An Encryption and Error-Control Coding scheme based on Non binary LDPC codes

M. C. Liberatori, D. M. Petruzzi, L. Coppolillo, J. C. Bonadero, J. Castiñeira Moreira

Laboratorio de Comunicaciones, Facultad de Ingeniería, Universidad Nacional de Mar del Plata, Argentina.

{mlibera, petruzzi, casti}@fi.mdp.edu.ar

Abstract. In this paper we present a combined error-control coding and encryption scheme that provides to a given system with both high levels of reliability of the transmission and security. These two aims are usually present in wireless data transmission systems. The scheme is based on efficient Non Binary Low Density Parity Check codes which were selected for this design because they outer perform their binary counterparts. By means of a set of operations over the parity check matrix of the code, encryption capabilities are added to the scheme, without producing any degradation in the corresponding Bit Error Rate performance, as usually happens when encryption and error control coding are applied separately.

Keywords: Non binary LDPC codes. Encryption

1 Introduction

Many communications systems in practical use are based on wireless operation, and are related to data transmission, which normally requires from data encryption and security. This is the case of wireless data networks. In such environments signal power levels rapidly decay and are strongly affected by the presence of noise in the channel. A measure of the reliability of the data transmission is usually characterized by a given Bit Error Rate (BER). On the other hand, in wireless networks data need to be encrypted for providing the transmission with levels of security.

First-Encrypt-Then-Encode approach is a traditional scheme in every communication system. Cryptographic algorithms process information to provide security but their decryption counterpart needs an errorless input to perform well. On the other hand, error-correcting algorithms handle errors in the input data and are not designed to provide security. The traditional approach applies cryptography and then error correcting techniques by a sequential execution of two separate algorithms.

Cryptocoding is a different approach, in which encryption and error-correction techniques are performed in a single step.

As said above, one direct approach to provide a given communication system with both security and reliability of the transmission, is to apply separately an algorithm for encryption, and an error-control code for a reliable operation in the presence of noise in the channel.
It has been found in [1] that schemes of this type are quite efficient, but they always suffer from a given degradation because, in general terms, encryption is a procedure that generates error propagation, especially in those routines of the algorithm related to diffusion operations. This has been analysed in [2, 3] for the particular case of the AES algorithm. A combination of an encryption algorithm and an efficient error-control code like an LDPC code, leads to a mitigation of the error propagation effect, but this degradation still remains even being mitigated, because it is essential to the encryption procedure.
Iterative decoded error-control codes like LDPC [4] and turbo [5] codes can be suitable options to be properly combined with these encryption algorithms to design a communication system with both good BER performance and security properties. However, a loss in BER performance is always present, mitigated or not, in theses schemes.

The design of new schemes that could provide to a given communications system with both security and reliability, appears as an interesting matter of work. In our design, the main idea is to obtain encryption and error-control coding by using a combined scheme. This combined scheme should maximize the encryption capability, and also provide an efficient error control, without generating degradation in the BER performance.
One of the first papers that deals with the use of error control coding for encryption purposes has been proposed by R. MacEliece [6]. A different approach has been carried out by Niederreiter [7]. In these papers Error-Control coding is used to give form to an NP problem, as an encryption technique.
McEliece´s proposal is a public key encryption system which uses error correcting codes to encrypt information. To transmit a message, it is first multiplied by a modified generator matrix G' to form the codeword, then, an error pattern of weight *t* (error correcting capability of the code) is added to the codeword and this information is transmitted over the noisy channel.
In the scheme, G' is the public key obtained from G, a true generator matrix which is pre-multiplied by a random dense non-singular matrix S and post-multiplied by a random permutation matrix P, so that $G' = SGP$. The secret key consist of G, S and P. The error correcting capability of the code, *t*, is part of the public key. The success of the decoding - decrypting process depends only on the number of errors and its security is based on the hardness of the decoding problem. To be effective, McEliece´s cryptosystem requires large block lengths with capability to correct high numbers of errors. This involves high computation overhead.

