ISIT'2013 1569720323

A New Polar Coding Scheme for Strong Security on Wiretap Channels

Eren Şaşoğlu
University of California San Diego
La Jolla, CA 92093, USA
esasoglu@ucsd.edu

Alexander Vardy
University of California San Diego
La Jolla, CA 92093, USA
avardy@ucsd.edu

***Abstract*—The problem of achieving the secrecy capacity of wiretap channels explicitly and with low complexity has been open since the work of Wyner in 1975. Recently, Mahdavifar and Vardy presented a solution to this problem, based on polar codes, for the class of symmetric and degraded wiretap channels. Their polar coding scheme achieves both security and reliability under the weak security criterion, but does not guarantee reliability under the strong security criterion. The main difficulty in providing both strong security and reliability using polar codes is the existence of a small number of bit-channels that are both unreliable and unsecure. In this paper, a multi-block polar coding scheme that resolves this difficulty is presented. It is shown that this coding scheme achieves the secrecy capacity of symmetric degraded wiretap channels while guaranteeing both reliability and strong security.**

I. Introduction

The wiretap channel [1] models a point-to-point communication system with an eavesdropper. There is a memoryless channel $V\colon \mathcal{X} \to \mathcal{Y}$ from a sender (Alice) to a legitimate receiver (Bob). The eavesdropper (Eve) has access to noisy observations of the sender's channel inputs through a separate memoryless channel $W\colon \mathcal{X} \to \mathcal{Z}$. Alice's aim is to communicate a message reliably to Bob while keeping it hidden from Eve.

A *randomized* (N, R)-code for the wiretap channel consists of messages $M \in [\lceil 2^{NR} \rceil] := \{1, \ldots, \lceil 2^{NR} \rceil\}$, distributions $p_{X_1^N|M}$ on length-N codewords, from which the sender picks the channel input, and a decoder $r\colon \mathcal{Y}^N \to [\lceil 2^{NR} \rceil]$ for the legitimate receiver. Throughout, X_1^N will denote the transmitted codeword, and Y_1^N and Z_1^N will denote the channel output of Bob and Eve, respectively. The reliability of the code is quantified by its average probability of error

$$P_e = \Pr[M \neq r(Y_1^N)]$$

with uniformly distributed messages. The information leaked to Eve is given by the mutual information

$$I(M; Z_1^N).$$

A rate R said to be achievable under the *strong secrecy* requirement if there exists a sequence of (N, R)-codes for which both P_e and $I(M; Z_1^N)$ vanish as $N \to \infty$. The supremum of the achievable rates is known as the *secrecy capacity* of the channel, and is given by [2]

$$\max_{p_{UX}} I(U; Y) - I(U; Z)$$

where the maximum is taken over all joint distributions for which U—X—(YZ) is a Markov chain.

In this paper we will be interested in binary-input wiretap channels in which Eve's channel W is stochastically degraded with respect to Bob's channel V. We will describe a polar coding scheme that achieves the secrecy capacity, which for this class of channels simplifies to [3]

$$C(V) - C(W),$$

where $C(\cdot)$ denotes channel capacity.

Polar coding for binary-input symmetric degraded wiretap channels has been studied by several groups. In [4] the achievability of secrecy capacity under the *weak security* guarantee, where instead of $I(M; Z^N)$, one only requires a vanishing $\frac{1}{N} I(M; Z^N)$, was shown. To our knowledge, this is one of only two secrecy-capacity achieving low-complexity constructions, the other being [7]. The more general problem of determining the achievable rates for arbitrary limiting values of $I(M; Z^N)$ (i.e., the rate-equivocation region) was studied in [5] and [6]. With the exception of a few special cases of channels (see [5] and [4]) the schemes proposed in [4]–[6] fail to achieve both strong security and reliability at rates approaching the secrecy capacity. The purpose of this note is to close this gap.

Recall some standard notation on Arıkan's polar codes [8]: The matrix $G_N = B_N \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]^{\otimes n}$ with $N = 2^n$,

$n = 1, 2, \ldots$ is the standard polarization transform, where B_N denotes the 'bit-reversal' operation. Given a uniformly distributed vector $U_1^N \in \{0,1\}^N$, let $X_1^N = U_1^N G_N$, and let Y_1^N be the output of a binary-input memoryless channel Q with input X_1^N. We will let Q_i denote the ith bit-channel created by the transform, i.e., the channel with input U_i and output (Y_1^N, U_1^{i-1}). The Bhattacharyya parameter of Q will be denoted by $Z(Q)$. (This notation should cause no confusion with the channel output Z_1^N.) Given a set $\mathcal{S} \subseteq [N]$, we will let S denote a random variable that takes values in $\{0,1\}^{|\mathcal{S}|}$. We will sometimes write a random vector U_1^N as a collection of its parts, for instance as $(U_{\mathcal{S}}, U_{\mathcal{S}^c})$.

