The Anti-Diversity Concept for Secure Communication on a Two-Link Compound Channel

Joseph J. Boutros
Texas A&M University
Electrical Engineering Dept.
23874 Doha, Qatar
Email: boutros@tamu.edu

Volkan Dedeoglu
Texas A&M University
Electrical Engineering Dept.
23874 Doha, Qatar
Email: volkan.dedeoglu@tamu.edu

Matthieu Bloch
Georgia Institute of Technology
School of Elec. and Comp. Eng.
Atlanta GA 30332, USA
Email: matthieu.bloch@ece.gatech.edu

***Abstract*—We propose new coding schemes for secrecy over a two-link compound channel. Firstly, a non-stochastic scheme is developed based on diversity-deficient LDPC ensembles and a source splitter. Secondly, a stochastic scheme is built from the same splitter with the adjunction of a random sequence. These coding structures achieve perfect secrecy in the algebraic and the information-theoretic sense respectively.**

I. Introduction and Notations

While the applications of Wyner's wiretap channel model [1] to physical-layer security have attracted much interest, see for instance [2][3] and references therein, few constructive and low complexity coding schemes have been developed [4]. Recent efforts exploiting powerful families of error-control codes have nevertheless met some success in certain cases. For instance, low-density parity check codes (LDPC) have been shown to provide secrecy over erasure channels [5][6][7], while Polar codes [8] and invertible extractors [9] have been proven to ensure secrecy over some symmetric channels. Several results also suggest the usefulness of LDPC codes and lattice codes over the Gaussian wiretap channel [10][11][12]. However, all the aforementioned constructions only apply to memoryless wiretap channels with full statistical knowledge of the eavesdropper's channel, which limits their scope of applications. In this paper, we provide a first step towards more robust designs by developing a coding scheme that provides secrecy over a compound wiretap channel [13] in which the eavesdropper gets to observe one of two channels.

Our compound channel has two identical links defined by their transition probabilities $p_{Y|X}(y_1|v)$ and $p_{Y|X}(y_2|w)$ respectively, as depicted in Figure 1. These two links can be any binary memoryless symmetric (BMS) channel, $v, w \in \mathbb{F}_2^{N/2}$ and $y_1, y_2 \in \mathcal{Y}^{N/2}$, where $\mathcal{Y}$ is the output alphabet as observed by the legitimate receiver. It is assumed that a uniform binary source produces K binary elements. The length-N codeword generated by a rate-K/N binary encoder is divided into parts v and w to be transmitted in parallel. For the sake of simplifying the notations, we decided to use a unique letter to denote a random variable and any given value taken by that random variable. We apologize for not keeping the notation rigour as Grimmett and Stirzaker. The reader should figure out easily from the context whether we are referring to a random variable or to a given value.

The work of Joseph J. Boutros and Volkan Dedeoglu was supported by QNRF, a member of Qatar Foundation, NPRP project 5-603-2-243 at Texas A&M University. The work of Matthieu Bloch was supported by the National Science Foundation, award CC 1320298.

Regarding the eavesdropper, our study considers the worst case scenario. Let the channel between Alice and Eve have output $z \in \mathbb{F}_2^{N/2}$. Eve is reading a noiseless copy of one of the two links, i.e. $z = v$ or $z = w$. While assuring that Bob has excellent performance, our aim is to prevent Eve from determining the source bits, part of the source bits, or any information derived from the source bits. Let $M = (a_1, a_2, \ldots, a_K) \in \mathbb{F}_2^K$ be the source message. In the upcoming sections, two types of security are studied:

- **Algebraic security**. Given z, Eve must not be able to find the value of an individual binary element a_i, $\forall i = 1 \ldots K$. This algebraic security is achieved by the means of a non-stochastic LDPC encoder and a weight-2 splitter as described in Section II.
- **Information theoretic security**. The system design must guarantee a zero leakage, i.e. zero mutual information $I(M;z) = 0$ or equivalently $H(M|z) = H(M)$. This perfect secrecy is achieved via a stochastic encoding including a random sequence as described in Section IV.