The functions of error correction and security were integrated in works like the Godoy and Pereira Scheme [8] which derive new generator matrices from existing generator matrices by row permutations. Also, [9] proposed a private key cipher that uses a class of non-linear channel codes but the scheme suffers from reduction in error correcting capacity.

The use of channel codes in cryptocoding must satisfy the diffusion property of a block cipher and at the same time, the codes must maintain the best possible level in their error correction capability.

On the other hand some interesting research has been carried out quite recently regarding the so called Non -Binary Low-Density Parity-Check (NB-LDPC) Codes [10]. NB-LDPC codes have been introduced by Mackay y Neal [11].
An NB-LDPC code is simply an LDPC code with a sparse parity check matrix containing elements that could be defined over groups, rings or fields. We will use NB-LDPC codes defined over finite fields $GF(2^m)$, where m is a positive integer greater than 1.
Mackay and Neal presented the idea of LDPC codes over finite fields. They have shown that NB-LDPC codes can achieve increases in performance over their binary counterparts if the size of the corresponding finite field is increased. Mackay also showed the generalization of the sum–product algorithm to decode NB-LDPC codes, but the decoding complexity increased enormously with the order of the finite field. They were able to decode only NB-LDPC codes over small finite fields.
Non-binary LDPC codes are usually constructed by taking the parity check matrix of a known binary LDPC code and replacing its nonzero elements with randomly-generated finite field elements. Shu Lin has presented several structured methods to construct good NB-LDPC codes using a technique known as array dispersion [12], one of which we will make use.

2 Construction of the sparse parity check matrix H of a NB-LDPC code. Shu Lin's method and its modification

The proposed scheme is based on the construction of a sparse parity check matrix $\boldsymbol{H}$ defined over the finite field $GF(2^m)$ by using a procedure proposed by Shu Lin [12]. The idea is to construct a given sparse parity check matrix $\boldsymbol{H}$ using a construction method that is ruled by a given user key.
Several array dispersion methods based on Euclidean and finite geometries, and also using a single code word from a very low-rate Reed–Solomon (RS) code have been proposed in [12]. We have selected the RS code word method for constructing a parity check matrix of an NB-LPDC code.
These NB-LDPC codes are constructed from RS codes with message length $k = 2$, and redundancy $n - k$. We will apply the restriction that $n - k$ has to be an even number. Since RS codes are maximum distance separable (MDS) their minimum Hamming distance is $d_{min} = n - k + 1 = n - 1$. Since a RS code defined over

$GF(q)$ has a block length of $n = q - 1$, this code will be a $(q-1, 2, q-2)$ RS code.

Since $d = q - 2$, any code word has at least the minimum weight of the code $q - 2$, so that the code word will contain $q - 2$ nonzero elements and a single zero.

In its classic form, the base code for this construction is a $(q-1, 2, q-2)$ RS code defined over $GF(q)$ with two information symbols and minimum distance $d = q - 2$. The corresponding generator polynomial has $\alpha, \alpha^2, ..., \alpha^{q-3}$ as its roots, where α is a primitive element of $GF(q)$. It can be proved that the two $(q-1)$-tuples over $GF(q)$, $(1 \quad \alpha \quad \cdots \quad \alpha^{q-2})$ and $(1 \quad 1 \quad \cdots \quad 1)$, are two code words of this RS code with weight $(q-1)$. The difference of these two code words, $\boldsymbol{c} = (c_0 \quad c_1 \quad \cdots \quad c_{n-1}) = (0 \quad \alpha - 1 \quad \cdots \quad \alpha^{q-2} - 1)$ gives a minimum weight codeword whose first component is zero.

This code word is then used to build a $(q-1)x(q-1)$ array by cyclically shifting it to the right to form the next row of the array. Since RS codes are cyclic, each row is a codeword and each column, when read from bottom to top, is also a code word, all with weights equal to $q - 2$. The array formed with the cyclic shifts to the right of the original code word gives form to a square matrix called the circulant matrix $\boldsymbol{W}$. In this matrix, the right cyclic shit rotation of the last row results into the first row code word. For a given minimum weight code word $\boldsymbol{c} = (c_0 \quad c_1 \quad \cdots \quad c_{n-1})$ the corresponding circulant matrix $\boldsymbol{W}$ has the form:

$$\boldsymbol{W} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix} \tag{1}$$

The circulant matrix $\boldsymbol{W}$ has the following structural properties [12]:

1) All the rows are minimum weight code words of the code;

2) All the columns (reading from bottom to top) are also minimum weight code words of the code;

3) Any two rows (or two columns) differ in all $(q-1)$ places;

4) All the entries of each row (or each column) are distinct elements of $GF(q)$.