II. Background

In order to identify the difficulty in achieving strong secrecy with polar codes, we will first review the weak secrecy-achieving polar coding scheme, following [4]. Here, the bit-index set $[N]$ is partitioned into three parts (as opposed to two in point-to-point polar coding): A set $\mathcal{M}$ that carries the message bits, a set $\mathcal{R}$ that carries random bits, and a set $\mathcal{F}$ of 'frozen' bits, whose values are revealed to Bob and Eve prior to transmission. Eve is also assumed to know the choice of the sets $\mathcal{M}$, $\mathcal{R}$, and $\mathcal{F}$ as well as the distribution of the bits in each set. The aim in polar coding is to choose these sets so as to ensure that Bob's probability of misdecoding and Eve's knowledge of the message vanish with increasing blocklength, while maximizing the data rate $|\mathcal{M}|/N$. Note that unlike polar coding for the point-to-point channel, some of the unfrozen bit indices are used to transmit random bits rather than data. The role of these bits is to mask the message from Eve. We will see that an appropriate choice for $\mathcal{R}$ is the set of reliable bits for Eve.

Encoding: The message bits $M \in \{0,1\}^{|\mathcal{M}|}$ are chosen from an arbitrary distribution, and the random bits $R \in \{0,1\}^{|\mathcal{R}|}$ are chosen uniformly and independently of M. The frozen bits F are set to zero. All bits are then assembled into U_1^N. The sender reveals the value of F to Bob and Eve prior to transmission, then transmits $X_1^N = U_1^N G_N$.

Decoding: Upon receiving the channel output $Y_1^N = y_1^N$, Bob decodes U_1^N successively as in [8] using his prior knowledge $F = 0^{|\mathcal{F}|}$. That is, Bob produces his estimate $\hat{u}_1^N$ as

$$\hat{u}_i = \begin{cases} 0 & \text{if } i \in \mathcal{F} \\ 0 & \text{if } i \in \mathcal{M} \cup \mathcal{R} \text{ and } \frac{p_{U_i|Y_1^N U_1^{i-1}}(0|y_1^N, \hat{u}_1^{i-1})}{p_{U_i|Y_1^N U_1^{i-1}}(1|y_1^N, \hat{u}_1^{i-1})} > 1 \\ 1 & \text{otherwise} \end{cases}. \tag{1}$$

Error probability: Recall from [8] that since Bob has prior knowledge of F, the probability of misdecoding can be upper bounded as

$$P_{e,SC} \leq \sum_{i \in \mathcal{M} \cup \mathcal{R}} Z(V_i). \tag{2}$$

The validity of this bound under any distribution of message and frozen bits is due to the symmetry of the channel V [8, Section VI]. Also, although Bob is ultimately not interested in the bits in $\mathcal{R}$, they are included in the error probability expression above due to the successive nature of the decoder. That is, it is not clear whether one can replace the above sum with one over the information set $\mathcal{M}$ only and still get an upper bound on the probability of misdecoding M.

Security: Since the frozen bits F are fixed to zero, Eve's information about the message $I(M; Z_1^N)$ can be written as $I(MF; Z_1^N)$. We can bound the latter quantity in a similar fashion to (2). Indeed, due to the symmetry of the channel $MF \to Z_1^N$ (proved in [4]), we have $I(MF; Z_1^N) \leq I(\tilde{U}_{\mathcal{M}} \tilde{U}_{\mathcal{F}}; \tilde{Z}_1^N)$, where $\tilde{U}_{\mathcal{M}}$ and $\tilde{U}_{\mathcal{F}}$ are independent and uniform versions of M and F and $\tilde{Z}_1^N$ is the corresponding channel output. Now letting $i_1 < i_2 < \ldots < i_{|\mathcal{M} \cup \mathcal{F}|}$ be the elements of $\mathcal{M} \cup \mathcal{F}$, we have

