A Variable-Parameter Coding Scheme Based on LDPC

Ling Zhao, Zhong Li
School of Electronics and Information Engineering,
Beihang University (BUAA), Beijing, China
E-mail: zhaoling@buaa.edu.cn, lizhong@buaa.edu.cn

Man-Jie Zhu
Space Star Technology Co., Ltd., China Academy of
Space Technology, Beijing, China
E-mail: Felicia_8147@163.com

***Abstract*-The paper proposes a channel coding system with both error correction performance and security performance. The implementation of security performance is to construct a cluster of parity check matrices with the same structure and to replace check matrices constantly in the coding process, which can be called variable-parameter coding scheme. (4096, 3328) code is constructed based on the proposed scheme, the coding gain achieves6.5dB on the condition that BER performanceis 10^{-6}, and the number of variable check matrices reaches 2^{47}. Applications of this physical layer security method indicate that illegal receivers cannot obtain the valid information.**

Keywords*- *physical layer security; variable code; LDPC; AES

I. Introduction

The history of cryptography can be traced back to ancient Egypt in the twentieth Century B. C. However, cryptography is became a real subject until [1] laid the theoretical foundation of cryptography, which represents the beginning of modern cryptography. Since Shannon proposed the channel coding theory [2], there are many scholars researching on how to construct a practical approximation of the channel capacity of good codes and a lot of results are achieved [3]-[7]. Before 1970s, channel coding theory and cryptography were two different subjects and they were almost independent of each other. Most of secure communication systems are hierarchical [8] and the communication scheme is first encrypting and then channel coding. While it is true that the two-step operation, on the one hand increases the complexity of the system, on the other hand, creates a certain time delay. In 1978, McEliece proposed the first public key cryptosystem based on algebraic coding theory, which combines channel coding and encryption [9]. Then, a cryptosystem which combines McEliece scheme and LDPC is proposed in [10]. However, there is the tradeoff between error correction capability and security performance in this McEliece scheme, and if not designed well, both of them will decrease. In addition, it has been proved that the secure communication can be realized without the key encryption if the error probability of the eavesdropping channel is higher than that of the main channel [11]. Reference [12] suggests to use physical layer security ideas in traditional designs to ensure security in wireless communication systems.

To achieve physical layer security while channel coding, a variable-parameter coding scheme based on LDPC is proposed. The scheme provides a method to construct a cluster of parity check matrices with same structure, so that check matrix can be replaced constantly by changing certain parameters when transmitting information. Besides, the set of matrices contains hundreds of trillions of elements. Since it has been proved by physical layer security theory that the channel error can improve the security of the system [13] and channel noise exists, illegal receiver can only obtain the encoded information instead of effective information without obtaining the correct matrix. Approaching from the angle of physical layer, this scheme takes advantages of propagation characteristics of the wireless channel and noise to solve the information security problem. In addition, with the goal of realizing high bit error rate performance as well as encryption performance, bidiagonal matrix structure is used in the proposed variable-parameter coding scheme.

The rest of this paper is organized as follows. Section II introduces bidiagonal matrices and corresponding encoding algorithms. Section III illustrates the proposed variable-parameter coding scheme and (4096, 3328) code is demonstrated as well. Both encryption performance and error-correcting performance are verified to be good. Section IV shows an application using the proposed scheme and gives the simulation results and analysis. Finally, a conclusion is drawn in Section V.

II. LDPC Encoding Algorithm Based on Bidiagonal Matrix

To simplify the encoding algorithm by taking advantage of the check matrix, the lower triangular bidiagonal matrix is utilized to construct the LDPC codes. The bidiagonal matrix is described by

$$H^p = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{1}$$

The check matrix based on the bidiagonal matrix is formulated by

$$H = [H^p H^d] \tag{2}$$

where H^p is the bidiagonal matrix with the size of $(N\text{-}M)(N\text{-}M)$, and H^d is composed of the circulant sub-matrices with the size of $(N\text{-}M)M$. It has the same property with the QC-LDPC matrix. Note that N is the code length of the LDPC codes and M is the length of the information bit. In Figure 1, each submatrix of H^d is obtained by shifting the unit matrix with the same size circularly.

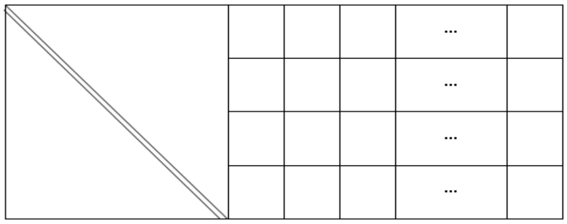

Figure 1. Code structure based on bidiagonal matrix.