The circulant matrix $\boldsymbol{W}$ is the basis for constructing the parity check matrix $\boldsymbol{H}$ of the NB-LDPC code.

For a non-binary code defined over finite fields $GF(q)$, array dispersion is an operation applied to each nonzero element in a matrix whereby each element is transformed to a location vector of length $q - 1$. A given element of the finite field

$\alpha^i \in GF(q)\ 0 \le i \le q-2$ will be placed in the *i*-th index of the location vector [12]:

$$\alpha^i \to \begin{pmatrix} 0 & 0 & \cdots & \alpha^i & \cdots & 0 \end{pmatrix} \tag{2}$$

The location vector has all its elements equal to zero excepting the element $\alpha^i \in GF(q)$, which is located at the i-th position.

Another way of doing this construction is to assign the position of the element to that of the decimal representation of the binary form of the element of the finite field.

In the classic construction proposed by Shu Lin, the element in this location vector is used to build an array with each row defined as the previous row cyclically shifted to the right and multiplied by the primitive element in $GF(q)$), resulting in a $(q-1)x(q-1)$ array [12].

Performing array dispersion on a matrix with dimensions axb would result in a larger matrix with dimensions $a(q-1)xb(q-1)$.

After applying array dispersion over the circulant matrix of size $(q-1)x(q-1)$ we will obtain an array or matrix $\boldsymbol{H}_d$ of size $(q-1)^2 x(q-1)^2$.

For any pair (γ,ρ) of integers with $1 \le \gamma,\rho \le q-1$, let $\boldsymbol{H}(\gamma,\rho)$be a $\gamma(q-1)x\rho(q-1)$ subarray of $\boldsymbol{H}_d$. The subarray $\boldsymbol{H}(\gamma,\rho)$) is a $\gamma(q-1)x\rho(q-1)$ matrix over $GF(q)$ which will be used as the parity check matrix of the NB-LDPC code.

Matrix $\boldsymbol{H}_d$ is constructed to satisfy the so called row-column (RC) constraint, so that $\boldsymbol{H}(\gamma,\rho)$ also satisfies this constraint. This means that the Tanner graph of the corresponding NB-LDPC code do not have cycles of length 4, so that the shortest cycles are of length 6. Thus, the so called girth of the LDPC code is at least 6 [12].

3 Construction of the sparse parity check matrix H for the proposed scheme

In the proposed scheme, which essentially aims the design of a communication system that can offer excellent BER performance and encryption capability, Shu Lin's method for constructing a parity check matrix $\boldsymbol{H}$ of a NB-LDPC code is modified. NB-LDPC codes are selected because of their structural agreement with many encryption algorithms, which also operate over finite fields, like the AES algorithm. A second reason for their use is that they have been proved to perform better than their binary counterparts. The price to be paid is an increase in complexity.

3.1 Modifications over the Shu Lin´s construction method of a parity check matrix $\boldsymbol{H}$

A first modification over the classic construction of a parity check matrix $\boldsymbol{H}$ of a NB-LDPC code based on RS codes is to use a RS code with the restriction of that $n-k$ has to be an even number.

When the restriction for the RS generating code is such that $n-k$ has to be a even number, the length of the initial code word that comes from the encoding procedure of the RS code with $k=2$ is equal to $q-2$. Therefore the size of the circulant matrix $\boldsymbol{W}$ is $(q-2)x(q-2)$. After applying the dispersion method to construct the final array, the resulting matrix $\boldsymbol{H}_d$ is of size $(q-2)(q-1)x(q-1)^2$. For any pair (γ,ρ) of integers with $1\le\gamma\le q-2$, $1\le\rho\le q-1$, let $\boldsymbol{H}(\gamma,\rho)$ be a $\gamma(q-1)x\rho(q-1)$ subarray of $\boldsymbol{H}_d$. The subarray $\boldsymbol{H}(\gamma,\rho))$ is a $\gamma(q-1)x\rho(q-1)$ matrix over $GF(q)$ which will be the basis of the parity check matrix of the NB-LDPC code of the proposed scheme.