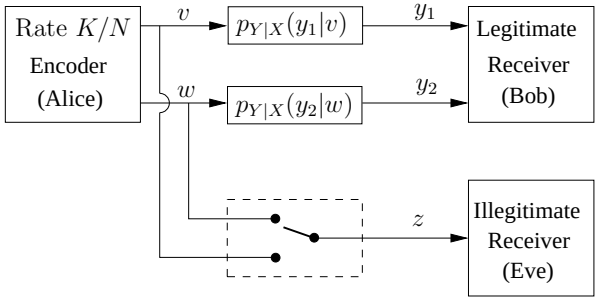

Figure 1. Model of the two-link compound channel. The two links defined by $p_{Y|X}$ are identical. Eve has access to the input of one link only.

II. Anti-Diversity LDPC Encoding

The reader is assumed to be familiar with LDPC codes [14] and diversity methods for fading channels [15][16]. The

compound channel with two parallel links is very similar to block fading channels considered in [17][18]. On a double diversity fading channel, channel coding is supposed to exhibit an error rate performance P_e proportional to $1/\gamma^2$ at high signal-to-noise ratio γ. In such a case, the channel code is said to be a full-diversity code. An example of full-diversity code ensemble is the Root-LDPC ensemble [17][18].

In coding for double diversity on block fading channels, three fundamental rules should be satisfied [17]:

- The coding rate R must satisfy $R \leq \frac{1}{2}$.
- Let the parity-check matrix be divided into two equal size sub-matrices, $H = [H_1|H_2]$. Under Maximum-Likelihood decoding, H_1 and H_2 must have full rank.
- Under iterative message-passing decoding, information bits must be connected to root checknodes of order one or higher.

Security cannot be achieved with a full-diversity code on the two-link compound channel. Double diversity would let Eve determine the missing link and hence all source bits will be revealed. The LDPC code design for security should not satisfy the rules listed above.

Definition 1: The anti-diversity concept refers to a code design where the three fundamental diversity rules are intentionally violated.

The LDPC code constructed via an anti-diversity concept will be called an anti-root LDPC. We briefly describe the structure of an anti-root LDPC. Let $\frac{K}{N}$ be the design rate (R is the effective rate), then $\frac{1}{2} \leq \frac{K}{N} \leq R < 1$. The N binary digits of a codeword are divided into four families. A family of $K/2$ information digits $1i$ and a family of $(N-K)/2$ parity digits $1p$ to be sent on the first link. Similarly, the two families $2i$ and $2p$ are to be sent on the second link. The design rate $\frac{K}{N}$ is taken in the range $[\frac{1}{2}, 1)$. In the special case $\frac{K}{N} = \frac{1}{2}$, a deficient diversity is assured by the last two rules.
Let H_1, the left half part of H, be written as a block matrix

$$H_1 = \begin{bmatrix} A_1 & B_1 \\ C_1 & S_1 \end{bmatrix}. \tag{1}$$

The submatrix A_1 of size $(N-K)/2 \times K/2$ corresponds to edges connecting bitnodes $1i$ to a first type of checknodes $1c$. The submatrix B_1 of square size $(N-K)/2 \times (N-K)/2$ corresponds to edges connecting bitnodes $1p$ to the first type of checknodes $1c$. In a similar fashion, C_1 and S_1 have the same size as A_1 and B_1 respectively. C_1 and S_1 define edges from $2i$ and $2p$ to the second type of checknodes $2c$. Now, the third rule is violated by taking $B_1 = I$, where I is the identity matrix of size $(N-K)/2$. In the special case $\frac{K}{N} = \frac{1}{2}$, A_1 and I commute, then

$$\det(H_1) = det(C_1 + S_1 A_1). \tag{2}$$

Forcing the equality $C_1 = S_1 A_1$ makes H_1 rank deficient, i.e. now the second fundamental rule is violated. The general structure of the anti-root LDPC ensemble is shown in Figure 2. The algebraic security is proved for a scrambler S_1 of any column and row weight greater than or equal to 1.