An encoding strategy based on the bidiagonal matrix is proposed to code immediately with the check matrix and to simplify the codes significantly. The encoding algorithm is derived as follows.

The information after encoding c is divided into c^p and c^d. c^p is the check bit with the size of N-M, and c^d is the information bit with the size of M. The coding process can be described by

$$Hc^T = [H^p H^d]\begin{bmatrix} c^p \\ c^d \end{bmatrix} = H^p c^p + H^d c^d = 0 \qquad (3)$$

$$H^p c^p = H^d c^d \qquad (4)$$

$$c^p = \left(H^p\right)^{-1} H^d c^d \qquad (5)$$

Therefore, the check bit c^p can be obtained by the linear product of the matrices during the encoding process. The inverse matrix $(H^p)^{-1}$ of the bidiagonal matrix H^p can be described by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad (6)$$

This matrix is a very special lower triangular square matrix with extremely strong regularities. The derivation reveals that the product of matrices is equal to the simple product and iteration of numbers. Therefore, the check bit c^p can be obtained easily. Specifically, assume the vector of the information bit $c^d=\{d_i\}$, and the vector of the check bit $c^p=\{p_i\}$. Then equation (7) and equation (8) can be obtained.

$$p_1 = \sum_j h_{1j}^d d_j\ , \qquad (7)$$

$$p_i = p_{i-1} + \sum_j h_{ij}^d d_j, \quad i = 2,\cdots,n-k-1 \qquad (8)$$

III. VARIABLE-PARAMETER CODING SCHEME

A. A Method of Constructing Variable Code

In bidiagonal matrix, code length is N, and information bit length is M. If the circulant sub-matrices of H^d is in the size of aa, H^d will have $(N$-$M)/a$ sub-matrices in the columns vision and M/a sub-matrices in rows vision, which can be denoted as i and j. Then, H^d is made up of ij sub-matrices in the size of aa. Because circulant sub-matrices are generated by cyclic shifting unit matrix in certain regulation, when N and M are given and fixed in LDPC coding, the code can be variable by changing the size of sub-matrices and offsets of sub-matrices. Namely, variable parameters include a and offsets of ij sub-matrices.

More specifically, a is less than M and N-M, besides, M and N-M are able to be divided evenly by a, since it is obvious that $(N$-$M)/a$ and M/a should be integer. So, all common divisors of M and N-M are suitable and the specific value of a depends on requirements of complexity error-correcting performance. When a is settled, the basic format of LDPC code is ascertained. The number of all sub-matrices can be proved to be $M(N$-$M)/a^2$, namely ij which is already deduced. The *offset*(i,j) is used to indicate offsets of all sub-matrices and it should be ensured that 0 *offset*(i,j) a-11 i $(N$-$M)/a$ 1 j M/a. To change the check matrix, *offset*(i,j) could range from 0 to a-1, and the number of variable offset parameter is $M(N$-$M)/a^2$.

Equation (9) gives a check matrix named H_1. Equation (10) gives an example where H_1 is changed by changing *offset*(i,j). In the first row of H_2, the offset parameters are 2, 0, 2, 1, different from H_1 whose parameters are 0, 1, 2, 1. Equation (11) gives an example where H_1 is changed by changing a. Sub-matrices of H_3 is in the size of 44 which means the value of a is not 3 but 4, and the number of sub-matrices is 9 instead of 16.

$$H_1 = \left[\begin{array}{cccccccccccc|ccc|ccc|ccc|ccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&1&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&0&1&0&0\\ \cline{13-24}
0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&0&1&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&1\\ \cline{13-24}
0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\ \cline{13-24}
0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&1&0&0&1
\end{array}\right] \qquad (9)$$

$$H_2 = \left[\begin{array}{cccccccccccc|ccc|ccc|ccc|ccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&1&0\\
1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&1\\
0&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&1&0&0\\ \cline{13-24}
0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&0&1&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&1\\ \cline{13-24}
0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\ \cline{13-24}
0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&1&0&0&1
\end{array}\right] \qquad (10)$$

$$H_3 = \left[\begin{array}{cccccccccccc|cccc|cccc|cccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\ \cline{13-24}
0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&1&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1&0&0&0&1&0&0&0\\ \cline{13-24}
0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&0&0&1&0&0
\end{array}\right] \quad (11)$$

This method, which provides variable codes, is the basis of constructing a cluster of parity check matrices and of replacing check matrices constantly in the coding process.