$$\begin{aligned} I(MF; Z_1^N) &\leq I(\tilde{U}_{\mathcal{M}} \tilde{U}_{\mathcal{F}}; \tilde{Z}_1^N) \\ &= \sum_{j=1}^{|\mathcal{M} \cup \mathcal{F}|} I(\tilde{U}_{i_j}; \tilde{Z}_1^N \mid \tilde{U}_{i_1} \cdots \tilde{U}_{i_{j-1}}) \\ &= \sum_{j=1}^{|\mathcal{M} \cup \mathcal{F}|} I(\tilde{U}_{i_j}; \tilde{Z}_1^N \tilde{U}_{i_1} \cdots \tilde{U}_{i_{j-1}}) \\ &\leq \sum_{j=1}^{|\mathcal{M} \cup \mathcal{F}|} I(\tilde{U}_{i_j}; \tilde{Z}_1^N \tilde{U}_1^{i_j - 1}) \\ &= \sum_{j=1}^{|\mathcal{M} \cup \mathcal{F}|} C(W_{i_j}), \end{aligned} \tag{3}$$

where the second equality is due to the independence of $\tilde{U}_{i_j}$'s and (3) follows from the definition of W_i. It follows that the reliability and the strong security requirements can be satisfied by ensuring that the right-hand-sides of

(2) and (3) vanish. One can now turn to basic results in polarization theory in order to find sets $\mathcal{M}$, $\mathcal{R}$, and $\mathcal{F}$ that provide these guarantees. Define for a channel Q and $\beta > 0$ the sets of very reliable and very unreliable indices

$$\mathcal{G}(Q) = \{i\colon Z(Q_i) \leq 2^{-N^\beta}\},$$
$$\mathcal{N}(Q) = \{i\colon I(Q_i) \leq 2^{-N^\beta}\}.$$

The following are immediate corollaries to results in [9] and [10, Lemma 4.7]: For all $0 < \beta < 1/2$,

$$\lim_{N\to\infty} |\mathcal{G}(Q)|/N = C(Q),$$
$$\lim_{N\to\infty} |\mathcal{N}(Q)|/N = 1 - C(Q),$$

and since W is degraded with respect to V,

$$\lim_{N\to\infty} |\mathcal{G}(V) \cap \mathcal{N}(W)|/N = C(V) - C(W),$$
$$\lim_{N\to\infty} |\mathcal{G}(V)^c \cap \mathcal{N}(W)^c|/N = 0. \tag{4}$$

Observe that the right-hand-side of (2) would vanish if one could choose $\mathcal{M} \cup \mathcal{R} \subseteq \mathcal{G}(V)$. Similarly, the right-hand-side of (3) would vanish if $\mathcal{M} \cup \mathcal{F} \subseteq \mathcal{N}(W)$. We may therefore call the indices in $\mathcal{G}(V)$ and $\mathcal{N}(W)$ respectively the *reliable* and the *secure* indices. This motivates partitioning the index set $[N]$ into four sets

$$\mathcal{A} = \mathcal{G}(V) \cap \mathcal{N}(W)$$
$$\mathcal{B} = \mathcal{G}(V) \cap \mathcal{N}(W)^c$$
$$\mathcal{C} = \mathcal{G}(V)^c \cap \mathcal{N}(W)$$
$$\mathcal{D} = \mathcal{G}(V)^c \cap \mathcal{N}(W)^c.$$

It is clear that from the requirements in (2) and (3) that one can assign the bits in $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ as

$$\mathcal{A} = \mathcal{M}$$
$$\mathcal{B} \subseteq \mathcal{R} \tag{5}$$
$$\mathcal{C} \subseteq \mathcal{F}.$$

Note that this allocation sets the rate of the message (asymptotically) to $C(V) - C(W)$, which is the secrecy capacity when both channels V and W are symmetric. Observe, however, that the assignment of $\mathcal{D}$ is problematic: Assigning random bits to $\mathcal{D}$ (i.e., setting $\mathcal{D} \subseteq \mathcal{R}$) may violate the reliability requirement, whereas freezing the bits in $\mathcal{D}$ (i.e., setting $\mathcal{D} \subseteq \mathcal{F}$) may compromise security. On the other hand, we know from (4) that while $\mathcal{D}$ may be nonempty, its size is negligible at large blocklengths. This implies the following:

Theorem 1 ([4])**.** *Along with the assignments in* (5)*, setting $\mathcal{D} \subseteq \mathcal{F}$ guarantees reliability as well as weak security in the sense that*

$$\lim_{N\to\infty} \frac{I(M; Z_1^N)}{N} = 0.$$

III. Coding for Strong Security

It is clear from the discussion above that the assignment of the indices in $\mathcal{D}$ is the only difficulty in achieving reliability and strong security simultaneously. This conflict could be resolved if $U_\mathcal{D}$ were conveyed to Bob separately while keeping it masked from Eve. If transmission is taking place over several blocks—this is typically the case in an operational system—then this can be accomplished by dedicating some of the reliable and secure indices (in $\mathcal{A}$) of the current block to send unsecure and unreliable random bits (in $\mathcal{D}$) of the next block. This guarantees that Bob can decode the problematic bits ahead of time, and that these bits are also masked from Eve. To initiate transmission, one may use a separate code to send the $U_\mathcal{D}$ of the first block. From here on we will assume that we are given such a code sequence $(\phi_N, \psi_N, \epsilon_N)$, with vanishing rate $|\mathcal{D}|/N$, where N is the blocklength, ϕ_N and ψ_N are the respective encoding and decoding functions, and the sequence $\epsilon_N \to 0$ upper bounds the error probability and the information leakage.

In the scheme outlined in the paragraph above, $U_\mathcal{D}$ of each block is transmitted twice, but the rate penalty incurred by this repeated effort is negligible since $\mathcal{D}$ is small. On the other hand, since the blocks in this scheme are dependent due to this retransmission, the single-block mutual information $I(M; Z_1^N)$ no longer quantifies Eve's knowledge of the message. We will see, however, that the dependence between blocks is insignificant, and this scheme guarantees reliability and strong security. We next describe and analyze the scheme in detail.

With sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ defined as above, fix an arbitrary $\mathcal{E} \subset \mathcal{A}$ with $|\mathcal{E}| = |\mathcal{D}|$, and define $\mathcal{M} = \mathcal{A}\backslash\mathcal{E}$. Fix an integer k and let M denote an arbitrarily distributed $k|\mathcal{M}|$-bit message to be sent over $k+1$ blocks. Also let $E_0, \ldots, E_k$ and $B_1, \ldots, B_k$ be uniformly distributed vectors independent of M_1^k. Fix $C_1^k = 0^{k|\mathcal{C}|}$ and reveal C_1^k to Bob and Eve.

Encoding: Divide the message M into k parts $M_1, \ldots, M_k$ of equal length. Encoding is done over $k+1$ blocks.

Block 0: Send $\phi_N(E_0)$.

Block $j = 1, \ldots, k$: Set $D_j = E_{j-1}$. Assemble $(M_j, E_j, B_j, C_j, D_j)$ into U_j and send $U_j G_N$.

Decoding: Let Y_j denote Bob's channel output corresponding to the jth input block. Also let $\mathrm{SC}(y, \mathcal{S}, v_{\mathcal{S}})$ denote the output of the successive cancellation decoder, given by (1), with channel output y, frozen set $\mathcal{S}$ and frozen bits $v_{\mathcal{S}}$. Bob decodes the random bits and the message bits in the $k+1$ blocks successively as

$$\hat{E}_0 = \psi_N(Y_0)$$
$$\hat{U}_j = \mathrm{SC}(Y_j, (\mathcal{C}, \mathcal{D}), (0, \hat{E}_{j-1})) \qquad j = 1, \ldots, k.$$

That is, Bob estimates the bits in $\mathcal{D}$ one block in advance and uses these estimates along with the frozen bits in $\mathcal{C}$ to decode the next block.

Theorem 2. *The encoding/decoding scheme above achieves reliability and strong security. The rate of the scheme approaches the secrecy capacity of symmetric channels for large values of k.*

IV. Proof

The second claim of the theorem is trivial, since the rate of the scheme is

$$\frac{k|\mathcal{M}|}{(k+1)N} = \frac{k(|\mathcal{A}| - |\mathcal{D}|)}{(k+1)N} \approx \frac{k}{k+1}[C(V) - C(W)]$$

for large N, which can be made as close to $C(V) - C(W)$ as desired by choosing a sufficiently large k. We now prove the reliability and the security claims.