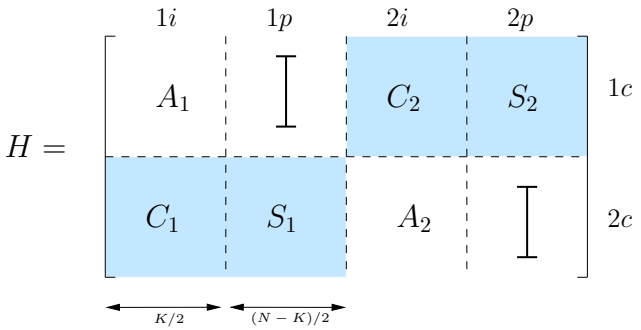

Figure 2. Parity-check matrix of an anti-root LDPC code for violating double diversity. Design rate is $\frac{K}{N}$, where $\frac{1}{2} \leq \frac{K}{N} < 1$.

Our system model is symmetric with respect to the LDPC code and to the two-link channel. Thus, the right half part H_2 has a structure identical to H_1 after switching checknodes $1c$ and $2c$. The expressions of C_1 and C_2 are maintained for any design rate $\frac{K}{N}$.

Definition 2: The anti-root LDPC ensemble is defined by its low-density parity-check matrix in Figure 2 where

$$C_1 = S_1 A_1 \quad \text{and} \quad C_2 = S_2 A_2. \tag{3}$$

The anti-root LDPC is systematic. Eve should not have direct access to source digits [10]. Hence, a source splitter S is placed between the source and the LDPC encoder. The matrix S is $K \times K$, non-singular, and sparse. Suppose that S is regular with degree d_s, i.e. the Hamming weight of all rows and columns is d_s. Let $u = (u_1, u_2, \ldots, u_K) \in \mathbb{F}_2^K$ be the LDPC encoder input. Then $u = MS^{-1}$, or equivalently $M = uS$. The latter is an operation that splits each source digit into d_s digits [19][20]. In this paper, we restrict the splitter to have a degree $d_s = 2$, except for one row and one column in S that have a degree equal to 1.

Lemma 1: Consider a quasi-regular weight-2 non-singular splitter S, except for one row and one column whose degree is 1. Then, S is equivalent to a double diagonal splitter S_0,

$$S = \Pi \cdot S_0 \cdot \Pi', \tag{4}$$

where Π and Π' are $K \times K$ permutation matrices.
In the sequel, we assume that $S = S_0$, i.e. we have

$$a_i = u_i + u_{i+1}, \tag{5}$$

for $i = 1 \ldots K-1$ and $a_K = u_K$. We force to zero the last source bit, $a_K = u_K = 0$. The exact message entropy is $H(M) = K - 1$ bits instead of K. The structure of the non-stochastic coding scheme is shown in Figure 3. The splitter K-bit output $u = (1i \,\&\, 2i)$ is dispatched at the LDPC encoder input such that the $K/2$ bits at odd positions go to $1i$ and the $K/2$ bits at even positions go to $2i$. Thus, Eve must know both family of bits $1i$ and $2i$ in order to find the source message M. When $z = v$, Eve knows all bits $1i$ but the bits $2i$ are all missing. The anti-root LDPC does not allow Eve to find any of the missing bits $2i$. Similarly, when $z = w$, the anti-root LDPC does not allow Eve to find $1i$. The proof of the following theorem is based on (3) and (5).

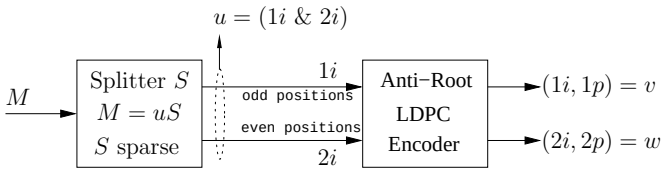

Figure 3. The non-stochastic encoder converts the source message M into half codewords v and w to be sent on each link. $M \in \mathbb{F}_2^K$, $v, w \in \mathbb{F}_2^{N/2}$.

Theorem 2: The anti-root LDPC ensemble of design rate $\frac{K}{N} \in [\frac{1}{2}, 1)$ guarantees the algebraic security of the communication system between Alice and Bob.

Given the non-stochastic scheme which is algebraically secure for any block length N, the next section studies the asymptotic performance of Bob for N sufficiently large.