The second modification is to take a message of size $k=2$ that can be any message word of two elements of the corresponding finite field over which the RS code is defined. This second modification introduces an uncertainty of q^2 in the selection of the final generator matrix of the code that will be derived from the parity check matrix $\boldsymbol{H}(\gamma,\rho)$.

In the Shu Lin´s construction, the initial code word is fixed to be one where all its elements are different. In our construction, any message word can be used as the seed of the method, generating q^2 possible code words.

3.2 An exponential operation over each non-zero element of the matrix $\boldsymbol{H}(\gamma,\rho)$

In order to provide the scheme with an increased level of security, we lie on a given expanded key, which can be generated by well known methods like the one used in the implementation of the AES algorithm. This key acts as a random generator of numbers that, in the particular case of being constructed using the AES key generator, results into a sequence Y_1^M of elements of the finite field $GF(256)$. The sequence Y_1^M contains M elements of the finite field $GF(256)$. Elements of this sequence can however be converted into their corresponding decimal representations, resulting into a sequence of integer numbers Yd_1^M in the range $\{0,255\}$.

Each non-zero element $\alpha^i \in GF(q)$ of the matrix $\boldsymbol{H}(\gamma,\rho)$, that was generated by the construction method detailed in the previous section, is replaced by another element $\alpha^j \in GF(q)$ that is calculated as:

$$\alpha^j = (\alpha^i)^v \tag{3}$$

Where v is an integer random number such that $v \in Yd_1^M$, which is sequentially taken from the sequence of integer numbers Yd_1^M. Thus, each element of the finite field $GF(q)$ of the original matrix $\boldsymbol{H}(\gamma,\rho)$ is replaced by a different element, which is obtained by exponential operation expressed in eqn. (3), using a pseudo random number v that is different for each element.
After performing this operation over the matrix $\boldsymbol{H}(\gamma,\rho)$, the resulting matrix will be the parity check matrix $\boldsymbol{H}$ of our NB-LDPC code. The knowledge of the key allows the receiver to successfully construct the parity check matrix $\boldsymbol{H}$ of the scheme. The null space over $GF(q)$ of the parity check matrix $\boldsymbol{H}$ gives a q-ary NB-LDPC code.

