A Joint Encryption and Error Correction Method Used in Satellite Communications

LI Ning, LIN Kanfeng, LIN Wenliang, DENG Zhongliang

Laboratory of Intelligent Communication, Navigation and Micro/Nano-Systems, Beijing University of Posts and Telecommunications, Beijing 100876, P. R. China

Abstract: Due to the ubiquitous open air links and complex electromagnetic environment in the satellite communications, how to ensure the security and reliability of the information through the satellite communications is an urgent problem. This paper combines the AES(Advanced Encryption Standard) with LDPC(Low Density Parity Check Code) to design a secure and reliable error correction method -- SEEC(Satellite Encryption and Error Correction).This method selects the LDPC codes, which is suitable for satellite communications, and uses the AES round key to control the encoding process, at the same time, proposes a new algorithm of round key generation. Based on a fairly good property in error correction in satellite communications, the method improves the security of the system, achieves a shorter key size, and then makes the key management easier. Eventually, the method shows a great error correction capability and encryption effect by the MATLAB simulation.

Key words: data encryption; error correcting cipher; advanced encryption standard; LDPC channel coding; satellite communications

I. INTRODUCTION

Satellite communications have the advantages of large coverage, wide bandwidth, huge capacity, flexibility in different businesses, stable and reliable performance, and no geographical restrictions. What's more, the cost has nothing to do with the distance. It is now widely used in military communications, emergency communications and the field of radio and television. It will become a focus in mobile communications research.

In satellite communications, due to fading, noise and interference, the signal will come through more serious distortion. A strong error correction method should be applied to reduce the bit error rate in the case of limit power. Meanwhile, the broadcast satellite communication links lack effective safety feedback, so a more secure encryption algorithm should be adopted. Therefore, how to improve the reliability and security of the data transfer is one key issue in research of satellite communications.

Existing satellite communication technology divides encryption and error correction into two steps, that's to say, to encrypt the information first, and then to encode the encrypted data by error correction coding. This step-by-step method not only increases the complexity of the system, but also leads to a longer delay. This will result in restrained system efficiency and limit the further miniaturization of the baseband chip. However, the credible and reliable data transfer method combined with encryption and error correction is at the forefront of research. When it applies in the satellite communications system, it can improve the transmission efficiency, reduce the system

In this paper, a joint encryption and error correction coding method which applies to satellite communications domain is designed combining the Advanced Encryption Standard (AES) with Low Density Parity Check Code (LDPC).

processing delay, and ameliorate the real-time nature of the business transfer.

A preliminary study on the joint encryption and error correction method is being carried out among the national and international researchers.

In 1978, based on the characteristics of the Goppa codes, McEliece firstly made use of error-correcting codes to construct a class of public-key system--M public key system [1]. M public key system can encrypt and decrypt easily, but its key size is too large. Worse still, the security confronts a hidden danger. In 1991, the Korzhik and Turkin claimed that it had been broken through [2].

After a few years, researches on encryption and error correction algorithm were mainly around the improvement of the M public key system. During this period of time, a number of different types of M key systems were proposed. In 1984, Rao proposed a private key cryptography [3], the basic idea was to apply the McEliece public key in the private key cryptography. In 1986, Wang Xinmei put forward Ms public-key system [4] and MC packet encryption and error correction system [5] by a deep study on the M public key system. At the same year, Niederreiter utilized Goppa codes checked matrix to construct a new public-key system, referred to as N public key system [6]. To some extent, these M-alike key systems make a progress in security, the error correction capability and decoding time.

In 2006, Mathur and Subbalakshmi proposed a high degree of diffusion codes (HD) in the literature [7]. This method is based on the SPN structure, which is used in the AES algorithm. It utilizes the HD codes as a diffusion layer of the SPN structure. Because the HD codes have the error correction capability, and it is also a byte-based encoding, it is achievable to combine the encryption and error correction. Compared with other methods, however, it has higher complexity.

In 2008, Zuquete and Barros proposed a concept referred as "physical-layer encryption"[8]. To channel encode on the message sequence firstly, and then to encrypt the message by using sequence password. With exchanging sequence of encryption and coding, unauthorized users can neither decrypt nor decode, so the security of the system has been improved. But this method can only use the sequence password to complete encryption and decryption operations. Therefore, it has some limitations.

