ON THE OPTIMALITY OF POLAR CODES FOR THE DETERMINISTIC WIRETAP CHANNEL

S. Ali. A. Fakoorian, A. Lee Swindlehurst

Center for Pervasive Communications and Computing (CPCC)
Department of EECS, University of California, Irvine
Irvine, CA 92697, USA
{afakoori, swindle}@uci.edu

ABSTRACT

Wiretap channel introduced by Wyner [1] in 1975, consists of a transmitter with a confidential message for the intended receiver which needs to be kept secret from the eavesdropper. The secrecy capacity of the wiretap channel quantifies the maximum rate at which a transmitter can reliably send a secret message to its intended recipient without it being decoded by an eavesdropper. While the secrecy capacity is achievable based upon a random-coding argument, constructing channel coding schemes that achieve the secrecy capacity of a general wiretap channel is still an open problem. In this paper, we show that polar coding is an optimal coding scheme in achieving the secrecy capacity for the deterministic wiretap channel, where the channel between the transmitter and the intended receiver and the channel between the transmitter and the eavesdropper are arbitrary and deterministic.

Index Terms— Deterministic Channel, Wiretap Channel, Secrecy Capacity, Physical Layer Security, Polar Codes, Channel Polarization.

1. INTRODUCTION

The broadcast nature of a wireless medium makes it very susceptible to eavesdropping, where the transmitted message is decoded by unintended receiver(s). The wiretap channel, first introduced and studied by Wyner [1], is the most basic model that captures the problem of communication security. This work led to the development of the notion of perfect secrecy capacity, which quantifies the maximum rate at which a transmitter can reliably send a secret message to its intended recipient, without it being decoded by an eavesdropper. For a general discrete memoryless wiretap channel, a single-letter expression for the secrecy capacity was obtained by Csiszár and Körner [2], whose result is based on a random coding argument. Such results show that there exist capacity-achieving

channel coding schemes, but they do not show how to construct such codes for a wiretap channel.

In [3], secrecy codes based on low-density parity-check (LDPC) codes that are decodable in linear time are constructed which achieve the secrecy capacity of a special wiretap channel when the main channel is noiseless and the eavesdropper's channel is the binary erasure channel (BEC). In [4] and [5], it is shown that polar codes, introduced by Arikan [6], can be constructed to achieve the secrecy capacity for the binary-input memoryless degraded wiretap channel when both the main and eavesdropper's channels are arbitrary symmetric channels and the marginal channel to the eavesdropper is physically degraded with respect to the marginal channel to the legitimate user. Similar works using polar codes for the wiretap channel are provided in [7], [8].

The notion of polar codes was first introduced for channel polarization by Arikan in [6], where it is shown that polar codes achieve the capacity of arbitrary binary-input symmetric point-to-point discrete memoryless channels with $O(n \log n)$ encoding and decoding complexity where n is the code length. Source polarization has been introduced for lossless compression of binary sources [9], and lossy source compression [10]. Polar codes for the multiple-access channel (MAC) without secrecy constraints was proposed in [11]. Polar codes for the deterministic broadcast channel without secrecy constraints was analyzed in [12].

In this paper, we first obtain the secrecy capacity of the deterministic wiretap channel (DWC), where both the legitimate and eavesdropper's channels are arbitrary and deterministic. Next, we propose a polar coding scheme that achieves the secrecy capacity of the DWC. The secrecy capacity is obtained in Section II, and the secrecy capacity achieving polar code is described in Section III.

We use boldface uppercase letters to denote matrices and vectors. Random variables are written with non-boldface uppercase letters (e.g., X), while the corresponding lowercase letter (x) denotes a specific realization of the random variable. The logarithm is to the base 2. We write $X \sim \text{Ber}(p)$ to denote a Bernoulli random variable (RV) with values in $\{0, 1\}$

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318, and by the National Science Foundation under grant CCF-1117983.

and $P_X(1) = p$. The entropy $H(X)$ of such a RV is denoted as $h(p) = p \log p - (1 - p) \log(1 - p)$.