III. Legitimate Receiver's Performance

Many anti-root LDPC ensembles can be defined, a given ensemble depends on how the submatrices A_1, S_1, A_2, and S_2 are constructed. Due to the lack of space, we restrict this section to a design rate $\frac{K}{N} = \frac{1}{2}$ and to $A_1 = \Pi_1$ and $A_2 = \Pi_2$, where Π_1 and Π_2 are uniformly chosen in the set of $\frac{K}{2} \times \frac{K}{2}$ binary permutation matrices.

The asymptotic performance of Bob under iterative message passing is found via density evolution (DE) [14]. The anti-root LDPC defined by its parity-check matrix H in Figure 2 and by (3) is a multi-edge type code on graphs. As in [17][18], an extra difficulty arises because only the performance on information bits is relevant. Hence, we define the following polynomials to be used by DE at bitnodes and checknodes. The global degree distribution of H from an edge perspective, at bitnodes and checknodes respectively, is [14]:

$$\lambda(x) = \sum_{i=2}^{d_b} \lambda_i x^{i-1}, \quad \text{and} \quad \rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}. \tag{6}$$

In this section, it is assumed that $\rho_j = 0$ for j odd. We introduce an edge-perspective polynomial $\tilde{\lambda}(x)$ when one edge is missing [18] and a node-perspective polynomial $\mathring{\lambda}(x)$,

$$\tilde{\lambda}(x) = \sum_{i=1}^{d_b-1} \tilde{\lambda}_i x^{i-1} = \frac{\bar{d}_b}{\bar{d}_b - 1} \sum_{i=1}^{d_b-1} i \ \lambda_{i+1}/(i+1) \ x^{i-1}, \tag{7}$$

$$\mathring{\lambda}(x) = \sum_{i=2}^{d_b} \mathring{\lambda}_i x^{i-1} = \bar{d}_b \sum_{i=2}^{d_b} \lambda_i / i \ x^{i-1}, \tag{8}$$

where $\bar{d}_b$ is the average degree of bitnodes. The polynomials $\tilde{\rho}(x)$ and $\mathring{\rho}(x)$ are defined in a similar manner for checknodes. Finally, two bivariate polynomials are necessary due to the separation of a checknode into two parts for information and parity bits on the same side of H,

$$\mathring{\rho}(x, y) = \sum_{j=2}^{d_c} \mathring{\rho}_j x^{(j-2)/2} y^{(j-2)/2}, \tag{9}$$

$$\hat{\rho}(x, y) = \sum_{j=1}^{(d_c-2)/2} \hat{\rho}_j x^{j-1} y^j = \sum_{j=1}^{(d_c-2)/2} \frac{2j\mathring{\rho}_j}{\bar{d}_c - 2} x^{j-1} y^j. \tag{10}$$

For a general anti-root ensemble with two distinct links in the compound channel, density evolution may involve up to eight message densities. In this section, due to the identical links and to the LDPC code symmetry, DE equations require two densities only: a- f is the probability density function of log-ratio messages from bitnode $1i$ to checknode $2c$, from $1p$ to $2c$, from $2i$ to $1c$, and from $2p$ to $1c$. b- q is the probability density function of log-ratio messages from bitnode $1i$ to checknode $1c$, from $1p$ to $1c$, from $2i$ to $2c$, and from $2p$ to $2c$. After drawing the local neighborhood of each type of bitnodes (tree representations omitted due to lack of space), we find the following DE equations at decoding iteration $m+1$:

$$q^{m+1} = \mu \otimes \mathring{\lambda}\left(\hat{\rho}(f^m, f^m) \odot (q^m)^{\odot 2}\right),$$

$$f^{m+1} = \mu \otimes (q^m \odot \mathring{\rho}(f^m, f^m)) \otimes \tilde{\lambda}\left(\hat{\rho}(f^m, f^m) \odot (q^m)^{\odot 2}\right),$$

where μ is the density at the channel output, $\otimes$ and $\odot$ denote convolution at bitnode and checknode levels.

Theorem 3: Consider a rate-$1/2$ anti-root LDPC ensemble. If the ensemble is regular then DE reduces to one equation $f^{m+1} = \mu \otimes \lambda(\rho(f^m))$, i.e. the anti-root LDPC has the same decoding threshold as a regular fully-random LDPC ensemble.

