and hence $\mathcal{F}_{1m} \subset \mathcal{F}_{1e}$. Now, for any given length $|\mathcal{F}_{1e}| - |\mathcal{F}_{1m}|$ vector $\bar{v}_{1m}$ and $u_{1\mathcal{F}_{1m}}$, we define the vector $u_{1\mathcal{F}_{1e}}(\bar{v}_{1m})$ with $u_{1\mathcal{F}_{1m}}(\bar{v}_{1m}) = u_{1\mathcal{F}_{1m}}$ and $u_{1\mathcal{F}_{1e}\setminus\mathcal{F}_{1m}}(\bar{v}_{1m}) = \bar{v}_{1m}$. Then, the code $\mathcal{C}_{1e}(\bar{v}_{1m}) \triangleq \mathcal{C}(N, \mathcal{F}_{1e}, u_{1\mathcal{F}_{1e}}(\bar{v}_{1m}))$ will be a symmetric capacity achieving polar code for the channel W_{1e} averaged over the ensemble.

We similarly define $\mathcal{A}_{2m}$, $\mathcal{A}_{2e}$, $\mathcal{C}_{2m}$, and $\mathcal{C}_{2e}$ for channels W_{2m} and W_{2e} by replacing the subscript 1 with 2 everywhere above.

Encoding: A code is chosen uniformly from the ensemble by choosing $u_{1\mathcal{F}_{1m}}$ i.i.d. according to uniform distribution. User 1 maps the secrecy message to be transmitted to $\bar{v}_{1m}$ and generate a random vector $\bar{v}_{1r}$, according to uniform distribution over $\mathcal{X}_1$, of length $|\mathcal{A}_{1e}|$. Then, the channel input is constructed with $x_{1_1}^N = u_{1_1}^N B_N F^{\otimes n}$, where $u_{1\mathcal{F}_{1m}}$ is the frozen vector of the polar code $\mathcal{C}_{1m}$, $u_{1\mathcal{F}_{1e}\setminus\mathcal{F}_{1m}} = \bar{v}_{1m}$, and $u_{1\mathcal{A}_{1e}} = \bar{v}_{1r}$.

User 2 maps the secrecy message to be transmitted to $\bar{v}_{2m}$ and generate a random vector $\bar{v}_{2r}$, according to uniform distribution over $\mathcal{X}_2$, of length $|\mathcal{A}_{2e}|$. Then, the channel input is constructed with $x_{2_1}^N = u_{2_1}^N B_N F^{\otimes n}$, where the vector $u_{2_1}^N$ is designed for channels W_{2m} and W_{2e} along the similar lines given above.

Decoding: The main receiver, having $u_{1\mathcal{F}_{1m}}$, decodes both $\bar{V}_{1m}$ and $\bar{V}_{1r}$ over the channel W_{1m} (considering the other user's input, x_2, as noise) with the SC decoder for polar codes with error probability $P_e = O(2^{-N^{\beta}})$ (averaged over the ensemble) achieving a rate $R_1 = \frac{|\bar{v}_{1m}|}{N} = I(W_{1m}) - I(W_{1e})$ for sufficiently large N.

After having $x_{1_1}^N$, it can decode both $\bar{V}_{2m}$ and $\bar{V}_{2r}$ over the channel W_{2m} (given the knowledge of $u_{2\mathcal{F}_{2m}}$) with the SC decoder for polar codes with error probability $P_e = O(2^{-N^{\beta}})$ (averaged over the ensemble) achieving a rate $R_2 = \frac{|\bar{v}_{2m}|}{N} = I(W_{2m}) - I(W_{2e})$ for sufficiently large N.

Security: Employing the SC decoding, the eavesdropper can decode the random vector $\bar{V}_{1r}$ over the channel W_{1e} with error probability $P_e = O(2^{-N^{\beta}})$ (averaged over $\bar{V}_{1m}$ and $U_{1\mathcal{F}_{1e}}$). Utilizing the Fano's inequality, similar to the proof of Theorem 5, we therefore have

$$H(\bar{V}_{1r}|\bar{V}_{1m}, U_{1\mathcal{F}_{1m}}, Y_{e1}^N) \leq N\epsilon_1(N), \tag{52}$$

where $\epsilon_1(N) \to 0$ as $N \to \infty$.

In addition, given the knowledge of $x_{1_1}^N$ (say by an oracle), the eavesdropper can decode $\bar{V}_{2r}$ over the channel W_{2e} with error probability $P_e = O(2^{-N^{\beta}})$ (averaged over $\bar{V}_{2m}$ and $U_{2\mathcal{F}_{2e}}$). Utilizing the Fano's inequality, we therefore have

$$H(\bar{V}_{2r}|\bar{V}_{2m}, U_{2\mathcal{F}_{2m}}, x_{1_1}^N, Y_{e1}^N) \leq N\epsilon_2(N), \tag{53}$$

where $\epsilon_2(N) \to 0$ as $N \to \infty$.