2. SECRECY CAPACITY OF THE DWC

Consider a wiretap channel where the transmitter has a confidential message W for the intended receiver in the presence of an eavesdropper. For the code-rate R , the message W is uniformly chosen from a set of size $\lfloor 2^{nR} \rfloor$, and is encoded to a codeword $\mathbf{X}$ with a block-length n over an alphabet $\mathcal{X}$. The codeword $\mathbf{X}$ is transmitted over the memoryless wiretap channel, where the channel output vectors $\mathbf{Y}$ and $\mathbf{Z}$ are respectively received by the legitimate user and the eavesdropper. For a general discrete memoryless wiretap channel, a single-letter expression for the secrecy capacity was obtained by Csiszár and Körner [2], [14]

$$C_s = \max_{P_{U|X}} I(U; Y) - I(U; Z) \quad (1)$$

where U is an auxiliary variable satisfying the Markov relation

$$U \rightarrow X \rightarrow (Y, Z).$$

The reliability is measured by the average error probability $P_e(n)$ of the decoded message [5]

$$P_e(n) = \frac{1}{\lfloor 2^{nR} \rfloor} \sum_{i=1}^{\lfloor 2^{nR} \rfloor} P(\hat{W}(\mathbf{Y}) \neq W_i | W = W_i), \quad (2)$$

where $\hat{W}$ represents the decoded message. A secrecy rate R is achievable if there exists a codebook $\mathcal{C}_n$ such that $\lim_{n \rightarrow \infty} P_e(n) = 0$, and also the following secrecy constraint is satisfied

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W|Z) \rightarrow \frac{1}{n} H(W), \quad (3)$$

where $H(W|Z)$ denotes the conditional entropy of the transmitted message W , given the received vector $\mathbf{Z}$ at the eavesdropper.

In this paper, we consider a discrete memoryless deterministic wiretap channel, where the channel between the transmitter and the intended receiver and the channel between the transmitter and the eavesdropper are arbitrary and deterministic, i.e., Y and Z are functions of X or equivalently the channel transition $P(Y|X)$ is a 0-1 function. In the rest of this section, we obtain the secrecy capacity expression for the deterministic wiretap channel.

Theorem 1 *The secrecy capacity of a deterministic wiretap channel is given by*

$$C_s = \max_{P_X} H(Y|Z). \quad (4)$$

Fig. 1. Blackwell wiretap channel.

Proof: The achievability of the secrecy rate $H(Y|Z)$ is simply obtained from the Csiszár-Körner [2] expression (1) by choosing the auxiliary random variable U as $U = Y$. We note that such a choice is possible because Y (and Z) are known at the transmitter. The converse of the theorem is proved using a well-known upper bound on the secrecy capacity of the wiretap channel [14, Eq. 6]

$$\begin{aligned} C_s &\leq \max_{P_X} I(X; Y|Z) \\ &= \max_{P_X} H(Y|Z) - H(Y|X, Z) = \max_{P_X} H(Y|Z) \end{aligned} \quad (5)$$

where (5) follows from the fact that the channel is deterministic.

As an example of a deterministic wiretap channel, the Blackwell channel with $\mathcal{X} = \{0, 1, 2\}$ is shown in Fig. 1. For any fixed distribution P_X , it is seen that out of four possible output combinations, $P_{YZ}(y, z)$ has zero mass for the pair $(1, 1)$.

Corollary 1 *The secrecy capacity of the Blackwell channel in Fig. 1 is $C_s = 1$, which is obtained for $P_X = \{0, \frac{1}{2}, \frac{1}{2}\}$.*

Proof: The proof is simply obtained by letting $P_X(1) = \alpha$, $P_X(2) = \beta$, and $P_X(0) = 1 - (\alpha + \beta)$. By evaluating (5) we have

$$\begin{aligned} C_s &= \max_{P_X} H(Y|Z) = \max_{P_X} (H(Y, Z) - H(Z)) \\ &= \max_{\alpha, \beta} (-\alpha \log \alpha - \beta \log \beta + (\alpha + \beta) \log(\alpha + \beta)) \quad (6) \\ &\text{s.t. } 0 \leq \alpha \leq 1, 0 \leq \beta \leq (1 - \alpha) \end{aligned}$$

which yields $\alpha = \beta = \frac{1}{2}$, and $C_s = 1$.