In the same year, Su Qing and Xiao Yang put forward a method combining the AES algorithm with the LDPC codes about operating the encryption and error correction, called LDPC-based error correcting cipher [9]. This method uses the diffusion performance of the LDPC codes to cut rounds of encryption in AES algorithm, therefore, it can guarantee security even in fewer rounds. However, this algorithm is still essentially traditional two-steps method (encrypt first, then error correct), and the key size is still too large.

In 2010, Leng Wenyan, from the point of reducing the key size [10], replaced the Goppa codes with irregular LDPC codes on the basis of M key system. At the same time, a calculation method was produced by using permutation matrix and error vectors which are generated by random numbers. This method significantly reduces the key size. However, it stills an M-like key cryptosystem. The encryption process is actually just a linear encoding process. Obviously, the security capability is far less than the AES algorithm with great avalanche effect.

In 2011, Adamo took a scheme named ECBC [11], operating the encryption and error correction in only one step. This scheme improves the algorithm efficiency. Moreover, there is no trade-off between error correcting performance and the security of encryption so that we can utilize its full capacity to correct channel errors. Whereas, the scheme is based on the Cipher Block Chaining (CBC) mode, so the encryption process must be carried out in sequence. Unlike in the Electronic Codebook (ECB) mode, it cannot operate parallelly, which slows down the encryption speed. In

addition, this scheme needs two initial vectors. In order to ensure the security, these two initial vectors should be protected just like the keys, which make the key management more difficult.

In 2012, Adamo designed a scheme based on McEliece public-key system that combined encryption, error correction, and modulation [12]. It can guarantee the security and reliability in the physical layer. The core idea is to use the error vector in the McEliece public key cryptography algorithm to control constellation mapping in the modulation process, making the modulation process random, so as to improve the system security. Similar to the discussed M-like key systems, the scheme possesses faster encryption speed, but is less secure and only suitable for resource-constrained wireless communication devices.

In summary, the proposed encryption and error correction algorithms can be classified into two categories. On one hand, some ensure the security performance by using advanced error correction coding algorithm. These methods can encrypt and correct the messages by encoding only once so that they can utilize the dual role of redundancy codes. These algorithms can encrypt and decrypt easily and quickly. However, using the matrix as a key leads to a large key size and insecurity. On the other hand, other algorithms ensure the error correction capability by improving encryption algorithm. These methods add or replace some of the linear modules on the basis of the block cipher algorithm structure to ensure the error correction capability. These algorithms usually have the problems of weak error correction capability and high complexity.

To solve the problems above, we propose a new encryption and error correction method used in the satellite communication system. This method can improve the security and reliability of the satellite communication system, while reducing the key size of the algorithm.

II. The Proposal of SEEC Method

This paper proposes a physical-layer encryption method based on AES and LDPC, which is suitable for satellite communication. Compared with the LDPC-based error correcting cipher that is also based on AES and LDPC mentioned in literature [9], the SEEC method has a better performance.

2.1 System structure model

The procedure of encryption and decryption in this system is shown as figure 1.

The encryption process is based on the 10 rounds model of AES algorithm, both the block length and the key length are 128 bits, using parallel encryption and one encoding operation. The input is n blocks of Plaintext data. The first 9 rounds of operation are the same to the standard AES algorithm's, but the algorithm in the 10^{th} turn is different. It uses the LDPC encoding instead of the row shifting in AES. After XOR with the sub-key, we can get the ciphertext. The decryption process is the inverse of the encryption process.