B. (4096,3328) Code

The constraint of coding parameter is that code length N is 4096 and code rate is greater than 0.8. Considering the number property and discipline of matrix construction, information bit length M is 3328, and parity check bit length (N-M) is 768. The code rate of the parameter above is 0.8125, which satisfies the constraint. Parity-check matrix$H$ is 7684096, H^p is 768768, and H^d is 7683328. If a is 128, H^d will be divided into 626 sub-matrices, which are in the size of 128128 and is generated by the cyclic shift of identity matrix.Figure 2 shows theparity-check matrix$H$, where*offset*(i,j)means the offset of the sub-matrices ofH^d, and 0 *offset*(i,j) 127.

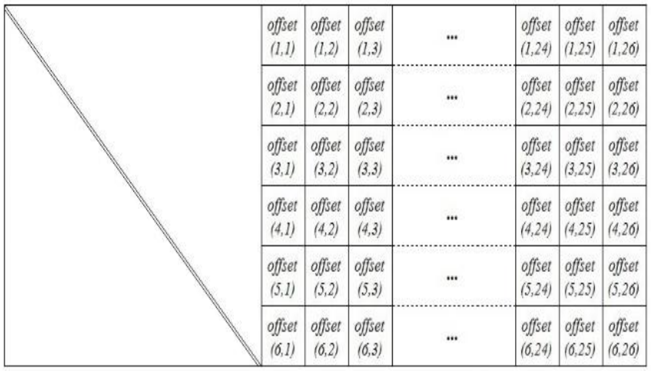

Figure 2. (4096, 3328) LDPC parity matrix.

In LDPC, to achieve high coding gain performance, four-short-cycles are not allowed to be existed in parity-check matrix. In the proposed parity-check matrix, necessary and sufficient condition of no four-short-cycles is that in arbitrary neighbouring row of arbitrary two columns, the offset differences cannot be equal. Namely, for arbitrary x, y, a, b:

$$offset(a,x) - offset(b,x) \neq offset(a,y) - offset(b,y)$$

$$1 \leq a,\ \ b \leq 6 \quad \& \quad 1 \leq x,\ \ y \leq 26$$

It can be proved that there are no four-short-cycles in parity check matrixif the constraints above are satisfied. This guarantees the encoding gain performance of parity check matrix. The matrix construction scheme is shown as Table 1 which can satisfy the constraints. The parameters *dif* and *ori_offset* in table 1 are intermediate parameters which are used to calculate *offset*(i,j).

TABLE I. PARAMETERS CHANGING PROGRAM FOR (4096,3328)

Input: *a*, *b*, *c*, *d*, *e*, *f*, *mod* (0*a*, *b*, *c*, *d*, *e*, *f*128, 1*mod*24)

Difference value of each offset parameter in row vision:
if mod =1: *dif*(1)=1, *dif*(2)=2, *dif*(3)=3, *dif*(4)=4, *dif*(5)=5, *dif*(6)=6
if mod =2: *dif*(1)=1, *dif*(2)=2, *dif*(3)=3, *dif*(4)=4, *dif*(5)=6, *dif*(6)=5
if mod =3: *dif*(1)=1, *dif*(2)=2, *dif*(3)=3, *dif*(4)=5, *dif*(5)=4, *dif*(6)=6
if mod =23: *dif*(1)=6, *dif*(2)=5, *dif*(3)=4, *dif*(4)=3, *dif*(5)=1, *dif*(6)=2
if mod =24: *dif*(1)=6, *dif*(2)=5, *dif*(3)=4, *dif*(4)=3, *dif*(5)=2, *dif*(6)=1

Offset parameter in first column: *offset*(1,1)= *a* *offset*(2,1)= *b* *offset*(3,1)= *c* *offset*(4,1)= *d* *offset*(5,1)= *e* *offset*(6,1)= *f*
Offset parameter in other columns: *ori_offset*(*i*,*j*)= *offset*(*i*,1)+ *dif*(*i*)(*j*-1) *offset*(*i*,*j*)= *ori_offset*(*i*,*j*)%128

The proposed method of constructing (4096, 3328) LDPC parity matrix based on two-diagonal-matrix can construct the parity check matrix without four-short-cycles.The coding gain can achieve6.5dB on the condition that the bit error rate (BER) performanceis 10^{-6}. Figure 3 shows the BER performance of constructedLDPC parity matrix.