It is interesting to note that for the Blackwell wiretap channel in Fig. 1, the optimal P_X is such that the symbol with no uncertainty at the eavesdropper side (symbol 0) has zero mass. It is also interesting to note that, in this example, the secrecy capacity equal the ordinary capacity of the point-to-point channel between the transmitter and the intended receiver, without a secrecy constraint. The question is: How to construct a channel coding scheme that achieves the secrecy capacity. We answer this question in the next section for general deterministic wiretap channels.

3. POLAR CODING FOR DWC

In this paper, we assume output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ are binary, i.e., $\mathbb{F}_2$. However, our polar code construction can be generalized to include output alphabets of different cardinalities. Also we note that the following code construction is for the P_X that attains the secrecy capacity given by (5). Our solution is based on the code construction for the deterministic broadcast channel *without* secrecy constraints, proposed in [12].

Let $\mathbf{X}_w$ be a realization of the vector-valued random variable $\mathbf{X}$ for a given confidential message W , where W is uniformly chosen. The secure polar encoding strategy for the given confidential message W is to construct two pairs of n -length binary sequences $\mathbf{U}_w$ and $\mathbf{V}_w$, where $\mathbf{U}_w$ contains information bits, while $\mathbf{V}_w$ contains artificial noise bits. As we will show, the artificial noise bits are selected to keep the entire message as secret as possible. Then $\mathbf{U}_w$ and $\mathbf{V}_w$ make the codeword $\mathbf{X}_w = (x_{1w}, x_{2w}, \dots, x_{nw})$ that goes through the DWC over n channel uses. The received binary vectors at the intended receiver and the eavesdropper after n channel uses are denoted as respectively $\mathbf{Y}_w$ and $\mathbf{Z}_w$.

3.1. Preliminaries

Let $n = 2^l$, and $l \geq 1$. The algebraic polarization is defined in terms of an invertible matrix

$$\mathbf{G}_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes l} \mathbf{B}_n$$

where $\otimes l$ denotes the l th Kronecker power and $\mathbf{B}_n$ is the “bit-reversal” permutation [6], [9]. Denote the polar transformation of the output random variables by [12]

$$\begin{bmatrix} \mathbf{U} \\ \mathbf{V} \end{bmatrix} = \begin{bmatrix} \mathbf{Y} \\ \mathbf{Z} \end{bmatrix} \mathbf{G}_n. \quad (7)$$

Theorem 2 (Theorem 1 [9], Theorem 2 [12]) *Let the random variables $\mathbf{Y}$, $\mathbf{U}$, $\mathbf{Z}$, and $\mathbf{V}$ be related according to Eq. (7). Then, as $n \rightarrow \infty$, for any $\delta \in (0, 1)$ we have*

$$|i \in [1, N] : H(V_i|\mathbf{V}^{i-1}) \in (1 - \delta, 1]| \rightarrow nH(Z) \quad (8)$$

$$|i \in [1, N] : H(U_i|\mathbf{U}^{i-1}, \mathbf{Z}) \in (1 - \delta, 1]| \rightarrow nH(Y|Z), \quad (9)$$

where $\mathbf{V}^{i-1} = \{V_1, V_2, \dots, V_{i-1}\}$ is a $1 \times i - 1$ sub-vector of $\mathbf{V}$, and $|\mathcal{M}|$ represents the size of set $\mathcal{M}$.

The above theorem states that, as n goes to infinity, there exist approximately $nH(Z)$ indices of the $1 \times n$ random vector $\mathbf{V}$ for which the conditional entropy is close to 1. At the same time, there exist approximately $nH(Y|Z)$ indices of the $1 \times n$ random vector $\mathbf{U}$ for which the conditional entropy is close to 1. As will be described below, we will use the high-entropy indices of $\mathbf{U}$ to encode message bits, and the high-entropy indices of $\mathbf{V}$ to encode artificial noise bits.