Combining the two above, we have

$$\begin{aligned} H(\bar{V}_{1r}, \bar{V}_{2r}|\bar{V}_{1m}, \bar{V}_{2m}, U_{1\mathcal{F}_{1m}}, U_{2\mathcal{F}_{2m}}, Y_{e1}^N) &\overset{(a)}{\leq} H(\bar{V}_{1r}|\bar{V}_{1m}, U_{1\mathcal{F}_{1m}}, Y_{e1}^N) \\ &\quad + H(\bar{V}_{2r}|\bar{V}_{1m}, \bar{V}_{2m}, U_{1\mathcal{F}_{1m}}, U_{2\mathcal{F}_{2m}}, \bar{V}_{1r}, Y_{e1}^N) \\ &\overset{(b)}{=} H(\bar{V}_{1r}|\bar{V}_{1m}, U_{1\mathcal{F}_{1m}}, Y_{e1}^N) \\ &\quad + \sum_{x_{1_1}^N \in \mathcal{X}_1^{\times N}} H(\bar{V}_{2r}|\bar{V}_{2m}, U_{2\mathcal{F}_{2m}}, X_{1_1}^N = x_{1_1}^N, Y_{e1}^N) \\ &\overset{(c)}{\leq} N\epsilon(N), \end{aligned} \tag{54}$$

where (a) is due to the fact that conditioning does not increase entropy and (b) is due to the fact that $X_{1_1}^N$ is determined by $\bar{V}_{1m}$, $\bar{V}_{1r}$, and $U_{1\mathcal{F}_{1m}}$; and $\{\bar{V}_{1m}, \bar{V}_{1r}, U_{1\mathcal{F}_{1m}}\} \to X_{1_1}^N \to Y_{e1}^N$ form a Markov chain; (c) follows from (52) and (53) with some $\epsilon(N) \to 0$ as $N \to \infty$.

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

$$\begin{aligned} I(M_1,M_2;Y_{e1}^N|U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}}) &= I(\bar{V}_{1m},\bar{V}_{2m};Y_{e1}^N|U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}}) \\ &= I(\bar{V}_{1m},\bar{V}_{2m},\bar{V}_{1r},\bar{V}_{2r};Y_{e1}^N|U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}}) \\ &\quad -I(\bar{V}_{1r},\bar{V}_{2r};Y_{e1}^N|\bar{V}_{1m},\bar{V}_{2m},U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}}) \\ &\leq I(X_{11}^N,X_{21}^N;Y_{e1}^N)-H(\bar{V}_{1r},\bar{V}_{2r}) \\ &\quad +H(\bar{V}_{1r},\bar{V}_{2r}|\bar{V}_{1m},\bar{V}_{2m},U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}},Y_{e1}^N) \\ &\overset{(a)}{\leq} N\left\{I(W_{1e})+I(W_{2e})\right\}-|\mathcal{A}_{1e}|-|\mathcal{A}_{2e}|+N\epsilon(N), \end{aligned} \tag{55}$$

where in (a) we have $I(X_{11}^N,X_{21}^N;Y_{e1}^N)=\sum_{i=1}^N I(X_{11}^N,X_{21}^N;Y_{ei}|Y_{e1}^{i-1})\leq NI(X_1,X_2;Y_e)$ due to the fact that conditioning does not increase entropy; with uniformly distributed channel inputs. As

$$\lim_{N\to\infty}\frac{|\mathcal{A}_{1e}|+|\mathcal{A}_{2e}|}{N} = I(W_{1e})+I(W_{2e}), \tag{56}$$

due to the code construction, and $\epsilon(N)\to 0$ as $N\to\infty$ from (54), we obtain that

$$\frac{1}{N}I(M_1,M_2;Y_{e1}^N|U_{1\mathcal{F}_{1m}},U_{2\mathcal{F}_{2m}}) \leq \epsilon \tag{57}$$

for any given $\epsilon>0$ for sufficiently large N.

Therefore, after an expurgation argument, we can find a code at each user satisfying the reliability and secrecy constraints and achieving the reported rates given in the theorem.

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. 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.

[8] 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.

[9] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," 2010, submitted for publication. [Online]. Available: http://arxiv.org/abs/1001.0210

[10] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Proc. 2010 IEEE International Symposium on Information Theory*, Seoul, Korea, Jun. 2009.

[11] S. B. Korada, "Polar codes for channel and source coding," *Ph.D. Thesis*, May 2009.

[12] P. 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.

[13] 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.

[14] J. L. Carter and M. N. Wegman, “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, pp. 143–154.

[15] 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*, 2000, pp. 351–368.

[16] E. Sasoglu, E. Arikan, and E. Telatar, “Polarization for arbitrary discrete memoryless channels,” 2009, submitted for publication. [Online]. Available: http://arxiv.org/abs/0908.0302

[17] A. J. Grant, B. Rimoldi, R. L. Urbanke, and P. A. Whiting, “Rate-splitting multiple access for discrete memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 47, pp. 873–890, Mar.

[18] E. Sasoglu, E. Telatar, and E. Yeh, “Polar codes for the two-user binary-input multiple-access channel,” in *Proc. 2010 IEEE Information Theory Workshop*, Cairo, Egypt, Jan. 2010.

[19] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.