In the regular case, the constraint in (3) did not weaken the LDPC code. For irregular ensembles, thresholds can be optimized by a judicious choice of $\lambda(x)$ and $\rho(x)$.

IV. Stochastic Encoding for Two Links

A non-stochastic algebraically-secure encoding scheme has been described in the previous sections and its performance analyzed via density evolution. Now, we would like to replace algebraic security by perfect secrecy in the information-theoretic sense. A perfectly secure stochastic encoding structure is proposed in this section.

In the non-stochastic case, we had $H(M) = K$ (we omit $a_K = 0$ in order to simplify the notations). The conditional message entropy was given by

$$H(M|z = v) = H(1i|z = v) + H(2i|z = v, 1i) = H(2i|v).$$

The information leakage between v and $2i$ is unknown and may depend on the particular choice of submatrices inside H. Nevertheless, we always have $0 < H(2i|v) \leq K/2$. Similar arguments can be made for $z = w$ and $H(1i|w)$. In summary, the non-stochastic coding scheme satisfies

$$H(M|z) \leq \frac{K}{2} < K = H(M). \tag{11}$$

Our stochastic scheme will sacrifice $K/2$ bits in the message by reducing the entropy of the message to $H(M) = K/2$ to achieve perfect secrecy in the information theoretic sense after satisfying $H(M|z) = H(M) = K/2$.

The splitter input is modified to include both $M = (a_1, a_2, \ldots, a_{K/2})$ and a zero sequence of length $K/2$. Let $r = (r_1, r_2, \ldots, r_{K/2})$ be a random sequence of $K/2$ independent uniform binary digits. r is added to both splitter

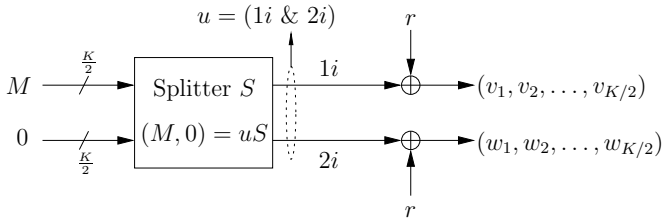

Figure 4. The $K \times K$ splitter in the stochastic scheme reads a message M of $K/2$ bits and a zero sequence of $K/2$ bits. A random sequence of $K/2$ bits is applied at the splitter output before channel transmission.

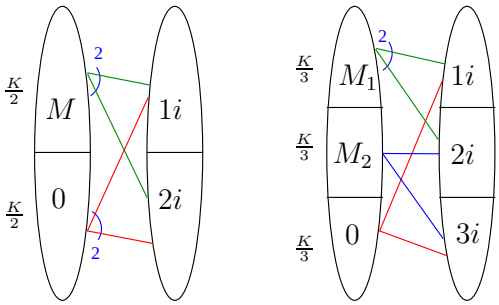

Figure 5. Splitter structure for stochasting encoding for two and three links respectively. The sparse graph represents the expression $(M, 0) = uS$ where S is sparse with degree 2.

outputs. The stochastic structure is shown in Figure 4 where the splitter output fills $K/2$ bits in v and $K/2$ bits in w. The remaining $N - K$ bits in v and w will be equal to parity bits of an LDPC encoder. The analysis below is valid for a two-link anti-root LDPC and for two separate length-$N/2$ LDPC codes. The splitter structure is also illustrated in Figure 5. In a straightforward manner, Theorem 4 can be generalized to an eavesdropper reading one link out of L links, for any $L \geq 2$.

Theorem 4: The stochastic encoding scheme yields $H(M|z) = \frac{K}{2} = H(M)$ on a two-link compound channel, i.e. it is perfectly secure in the information-theoretic sense.