To track the rate of polarization of the conditional entropy terms $H(V_i|\mathbf{V}^{i-1})$ and $H(U_i|\mathbf{U}^{i-1}, \mathbf{Z})$, the Bhattacharyya Parameter of random variables U_i and V_i is considered. Let two random variables $A \in \{0, 1\}$ and $C \in \mathcal{C}$, where $\mathcal{C}$ is an arbitrary discrete alphabet, have the joint probability mass function P_{AC} . The Bhattacharyya parameter $B(A|C) \in [0, 1]$ is defined as [12]

$$B(A|C) = 2 \sum_{c \in \mathcal{C}} P_C(c) \sqrt{P_{A|C}(0|c) P_{A|C}(1|c)}. \quad (10)$$

It is shown in [9], [13] that $H(A|C)$ is near 0 or 1 if $B(A|C)$ is near 0 or 1, respectively.

For any fixed $0 < \beta < \frac{1}{2}$, let $\delta_n = 2^{-n^\beta}$. Based on the Bhattacharyya parameter, the following sets are defined

$$\mathcal{N}_n = \{i \in [1, N] : B(V_i|\mathbf{V}^{i-1}) \in (1 - \delta_n, 1]\} \quad (11)$$

$$\mathcal{I}_n = \{i \in [1, N] : B(U_i|\mathbf{U}^{i-1}, \mathbf{Z}) \in (1 - \delta_n, 1]\}. \quad (12)$$

As a result of Theorem 2 and the properties of the Bhattacharyya source parameter, for any $\epsilon > 0$ there exists an n large enough so that $|\mathcal{N}_n| > n(H(Z) - \epsilon)$ and $|\mathcal{I}_n| > n(H(Y|Z) - \epsilon)$ [12].

It should be noted that the sets $\mathcal{I}_n$ and $\mathcal{N}_n$ do not depend on the realization of the random variables. In [13, Sec. IV-E], a Monte Carlo sampling approach for estimating Bhattacharyya parameters is reviewed. See, e.g., [15] for other efficient algorithms for finding the high-entropy indices defined in (11)-(12).

3.2. Reliability and Security Constraints

Here we show how polar encoding is able to achieve the secrecy capacity given by (4). Letting $\epsilon > 0$, we want to show that with $n \rightarrow \infty$, the secrecy rate $R \geq H(Y|Z) - \epsilon$ is achievable while the reliability and security constraints, given by (2)-(3), are satisfied. The encoder maps the confidential message W , uniformly chosen from a set of size 2^{nR} , to a codeword $\mathbf{X}_w$, which is transmitted over n channel uses. The received binary vectors at the legitimate receiver and the eavesdropper are $\mathbf{Y}_w$ and $\mathbf{Z}_w$, respectively.

To construct a codeword, first $1 \times n$ binary vectors $\mathbf{U}_w = \{u_{1w}, \dots, u_{nw}\}$ and $\mathbf{V}_w = \{v_{1w}, \dots, v_{nw}\}$ are formed at the encoder, where uniformly selected information bits corresponding to the confidential message W are inserted into the positions indexed by the set $\mathcal{I}_n$, given by (12). Also, $\mathbf{V}_w$ contains artificial noise bits which are chosen uniformly at random and are independent of the confidential message. The artificial noise bits are inserted into the positions indexed by the set $\mathcal{N}_n$, given by (11). The remaining indices in the binary vectors $\mathbf{U}_w$ and $\mathbf{V}_w$ are computed via a bit-by-bit mapping,

which is called successive randomization in [12]. We have

$$\forall i \notin \mathcal{N}_n : v_{iw} = \arg \max_{v \in \{0,1\}} \{ P(V_i = v | \mathbf{V}^{i-1} = \mathbf{V}_w^{i-1}) \} \quad (13)$$

$$\forall i \notin \mathcal{I}_n : u_{iw} = \arg \max_{u \in \{0,1\}} \{ P(U_i = u | \mathbf{U}^{i-1} = \mathbf{U}_w^{i-1}, \mathbf{V} = \mathbf{V}_w) \} , \quad (14)$$

where in (14), we used the fact that, because the polar transform $\mathbf{G}_n$ is invertible, we have

$$P(U_i = u | \mathbf{U}^{i-1} = \mathbf{U}_w^{i-1}, \mathbf{V} = \mathbf{V}_w) = P(U_i = u | \mathbf{U}^{i-1} = \mathbf{U}_w^{i-1}, \mathbf{Z} = \mathbf{Z}_w) .$$

We note that the complexity of this bit allocation is $O(n \log n)$ [9].