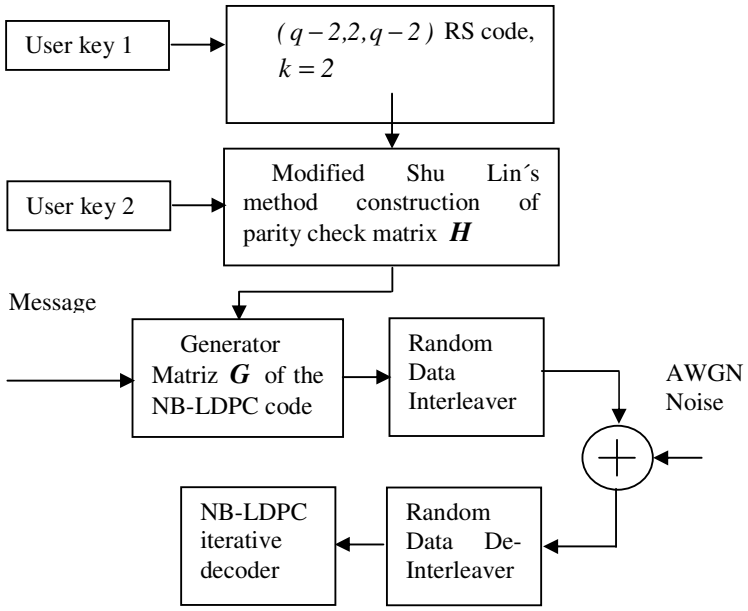

Figure 1. Block diagram of the proposed scheme

3.3 Matrix hopping transmission and random data interleaver

Two parts of the proposed scheme can be determined by external user keys: the seed message word that is input to the RS code, and the sequence Yd_1^M of integer numbers that are used in the exponential operation that modifies each non-zero entry of the parity check matrix $\boldsymbol{H}$ of the NB- LDPC code. A first idea is to periodically change user keys 1 and 2 during transmission to provide the scheme with increased levels of security. However, since key 2 is a sequence of integer numbers of length $\gamma p(q-1)$, a very large key is required to perform its change during transmission. In a practical implementation it is expected to generate user key 2 by any key expander, and to keep it fixed during transmission for a given user. User key 1 can be periodically changed by means of a long expanded key generated externally. This validates the effect of the exponential operation over the non-zero entries of the parity check matrix $\boldsymbol{H}$ using all the time the same exponents, because each initial non-zero entry being under exponential operation is periodically changed.

Since code words are transmitted to the channel, it is necessary to change the generator matrix $\boldsymbol{G}$ of the code before a set of k code words are transmitted, to avoid reconstruction of this matrix by reading k error-free linearly independent code words from the channel, which could allow the attack to successfully obtain this matrix. This procedure is called matrix hopping. Thus, the number of code words that remain generated by the same generator matrix $\boldsymbol{G}$ is called the length L_{mh} of the matrix hopping procedure.

In spite of that a collection of k linearly independent code words taken from the channel could allow an eavesdropper to reconstruct a generator matrix $\boldsymbol{G'}$, this matrix could be luckily a generator matrix of the same code, but the last process of decoding requires to determine the assignment message-to-code word of the error control code, in order to finally get the message. The change of the generator matrix during transmission done before a set of k code words are sent, does not allow the eavesdropper to construct such matrix, neither form a proper set of equations in a given algebraic attack, to obtain matrix $\boldsymbol{G}$.

Another simple, but effective method to avoid transparency of the code words over the channel is the use of a random data interleaver of length n which introduces an uncertainty of $n!$. This procedure is very simple, and it makes code words lose its original form.

4 Encryption properties of the proposed scheme

In our construction of a parity check matrix $\boldsymbol{H}$ of a NB-LDPC code we start from a RS codeword with length equal to $q-2$. There are q^2 messages from the $k=2$ space of the RS code selected and q^2 code words which are possible to be used as

the seed of the matrix $\boldsymbol{H}$. Each codeword generates a different circulant matrix $\boldsymbol{W}$ and so a different resulting matrix $\boldsymbol{H}_d$. Each circulant matrix has at most one zero per row and so, the resulting matrix $\boldsymbol{H}_d$ has at least $(q-2)x(q-1)^2$ non-zero elements whose position is determined by the initial RS codeword selected to generate the QC-LDPC code and it represents an uncertainty proportional to q^2.

$\boldsymbol{H}(\gamma,\rho)$ is a $\gamma(q-1)x\rho(q-1)$ subarray of $\boldsymbol{H}_d$. If we consider the elements equally spaced $\boldsymbol{H}(\gamma,\rho)$ has at least $\gamma\rho(q-1)$ non-zero elements for each possible codeword selected as a seed. In this sense, there exist $q^{\gamma\rho(q-1)}$ possible combinations for each generated matrix $\boldsymbol{H}(\gamma,\rho)$. The position of the non-zero elements is bounded to the selected original codeword and the uncertainty is augmented by q^2.

If we consider q as a power of 2, LDPC codes of $R_c = 1/2$ and $d_{\min} \geq 8$, there are at least $2^{mx7x14(2^m-1)}$ possible matrices with an uncertainty of 2^{2m}. Working in $GF(16)$ it means 2^{5880} possible combinations with 256 possible different position distribuions.

In this way, the private key would be the initial RS message which is changed periodically with a secret law previously established.

This periodical change is necessary to avoid a chosen-plaintext attack where the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of this type of attack is to reveal the scheme's secret key.