A. Error probability

Since the receiver decodes the blocks successively, its probability of misdecoding is identical to that of a genie-aided decoder which in each block uses the correct values of the previous blocks rather than their estimates [8]. The error probability of the latter can be upper bounded in a similar manner to (2). That is, if we let P_e denote the probability of misdecoding any of the bits in the $k+1$ blocks, we have the union bound

$$\begin{aligned} P_e &= \Pr[\hat{E}_0 \neq E_0 \text{ or } \hat{U}_1^k \neq U_1^k] \\ &\leq \epsilon_N + \sum_{j=1}^{k} \Pr[U_j \neq \mathrm{SC}(Y_j, (\mathcal{C}, \mathcal{D}), (0, D_j))]. \end{aligned}$$

Since the channel is symmetric, the error probability term inside the summation is independent of the distribution of U_j [8], and is upper bounded by

$$\sum_{i \in \mathcal{A} \cup \mathcal{B}} Z(V_i) = o(2^{-N^\beta})$$

for all $\beta < 1/2$, where the equality is due to the definition of $\mathcal{A}$ and $\mathcal{B}$. It then follows that

$$P_e \leq \epsilon_N + ko(2^{-N^\beta}),$$

and thus the error probability vanishes for fixed k.

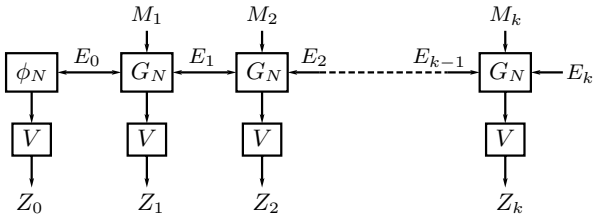

Fig. 1. The coding scheme described in Section III. Inputs B_j, C_j, and D_j to the encoders are not shown.

B. Security

Let Z_j denote Eve's channel output corresponding to the jth input block. The total amount of information leaked to her is given by $I(M_1^k; Z_0^k)$. We will prove strong security by showing that the larger quantity

$$I_k := I(M_1^k E_k; Z_0^k)$$

vanishes. For this purpose, first note that since the channel is memoryless, and since $E_0, \ldots, E_k$ are independent of each other and of the messages $M_1, \ldots, M_k$, we have the Markov chains (see Figure 1)

$$M_1^{k-1} — M_k E_k — Z_k \tag{6}$$

and

$$M_k E_k Z_k — M_1^{k-1} E_{k-1} — Z_0^{k-1}. \tag{7}$$

We can then bound I_k as

$$\begin{aligned} I_k &= I(M_1^k E_k; Z_0^k) \\ &= I(M_1^k E_k; Z_k) + I(M_1^k E_k; Z_0^{k-1} \mid Z_k) \\ &\overset{(a)}{=} I(M_k E_k; Z_k) + I(M_1^k E_k; Z_0^{k-1} \mid Z_k) \\ &\leq I(M_k E_k; Z_k) + I(M_1^k E_k; Z_0^{k-1} \mid Z_k) \\ &\quad + I(Z_k; Z_0^{k-1}) + I(E_{k-1}; Z_0^{k-1} \mid M_1^k E_k Z_k) \\ &= I(M_k E_k; Z_k) + I(M_1^k E_{k-1}^k Z_k; Z_0^{k-1}) \\ &\overset{(b)}{=} I(M_k E_k; Z_k) + I(M_1^{k-1} E_{k-1}; Z_0^{k-1}) \\ &= I(M_k E_k; Z_k) + I_{k-1}, \end{aligned}$$

where (a) is due to (6) and (b) is due to (7). Applying this bound k times we obtain

$$\begin{aligned} I_k &\leq \sum_{j=1}^{k} I(M_j E_j; Z_j) + I(E_0; Z_0) \\ &= \sum_{j=1}^{k} I(M_j E_j C_j; Z_j) + I(E_0; Z_0), \end{aligned} \tag{8}$$

where equality is due to C_j being fixed to zero. Observe that the jth mutual information $I(M_j E_j C_j; Z_j)$