Once the binary sequences $\mathbf{U}_w$ and $\mathbf{V}_w$ are constructed, the encoder applies the inverse polar transform [12]

$$\begin{bmatrix} \mathbf{Y}_w \\ \mathbf{Z}_w \end{bmatrix} = \begin{bmatrix} \mathbf{U}_w \\ \mathbf{V}_w \end{bmatrix} \mathbf{G}_n^{-1} \quad (15)$$

where $\mathbf{G}_n^{-1} = \mathbf{G}_n$ in the binary case. Each channel symbol x_{iw} of the codeword $\mathbf{X}_w$ is then formed from the intersection of (y_{iw}, z_{iw}) . If the intersection set is empty, the encoder declares a block error. A block error only occurs at the encoder [12]. Following the proof of error performance of polar coding for the deterministic broadcast channel without secrecy constraint in [13, Sec. V-C], the expected average block error probability of the deterministic wiretap channel is bounded as $P_e(n) = O(2^{-n^\beta})$.

Once the codeword $\mathbf{X}_w$ is constructed and transmitted, the received vectors at the intended receiver and the eavesdropper after n channel uses are respectively $\mathbf{Y}_w$ and $\mathbf{Z}_w$. The legitimate receiver and the eavesdropper apply the $\mathbf{G}_n$ transform to exactly obtain the binary vectors $\mathbf{U}_w$ and $\mathbf{V}_w$, respectively. Assuming that the intended receiver knows the location of message indices $\mathcal{I}_n$, and the eavesdropper knows both $\mathcal{I}_n$ and the location of artificial noise indices $\mathcal{N}_n$, the intended receiver is able to recover the confidential message bits correctly, and the eavesdropper is able to recover the artificial noise bits correctly.

It only remains to prove that the above polar coding scheme is secure. To do so, we need to show that

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W|\mathbf{Z}) \rightarrow \frac{1}{n} H(W) .$$

Let $\mathbf{U}_{\mathcal{I}_n}$ be a $1 \times |\mathcal{I}_n|$ sub-vector of $\mathbf{U}$, which represents $\mathbf{U}$ in message bit indices. We have

$$\begin{aligned} \frac{1}{n} H(W|\mathbf{Z}) &= \frac{1}{n} H(\mathbf{U}_{\mathcal{I}_n}|\mathbf{Z}) \\ &= \frac{1}{n} H(\mathbf{U}_{\mathcal{I}_n}) - I(\mathbf{U}_{\mathcal{I}_n}|\mathbf{Z}) \\ &= \frac{1}{n} H(W) - I(\mathbf{U}_{\mathcal{I}_n}|\mathbf{Z}) \end{aligned} \quad (16)$$

where (16) comes from the fact that W is uniform over the vector $\mathbf{U}_{\mathcal{I}_n}$ of length $|\mathcal{I}_n|$. Using the chain rule of mutual information [5]

$$\begin{aligned} I(\mathbf{U}_{\mathcal{I}_n}, \mathbf{X}; \mathbf{Z}) &= I(\mathbf{U}_{\mathcal{I}_n}; \mathbf{Z}) + I(\mathbf{X}; \mathbf{Z}|\mathbf{U}_{\mathcal{I}_n}) \\ &= I(\mathbf{X}; \mathbf{Z}) + I(\mathbf{U}_{\mathcal{I}_n}; \mathbf{Z}|\mathbf{X}) = I(\mathbf{X}; \mathbf{Z}) , \end{aligned} \quad (17)$$

where (17) follows since the channel is deterministic. Thus, we have

$$\begin{aligned} I(\mathbf{U}_{\mathcal{I}_n}; \mathbf{Z}) &= I(\mathbf{X}; \mathbf{Z}) - I(\mathbf{X}; \mathbf{Z}|\mathbf{U}_{\mathcal{I}_n}) \\ &= H(\mathbf{Z}) - I(\mathbf{X}; \mathbf{Z}|\mathbf{U}_{\mathcal{I}_n}) . \end{aligned} \quad (18)$$