2.2 Encryption method

The idea of this algorithm is based on the classical SPN structure in block coding area. SPN

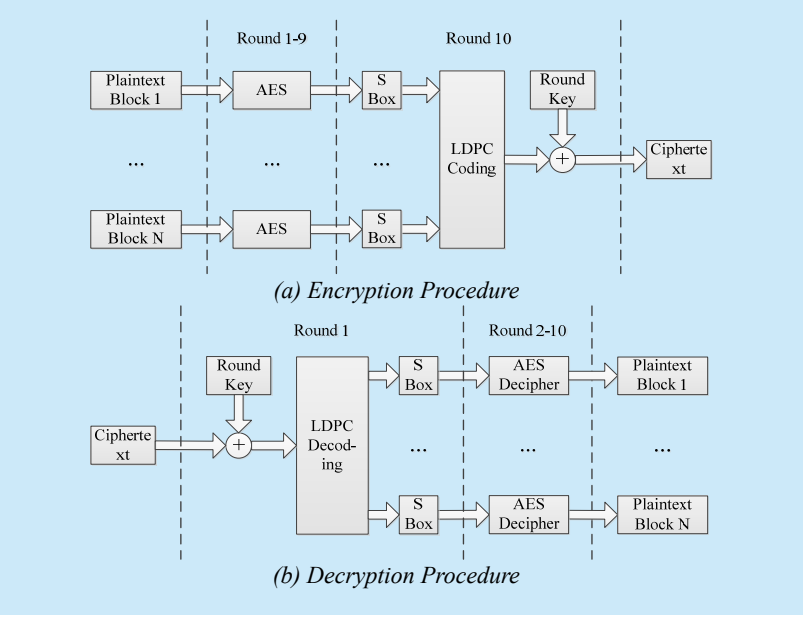

Fig.1 *System Structure of Encryption and Decryption Procedure*

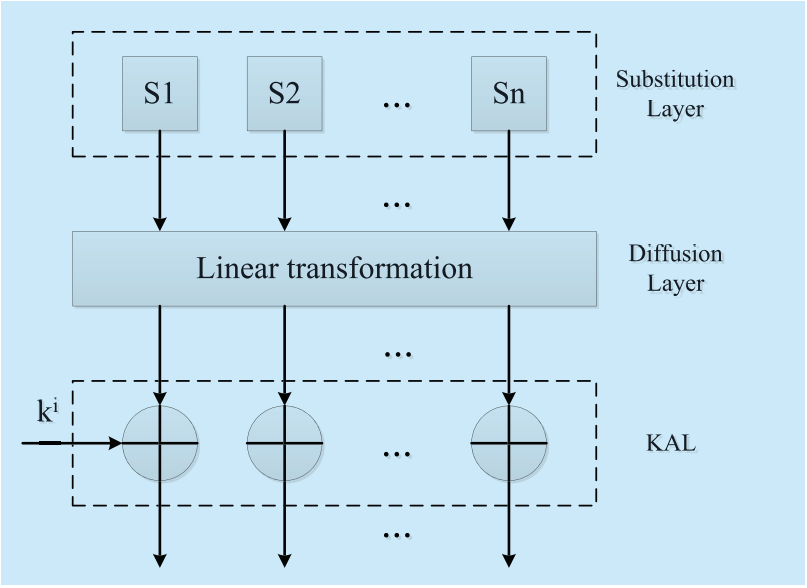

Fig.2 *SPN layer structure*

structure uses three functional modules, just as shown in figure 2. In these three layers, the substitution layer is for confusion achieving by the S-box, and it is the nonlinear part in block coding, Characteristics of the cryptography directly affect the security level. A good S-box can ensure the encryption algorithm to resist against different kind of attacks, such as differential cryptographic analysis attacks and linear cryptographic analysis attacks. The diffusion layer is for diffusion. Because of the limited storage and the speed requirements, we have to restrict the scale of the S-box, so diffusion layer is needed for diffusing the confusion effect of the substitution layer to a larger scale, and it is also for avalanche effect. So, we can conclude that, substitution layer has the capability to resist against differential and linear attacks, and diffusion layer propagates this capability to a larger scale. The Key Adding Layer (KAL) realizes the combination of data and key, using the key to control the round function.

AES is a typical representative of the SPN structure cryptographic algorithm. This algorithm always completes the encryption in 10 rounds. Except for the final round, each round consists of four transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round Key. The final round doesn't have the Mix Columns transformation. In these transformations, Sub Bytes corresponds to the substitution layer in the SPN structure, Shift Rows and Mix Columns correspond to the diffusion layer, and Add Round Key corresponds to the KAL.