In this context, the attacker could encrypt successive messages with only one element of value 1 and the rest of the elements zero. In this way, if She/he first encrypts the message $\boldsymbol{m} = (1 \quad 0 \quad 0 \quad \ldots \quad 0)$ and then the message $\boldsymbol{m} = (0 \quad 1 \quad 0 \quad \ldots \quad 0)$ and so on, She/he could obtain the rows of matrix $\boldsymbol{G}$.

We must prevent that She/he obtain the secret matrix before She/he can encrypt k messages of this type. We avoid this attack if we change the matrix before She/he can obtain the information desired.

If some time later the key is repeated, and so are the exponents that modifies each non-zero entry of the parity check matrix $\boldsymbol{H}$, the attacker could take up again the attack and obtain the rest of the rows of the matrix G. To mitigate this possibility, we combine the exponentiation with changes in the position of the non zero elements of the matrix G, by selecting another RS codeword to construct $\boldsymbol{H}$. To avoid repetition, it is also possible to apply exponentiation in a cumulative way, using addition modulo-q of the integer numbers used as exponents for this operation.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

In order to provide the scheme with an increased level of security, we generate an expanded key from another secret private key.
In this manner we enhance the diffusion property of the scheme and, at the same time, maintaine the error correcting capacity of the code.
Depending on the size of the involved keys and other parameters of the scheme, the exponent of the exponential operation can be determined cumulatively through the transmission, by using modulo-q addition, to avoid repetition.

The use of the random interleaver, which essentially performs a permutation of positions of the elements of the output code word, makes the word being transmitted be not a code word of the NB-LDPC code utilised, reinforcing the security of the scheme.

5 BER performance simulation results

We have evaluated the BER performance of the proposed scheme using a $C(196,98)$ NB-LDPC code defined over $GF(16)$ in a transmission of 10 hops of 1000 code words each, in an Additive White Gaussian Noise (AWGN) channel, and it is compared with a similar $C(196,98)$ NB-LDPC code using the traditional Shu Lin's method for the construction of the corresponding parity check matrix $\boldsymbol{H}$, where neither the exponentiation nor the hopping procedures are applied. In this later case the transmission over the same channel is of 10000 code words defined over the field $GF(16)$. Decoding is performed using the Fast Fourier Transform Belief Propagation (FFT-BP) algorithm using 10 iterations. Results are seen in Figure 2, and they show that there is no BER performance degradation for the proposed scheme with respect to the classic one.