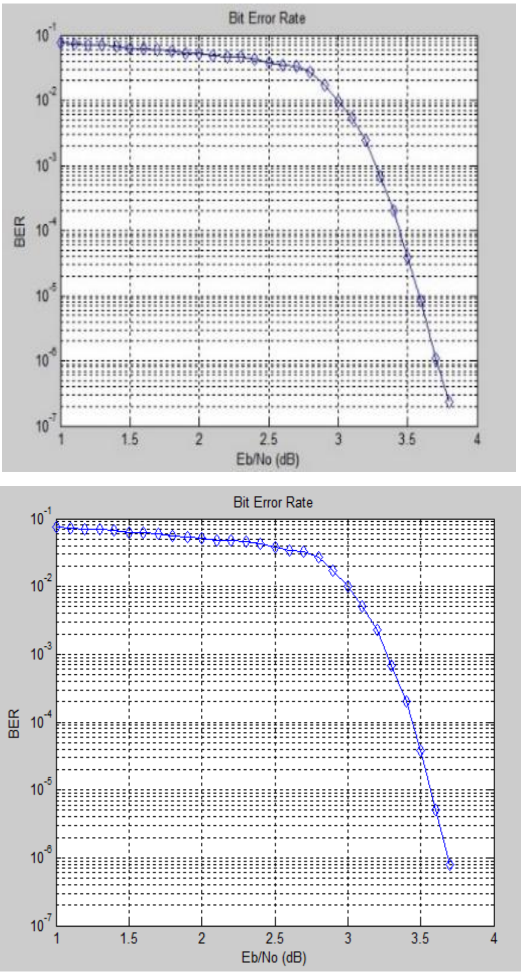

Figure 3. The BER performance of (4096, 3328) code.

The two different curves above represent different parameters. In the left one, *offset*(1,1) is 11, *offset*(2,1) is 79, *offset*(3,1) is 126, *offset*(4,1) is 47, *offset*(5,1) is 1, *offset*(6,1) = 101, and *dif* is [1 2 3 4 5 6]. In the right one, they are 1, 58, 126, 47, 101 and [6 5 4 3 2 1] respectively.

C. *Physical Layer Security and Variable-Parameter Coding Scheme*

Similar to wired network, traditional wireless network achieves secured communication through the key and encryption on the upper layer in the protocol stack using a variety of encryption algorithms. However, the invention of a new encryption algorithm is always followed by its decryption algorithm. Although encryption can ensure the information security of wireless network communication, it is computationally more complex. Different from encryption, which is based on protocol stack, physical layer is used to approach the information security of wireless network from another perspective. Open physical channel, multipath, attenuation, and transmission characteristics make wireless network undergo more serious security issues than wired network. However, some of the unfavorable channel characteristics can be utilized to solve this problem. Approaching from the angle of information theory, wireless network physical layer method takes advantage of various propagation characteristics of the wireless channel to solve the information security problem.

During the process of encoding, according to physical layers characteristics, noise exists in the wireless channel between the receiver and the transmitter. After being jammed by the noise, rather than read the information directly, check matrixwhich can be treated as a keymust be sued to decode the information, and the eavesdropper cannot get the message without cracking the key. The noise can be either from natural channel or added artificially. Additionally, White Gaussian Noise can further improve performance. The ultimate goal of wireless communication security is to allow legitimate users to have normal communication and prevent illegal receivers from accessing the information. Based on traditional data encryption solutions, this method fully utilizes the characteristics of physical layer security (channel coding) and ensures the information security by adding artificial noise to the signal.

Before channel encoding,randomized algorithm is usedto generate offset parameters for change the parity check matrix. Such a random parity check matrix is avariable random parity check matrix and the process is defined as randomization. The significance of randomization is transforming the key in traditional encryption algorithms from constant to variable, resulting in the significant increase in the difficulty of password attacks. The randomly generating of matrix makes it incapable to obtain a converged solution via blind estimation algorithm, and hence guarantee the secure transmission of wireless communication information in the physical layer. The scheme of the conversion for parity check matrix is shown in Figure 4.