in the sum above only contains random variables from the jth block. Since Eve's channel is memoryless, this mutual information determined by the joint distribution of the random variables in the jth block only, i.e., $(B_jC_jD_jE_jM_jZ_j)$. Note, on the other hand, that encoder inputs B_j, D_j, and E_j are uniformly distributed and independent from each other and from the message M_j, as in single-block polar coding. Therefore, one can use standard results to bound $I(M_jE_jC_j; Z_j)$. In particular, we know from [4] that under this joint distribution, the channel $M_jC_jE_j \to Z_j$ is symmetric, and therefore the mutual information between its input and output is maximized by the uniform distribution on the input. Let $\tilde{M}_j$, $\tilde{C}_j$, and $\tilde{E}_j$ denote uniformly distributed versions of M_j, C_j, and E_j, respectively, with corresponding channel output $\tilde{Z}_j$, and let $i_1 < \ldots < i_{|\mathcal{M}\cup\mathcal{C}\cup\mathcal{E}|}$ denote the elements of $\mathcal{M} \cup \mathcal{C} \cup \mathcal{E}$. We have as in Section II

$$\begin{aligned} I(M_jC_jE_j; Z_j) &\leq I(\tilde{M}_j\tilde{C}_j\tilde{E}_j; \tilde{Z}_j) \\ &\leq \sum_{l=1}^{|\mathcal{M}\cup\mathcal{C}\cup\mathcal{E}|} C(W_{i_l}) \qquad (9) \\ &\leq o(2^{-N^\beta}), \qquad (10) \end{aligned}$$

where (10) follows from the definition of the sets $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{E}$. Combining this with (8) we obtain the bound

$$I(M_1^k; Z_0^k) \leq I_k \leq ko(2^{-N^\beta}) + \epsilon_N$$

which vanishes for fixed k. This completes the proof.

V. Remarks

In the coding scheme above, it may not be immediately clear why the random bits in sets $\mathcal{B}$ and $\mathcal{D}$ were restricted to be uniform and independent of the message; recall that no constraints were imposed on the message distribution. In fact, fixing these bits to arbitrary values would guarantee reliability since Bob's channel assumed symmetric. The reason for the restriction is the security requirement. Indeed, the security of the bit-channels in $\mathcal{M} \cup \mathcal{C} \cup \mathcal{E}$, i.e., the validity of (9) and (10), depends strongly on the random bits being uniformly distributed. See [4, Section IV] for a detailed discussion.

Theorem 2 can be extended to non-symmetric binary-input channels. For such channels, if one restricts the message and the frozen bits in the scheme above to be independent and uniformly distributed, then a simple extention to the analysis in Section IV yields the following.

Theorem 3. *There exists $v \in \{0,1\}^{|\mathcal{C}|}$ such that setting $C_j = v$ for all j in the coding scheme above guarantees reliability and strong security at rates approaching $I(V) - I(W)$, where $I(\cdot)$ denotes* symmetric-capacity.

It is also worth noting that for channels with input alphabets of prime cardinality, Theorems 2 and 3 continue to hold if the polarizing transform is chosen to be G_N with matrix multiplications performed over the corresponding finite field.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Systerm Tech. J.*, vol. 54, no. 8, pp. 1355–1387, October 1975.

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

[3] S. Leung-Yan-Cheong, "On a special class of wire-tap channels," *IEEE Trans. Inform. Theory*, vol. 23, no. 5, pp. 625–627, September 1977.

[4] H. Mahdavifar, A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inform. Theory,* 2011

[5] E. Hof, S. Shamai, "Secrecy-achieving polar-coding," *Proc. IEEE Information Theory Workshop,* pp. 1–5, Aug–Sept. 2010.

[6] M .Andersson, V. Rathi, R. Thobaben, J. Kliewer, M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communication Letters,* vol. 14, no. 8, pp. 752–754, August 2010.

[7] M. Bellare, S. Tessaro, and A. Vardy, Semantic security for the wiretap channel, *Proc. 32-nd Annual Cryptology Conference* (CRYPTO), Santa Barbara, CA., *Springer-Verlag Lecture Notes in Computer Science*, vol. 7417, pp. 294–311, August 2012.

[8] E. Arıkan, "Channel polarization: a method to construct capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory,* vol. 55, no. 7, pp. 3051–3073, July 2009.

[9] E. Arıkan, E. Telatar "On the rate of channel polarization," *Proc. Intl. Symp. Inform. Theory,* pp. 1493–1495, July 2009.

[10] S. B. Korada, *Polar codes for source and channel coding,* PhD Thesis, EPFL 2009.

[11] E. Şaşoğlu, E. Telatar, E. Arıkan, "Polarization for arbitrary discrete memoryless channels," *Proc. IEEE Information Theory Workshop,* pp. 144–148, Oct. 2009.