The conditional mutual information $I(\mathbf{X}; \mathbf{Z}|\mathbf{U}_{\mathcal{I}_n})$ is given by

$$\begin{aligned} I(\mathbf{X}; \mathbf{Z}|\mathbf{U}_{\mathcal{I}_n}) &= H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}) - H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z}) \\ &\geq H(\mathbf{X}|\mathbf{U}) - H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z}) \\ &= H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z}) \end{aligned} \quad (19)$$

$$= H(\mathbf{Z}) - H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z}) , \quad (20)$$

where (19) is due to the fact that, since the polar transform $\mathbf{G}_n$ in (7) is invertible, having $\mathbf{U}$ is equivalent to having $\mathbf{Y}$. Similar to the approach used in [5], we let P_{eF} denote the error probability of decoding $\mathbf{X}$, when the decoder has access to both the eavesdropper observation vector $\mathbf{Z}$, and the confidential message vector $\mathbf{U}_{\mathcal{I}_n}$. Thus, the remaining uncertainty in the codeword $\mathbf{X}$ relates only to the random vector $\mathbf{U}_{\mathcal{I}_n^c}$ of size $|\mathcal{I}_n^c|$, where $\mathcal{I}_n \cup \mathcal{I}_n^c = [1, n]$. Using Fano's inequality, the conditional entropy $H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z})$ is therefore bounded according to [5]

$$\begin{aligned} H(\mathbf{X}|\mathbf{U}_{\mathcal{I}_n}, \mathbf{Z}) &\leq h(P_{eF}) + P_{eF} \log(2^{|\mathcal{I}_n^c|} - 1) \\ &\leq h(P_{eF}) + P_{eF} |\mathcal{I}_n^c| \\ &= h(P_{eF}) + n(1 - H(Y|Z)) P_{eF} , \end{aligned} \quad (21)$$

where (21) follows from (12), as shown in [9]. From (16)-(21) it follows that

$$\frac{1}{n} H(W|\mathbf{Z}) \geq \frac{1}{n} H(W) - \frac{1}{n} h(P_{eF}) - (1 - H(Y|Z)) P_{eF} . \quad (22)$$

The error probability P_{eF} in (22) can be upper bounded by the error probability under the encoder error probability in [2]. Thus, $P_{eF} \leq P_e(n) = O(2^{-n^\beta})$, which concludes the proof of (3).

4. CONCLUSION

A secure polar encoding scheme is provided in this paper for the memoryless deterministic wiretap channel, where both the intended receiver's channel and the eavesdropper's channel are arbitrary and deterministic. It was shown that the proposed polar coding scheme achieves the secrecy capacity for the deterministic wiretap channel.

Acknowledgment

Ali Fakoorian would like to thank Naveen Goela from U.C. Berkeley for helpful discussions on [12].

5. REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
- [2] I. Csiszàr and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.
- [3] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2933-2945, Aug. 2007.
- [4] H. MahdaviFar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, Oct. 2011.
- [5] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. IEEE Information Theory Workshop*, Dublin, Ireland, 2010.
- [6] E. Arkan, "Channel polariazation: a method for constructing capacity acheiving codes for symmetric binary-input memoryless channels," *IEEE Trans. on Information Theory*, vol. 55, no. 7, pp. 3051-3073, July 2009.
- [7] O. Koyluoglu and H. El-Gamal, "Polar Coding for Secure Transmission and Key Agreement," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 5, Oct. 2012.
- [8] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer and M. Skoglund, "Nested Polar Codes for Wiretap and Relay Channels," *IEEE Communications Letters*, vol. 14, no. 8, Aug. 2010.
- [9] E. Arkan, "Source polarization," in *Proc. of the IEEE Intern. Symposium on Information Theory*, June 2010.
- [10] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1751-1768, 2010.
- [11] E. Abbe and E. Telatar, "Polar codes for the m-user multiple access channel," *IEEE Transactions on Information Theory*, vol. 58, pp. 5437-5448, August 2012.
- [12] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for the deterministic broadcast channel," in *Proc. Intern. Zurich Seminar on Communications*, Feb. 2012.
- [13] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for broadcast channel," in <http://arxiv.org/abs/1301.6150>, Jan. 2013.
- [14] T. Liu and S. Shamai (Shitz), "A note on secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, 2009.
- [15] I. Tal and A. Vardy, "How to construct polar codes," in <http://arxiv.org/abs/1105.6164>, 2011.