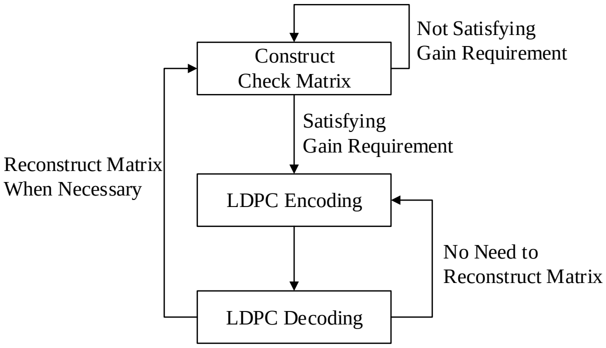

Figure 4. Variable-parameter coding scheme

Against exhaustive attack (brute force method), each sub-matrix is sized as 128128, and the 626 sub-matrices all have 128 possible offsets, so that the number of elements in the matrix space is $156^{128}510^{280}$. Assuming the 1 million matrix testing per second , it requires 510^{274}s, about 10^{267} years. When the generating technique for the parity check matrix is deciphered, there will be collapse phenomenon, and the parameters *a*, *b*, *c*, *d*, *e*, *f*, *mod* can determine the matrix. However, the parity check matrix sample space capacity can also reach $128^{6}242^{47}$, which is still an enormous data amount that requires a very lot of time to decipher. Therefore, a good safety performance of the system is achieved.

IV. APPLICATION AND ANALYSIS

A. *Combined with AES*

AES (Advanced Encryption Standard) algorithm is a symmetric cryptographic algorithm, both sides in the communication share a single key in encryption and decryption process. The AES algorithm and LDPC variable code technology can be cascaded. On the one hand, such cascade keeps the original encryption characteristics the AES algorithm, on the other hand, after channel decoding, the main channel can get the correct cipher text, and the original information can be obtained by the decryption algorithm. For the wiretap channel, due to the existence of noise in the transmission of information in the channel, if the tapped information is not decoded or is not properly decoded, the obtained cipher text information may have error bits. Even if the correct decryption process is conducted, because of the high diffusion rate of the encryption algorithm, the decoded information may have great difference with the original information. This scheme takes full consideration of characteristics of the physical layer, and uses the noise characteristics of the channel to further achieve the purpose of encryption.

When AES algorithm combines with variable code technology, variable code technology ensures the existence of error bits in decoding process, and AES encryption algorithm for the line displacement and column mixture transformation play the role of diffusion, which means that the change of 1 bit information will affect other bits. In each round of operation, the hybrid transformation makes the diffusion rate R equals to 4 (that is, the change of 1 bit will affect the 4 bits). After the 10 round of the transformation, the diffusion rate reaches 4^9 (the last round of operation does not include the hybrid transform). We further spread the error, so that the eavesdropping side cannot get useful information.

B. *Execute Solution and Applied Case*

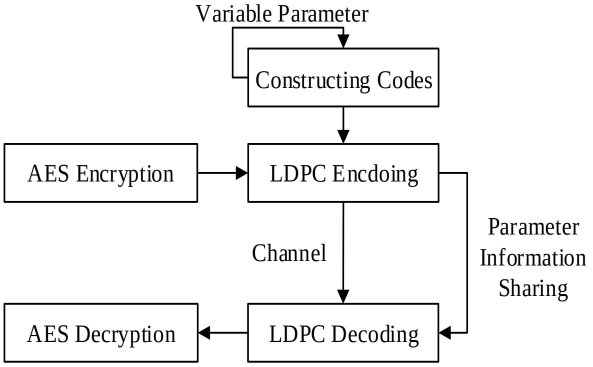

Figure 5. Implementation scheme of physical layer security

As shown above, this system combines two components, one is the AES module and the other is encryptable encoding module using variable-parameter coding. The encoding module is responsible for integrating encryption and encoding to encrypt for data and also responsible for constructing parity check matrix, key variable and sharing matrix information. The AES module is made for data security using its diffusibility. The relation of different modules is shown in Figure 5.

It uses serial combination to combine AES algorithm and LDPC error coding for data security. This method keeps original AES security and performs better with less brute-force time for specific brute-force method. The AES algorithm uses brute force method to solve encryption. Because the key is 128 bit, the space complexity for key is 2^{128}. Assuming it can test 2^{40} keys per second, this will spend seconds which is approximately equal to 10^{19}years. This system performs well with high AES security for specific to differential attack and Square attack. Besides that, when the illegal tapping point can't solve LDPC parity check metric, the key content has error bit when transporting, even use the right key can't decrypt in terms of high security.

