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.

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.

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
Forcing the equality 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.

- The coding rate $R$ must satisfy $R < 1$.
- 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 $K/N$ be the design rate ($R$ is the effective rate), then $1/2 < K/N < R < 1$. 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 $K/N$ is taken in the range $[1/2,1)$. In the special case $K/N = 1/2$, 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 $K/N = 1/2$, $A_1$ and $I$ commute, then

$$\det(H_1) = \det(C_1 + S_1A_1). \tag{2}$$

Forcing the equality $C_1 = S_1A_1$ 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.

\[ H = \begin{bmatrix} A_1 & B_1 & C_2 & S_2 \\ C_1 & S_1 & A_2 & \end{bmatrix} \]

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

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

$$C_1 = S_1A_1 \quad \text{and} \quad C_2 = S_2A_2. \tag{3}$$

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 $S_0$, where $\Pi$ and $\Pi'$ 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 $u = (1i \text{ and } 2i)$ 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).
The anti-root LDPC ensemble of design rate \( \frac{K}{2} \in [\frac{1}{2}, 1) \) 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 \( \frac{K}{2} = \frac{1}{2} \) and to \( A_1 = \Pi_1 \) and \( A_2 = \Pi_2 \), where \( \Pi_1 \) and \( \Pi_2 \) are uniformly chosen in the set of \( \frac{L}{2} \times \frac{L}{2} \) 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 has the following polynomials to be used by DE at bitnodes and checknodes.

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 has 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]:

\[
\begin{align*}
\lambda(x) &= \sum_{i=2}^{d_x} \lambda_i x^{i-1} , \quad \text{and} \quad 
\rho(x) &= \sum_{j=2}^{d_x} \rho_j x^{j-1} . 
\end{align*}
\]

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

\[
\begin{align*}
\hat{\lambda}(x) &= \sum_{i=1}^{d_x-1} \hat{\lambda}_i x^{i-1} = \frac{d_b}{d_v} - 1 \sum_{i=1}^{d_x-1} i \lambda_{i+1} / (i+1) x^{i-1} , \\
\hat{\lambda}(x) &= \sum_{i=2}^{d_x} \lambda_i x^{i-1} = \frac{d_b}{d_v} \sum_{i=2}^{d_x} \lambda_i / i x^{i-1} ,
\end{align*}
\]

where \( d_b \) is the average degree of bitnodes. The polynomials \( \hat{\rho}(x) \) and \( \hat{\rho}(x) \) 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 \( H \),

\[
\hat{\rho}(x, y) = \sum_{j=2}^{d_x} \rho_j x^{(j-2)/2} y^{(j-2)/2} ,
\]

\[
\rho(x, y) = \sum_{j=1}^{d_x} \rho_j x^{(j-2)/2} y^{(j-2)/2} .
\]

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 the LDPC code symmetry, DE equations require two densities only: \( a \cdot f \) is the probability density function of log-ratio messages from bitnode \( i \) to checknode \( 2c \), from \( 1p \) to \( 2c \), from \( 2i \) to \( 1c \), and from \( 2p \) to \( 1c \). \( b \cdot q \) 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 \( m + 1 \):

\[
f^{m+1} = \mu \odot (q^m \odot \hat{\rho}(f^m, f^m)) \odot \tilde{\lambda}(f^m, f^m) \odot (q^m \odot 2 \hat{\rho}(f^m, f^m)) ,
\]

where \( \mu \) is the density at the channel output, \( \odot \) and \( \odot \) denote convolution at bitnode and checknode levels.

### 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 \( \alpha_K = 0 \) in order to simplify the notations). The conditional message entropy was given by

\[
H(M|z = v) = H(1|z = v) + H(2|z = v, 1i) = H(2|i|v) .
\]

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

\[
H(M|z) \leq \frac{K}{2} < K = H(M) .
\]

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 stochastically 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 $r$ 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