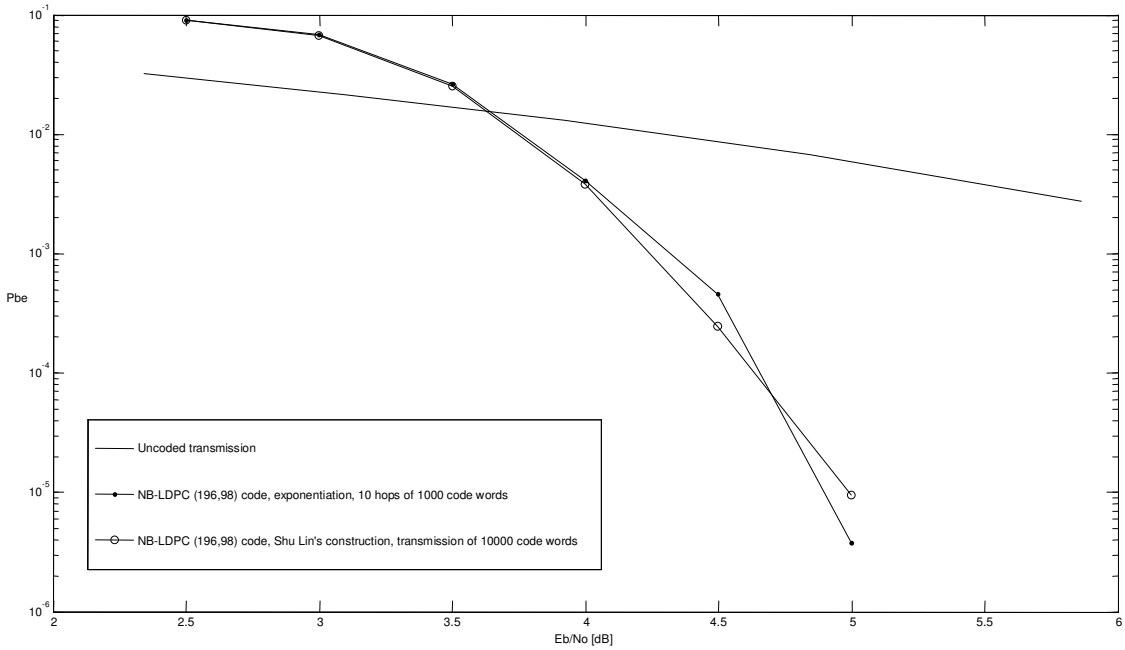

Figure 2. BER performance of the proposed scheme

6 Conclusions

The proposed combined error-control coding and encryption scheme is suitable for applications where transmission reliability and security are both important aims of the design. This proposed scheme is based on NB-LDPC codes, it shows a BER performance without degradation with respect to classic similar schemes, and it has a strong encryption capability. This is an advantage with respect to First-Encrypt-Then-Encode schemes usually utilised in practice, since the proposed scheme shows encryption capability that is obtained without any BER performance degradation.

The use of NB-LDPC codes brings the additional advantage of obtaining better BER performances than similar schemes defined over the binary field.

References

1. L. Arnone, C. González, C. Gayoso, J. Castiñeira Moreira and M. Liberatori, "Security and BER performance trade-off in Wireless

communication systems applications," *Latin American Applied Research*, Vol. 39, pags. 187-192, ISSN 0327-0793, 2009.

2. L. Coppolillo, M. C. Liberatori, D. M. Petruzzi, J. Castiñeira Moreira, "Analysis of error propagation of AES encrypted information transmission in noisy channels," XIII RPIC, Rosario, Santa Fé, Arg. Septiembre 2009.
3. L. Coppolillo, M. C. Liberatori, D. M. Petruzzi, J. C. Bonadero, J. Castiñeira Moreira, "Characteristics of AES encrypted data transmission in noisy channels as a measure of the AES algorithm encryption capability," *38º JAIIO - Argentine Symposium on Computing Technology (AST 2009),* Mar del Plata, Arg. 2009.
4. D.J.C.MacKay and R.M.Neal, "Near Shannon limit performance of low density parity check codes", *Electronics Letters*, vol. 3, no6, pp. 457-458, March 1997.
5. Berrou, C., A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo codes", *Proc.1993 IEEE International Conference on Communications,* Geneva, Switzerland, 1064-1070. (1993).
6. McEliece, R. J. "A public-key cryptosystem based on algebraic coding theory". DSN Progress Report, pp. 114–6. 1978.
7. Niederreiter, H., "Knapsack-type cryptosystems and algebraic coding theory," Problems of Control and Information Theory, 15(2):157–66. 1986.
8. Mathur, Chetan Nanjunda. Narayan, Karthik and Subbalakshmi, K. P. "On the Design of Error-Correcting Ciphers". Hindawi Publishing Corporation EURASIP Journal onWireless Communications and Networking Volume 2006, Article ID 42871, Pages 1–12. DOI 10.1155/WCN/2006/42871
9. Mathur, Chetan N. " A Mathematical Framework for Combining Error Correction and Encryption ". Dissertation. Stevens Institute of Technology. Castle Point on Hudson, Hoboken, NJ 07030. 2007
10. V.S. Ganepola, R.A. Carraso, I.J. Wassell and S. Le Goff, "Performance Study of Non-Binary LDPC Codes over GF(q)", *6th Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP08),* Graz, Austria, July 2008.
11. M.C. Davey and D.J.C. MacKay, "Low-Density Parity-Check Codes over GF(q)", *IEEE Information Theory Workshop, Killarney,* Ireland, June 1998.
12. Bo Zhou, "Algebraic Constructions of High Performance and Efficiently Encodable Non-Binary Quasi-Cyclic LDPC Codes," PhD Thesis, Univ. California, 2008.