Proof. A sketch of the proof is given. Notice that the zero sequence at the splitter input makes $2i$ a permuted version of $1i$. So $H(2i|z, 1i) = 0$. The equivocation is $H(M|z) = H(1i, 2i|z) = H(1i|z) + H(2i|z, 1i) = H(1i|z)$. Consider $z = v$. For the case of two separate length-$N/2$ codes, we have $H(1i|v) = H(1i|1i + r) = H(1i) = K/2$. For an anti-root LDPC, $H(1i|v) = H(1i|1i + r, 1p)$, the latter is equal to $H(1i|1i + r) = K/2$ because $1p$ is a function of $1i + r$ only thanks to the splitter. Similar proof is made for $z = w$. □.

V. Conclusion

We proposed two original coding schemes for secure communication over a two-link compound channel. A non-stochastic scheme has been developed based on diversity-deficient LDPC ensembles and a source splitter. The anti-root LDPC code guarantees perfect algebraic security. Its joint structure makes it twice longer than two separate LDPC codes for each link and forbids Eve from correcting channel errors when $z = y_1$ or $z = y_2$. The second scheme is stochastic and attains perfect information-theoretic secrecy. It is built from a splitter with the adjunction of a random sequence.
Our work is related to methods in secret sharing such as the material found in [21][22][23], but our channel model does not include feedback and our aim is to increase the information rate rather than finding the worst channel conditions.

References

[1] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 13551387, Oct. 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai, *Information-Theoretic Security*, Now Publishers, 5 (1–5), pp. 355-580, 2009.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[4] W.K. Harrison, J. Almeida, M.R. Bloch, S.W. McLaughlin, and J. Barros, "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41-50, 2013.

[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. Inform. Theory*, vol. 53, no. 8, pp. 2933-2945, Aug. 2007.

[6] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. Inform. Forensics Sec.*, vol. 6, no. 3, pp. 585-594, Sept. 2011.

[7] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," *in Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, St. Petersburg, Russia, Aug. 2011, pp. 2393-2397.

[8] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 10, pp. 6428-6443, 2011.

[9] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," *in Advances in Cryptology, CRYPTO 2012* (Lecture Notes in Computer Science, vol. 7417). Berlin, Heidelberg, Germany: Springer-Verlag, pp. 294-311.

[10] M. Baldi, M. Bianchi, and Franco Chiaraluce, "Non-Systematic Codes for Physical Layer Security," *in Proc. IEEE Information Theory Workshop (ITW 2010)*, pp. 1-5, Dublin, Ireland, Aug. 30 - Sept. 3, 2010.

[11] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inform. Forensics Sec.*, vol. 6, no. 3, pp. 532-540, Sept. 2011.

[12] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehl, "Semantically secure lattice codes for the Gaussian wiretap channel," *Computing Research Repository*, Oct. 2012, pp. 1-19.

[13] Y. Liang, G. Kramer, H. V. Poor and S. Shamai, "Compound Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, 2009, 142374, 1-12.

[14] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[15] D.N.C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

[16] E. Biglieri, *Coding for Wireless Channels*, New York, Springer, 2005.

[17] J.J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, "Low-Density Parity-Check Codes for Nonergodic Block-Fading Channels," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4286-4300, Sept. 2010.

[18] J.J. Boutros, "Diversity and coding gain evolution in graph codes," *in Proc. Information Theory and Appl. (ITA'2009)*, pp. 34-43, UCSD, San Diego, Feb. 2009.

[19] G. Shamir and J. Boutros, "Non-systematic low-density parity-check codes for nonuniform sources," *in Proc. International Symp. on Information Theory (ISIT 2005)*, Adelaide, Australia, pp. 18981902, Sept. 2005.

[20] A. Alloum, J. Boutros, G. Shamir, and L. Wang, "Non-systematic LDPC codes via scrambling and splitting," *in Proc. Allertons Conference on Comm. and Control*, Monticello, Illinois, pp. 1879-1888, Sept. 2005.

[21] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *Journal of the ACM*, vol. 40, no. 1, pp. 1747, Jan. 1993.

[22] T. Rabin, "Robust sharing of secrets when the dealer is honest or cheating," *Journal of the ACM*, vol. 41, no. 6, pp. 1089-1109, Nov. 1994.

[23] Q. Yang and Y. Desmedt, "General Perfectly Secure Message Transmission Using Linear Codes," *Advances in Cryptology - ASIACRYPT 2010*, vol. 6477, pp. 448-465, Dec. 2010.