Transmitting a picture, the communication system is implemented. Figure 6-8 give the result.

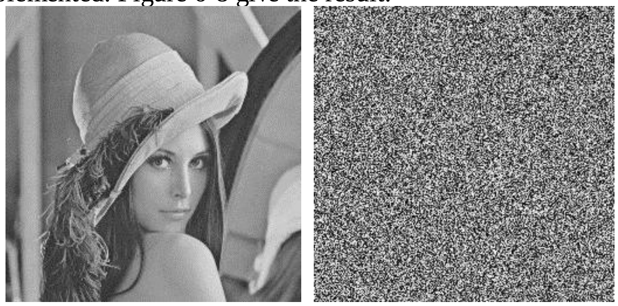

Figure 6. Transmitter: original information encrypted information.

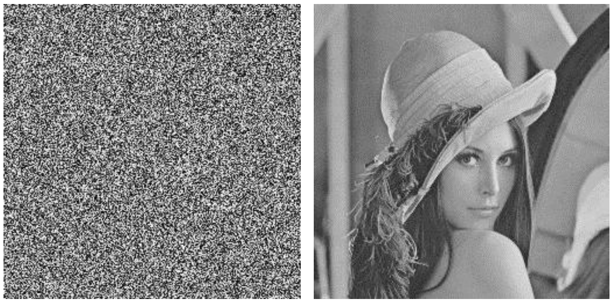

Figure 7. Legal receiver: received information and decrypted information which is same as Figure 6.

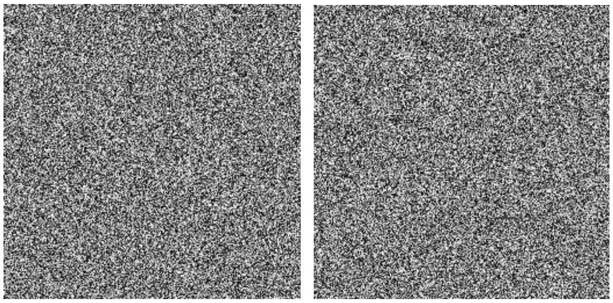

Figure 8. Illegal receiver: received information and decrypted information which is totally different from Figure 6 and invalid.

V. Conclusion

The paper proposes a variable-parameter coding scheme and a channel coding system based on bidiagonal matrices, which ensures both error correction performance and security performance. Taking advantage of various propagation characteristics in the physical layer, the system completes encryption and ensures the safety performance in the process of channel coding. Taking (4096, 3328) LDPC code as an example, the coding gain achieves6.5dB on the condition that BER performanceis 10^{-6}, and the number of variable check matrices reaches 2^{47}. Finally, combined with AES, the scheme turns out to be flexible, applicable and effective.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (61401010).

References

[1] Shannon, Claude E. Communication theory of secrecy systems. Bell system technical journal 28.4 (1949): 656-715.

[2] Shannon, C. E. A Mathematical Theory of Communication: The Bell System Technical Journal. Bell System Technical Journal 27.3(1948):3 - 55.

[3] R., W. Error detecting and error correcting codes. Bell System Technical Journal 29.2(1950):147-160.

[4] P. Elias, P. Elias. Coding for Noisy Channels,[J]. Ire Convention Record, 1955, 6.

[5] Hocquenghem, A. Codes correcteurs derreurs. Chiffres (1959):147-156.

[6] Forney, G. David. Concatenated codes. M. I. T. Press, 1966.

[7] Gallager, R G. Loiv-Density Parity-Check Codes. Information Theory Ire Transactions on 8(1962).

[8] Khisti, et al. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. IEEE Transactions on Information Theory 56.7(2010):3088-3104.

[9] R. J. Mceliece, A public-key cryptosystem based on algebraic coding theory, DSN Progress Report, pp. 114116, 1978.

[10] C. Monico, J. Rosenthal, and A. Shokrollahi, Using low density parity check codes in the Mceliece cryptosystem, in Proc. IEEE ISIT 2000, Sorrento, Italy, June 2000, p. 215.

[11] Wyner, A. D. The wire-tap channel. Bell System Technical Journal 54.8(1975):1355-1387.

[12] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. on Information Theory, vol. 54, no. 6, June 2008.

[13] Tekin, Ender, and A. Yener. "The Gaussian Multiple Access Wire-Tap Channel." IEEE Transactions on Information Theory 54.12(2008):5747-5755.