This method refers to the basic structure of AES algorithm. Both block length and key length are 128 bits. The computation of the former 9 rounds is same as the AES algorithm. In the final round, do the Sub Bytes (S-box) firstly, then, do the LDPC encoding by using the upper result as the information bit, in which the scale of LDPC check matrix depends on the corresponding standards of satellite communications. Because the good coding performance of LDPC can be only realized with long LDPC codes, we take the encryption processing parallel in the anterior 9 rounds before the last round of the LDPC coding. At last, we obtain the ciphertext by XOR the result with the sub-key. So we get the encryption control of the LDPC encoding round. The encryption process is shown in figure 1(a).

2.3 Encoding method

According to the related standards of channel coding in satellite communications, we adopt the specified LDPC codes in this method. Here, the coding length can be selected freely according to the different needs of application. For different coding length, we need only to change the block number of plaintext which encrypts in a parallel way. This paper refers to the CCSDS(Consultative Committee for Space Data Systems) standard in simulations [13], we choose n = 1024 as code length, 1/2 as rate in our coding scheme. That is to say, we use a 512*1024 check matrix for encoding. When encoding, we get generator matrix from LDPC check matrix by using Gauss elimination, then we multiply the information vector with the generator matrix to get the result of encoding. When decoding, we use min-sum decoding algorithm to realize iterative decoding [14].

2.4 Key control method

The method is a reference to the thought of "physical-layer encryption", combining the LDPC coding with AES as a part of encryption algorithm. Because the LDPC generator matrix and the coding algorithm are public, in order to keep the encoding process security, and unauthorized users can't decode the information, the round keys of AES should have higher security. In addition, the key expansion algorithm of AES still has some security problems. Therefore, a new algorithm for generating AES round keys is proposed in this paper.

It is known the 4-characters round key in each round can be obtained from the 4-characters of former round key in AES key expansion algorithm. On the contrary, the 4-characters of former round key can also be deduced by the latter ones. So if one round key is known, the attacker can get the sub-key of every round, and even the seed key. Power analysis attack and Saturation attack which are effective to AES, both make use of the simple character of key expansion algorithm. In literature [15], Chari and others believe that a more complicated key algorithm can be helpful to this problem. Thus, if we change the AES key expansion algorithm, to make every round key not only depend on one former round key, but on two or even more round keys, then the upper attacks will become much more difficult, and it will provide the AES algorithm a higher security level. So we propose a new key generating algorithm.

In the traditional 10 rounds AES key expansion algorithm, the 4 characters round key extended to 44 characters. Supposing that the original key is (k_0, k_1, k_2, k_3), it generates the sub-keys (k_0, k_1, ..., k_{43}),

Where original key: k_0, k_1, k_2, k_3;

1st round key: k_4, k_5, k_6, k_7;

2nd round key: k_8, k_9, k_{10}, k_{11};

…

10th round key: k_{40}, k_{41}, k_{42}, k_{43};

The key expansion process of the first two rounds is

$$k_4 = k_0 \oplus SubWord(RotWord(k_3)) \oplus Rcon(1) \quad (1)$$

$$k_5 = k_1 \oplus k_4 \quad (2)$$

$$k_6 = k_2 \oplus k_5 \quad (3)$$

$$k_7 = k_3 \oplus k_6 \quad (4)$$

$$k_8 = k_4 \oplus SubWord(RotWord(k_7)) \oplus Rcon(2) \quad (5)$$

$$k_9 = k_5 \oplus k_8 \quad (6)$$

$$k_{10} = k_6 \oplus k_9 \quad (7)$$

$$k_{11} = k_7 \oplus k_{10} \quad (8)$$

The new algorithm in this paper introduces the idea of sub-key generating in a European cipher standard --KHAZAD [16], that is

$$k_i = k_{i-8} \oplus H(S(k_{i-4})) \oplus c^{[(i-8)/4]} \quad (i = 8, 9, \ldots, 43) \quad (9)$$

In which, H is a linear diffusion function, S is a byte substitution function, and c is a round constant. In which, every round key depends on its two former round keys. The second round can be expressed as

$$k_8 = k_0 \oplus H(S(k_4)) \oplus c^0 \quad (10)$$

$$k_9 = k_1 \oplus H(S(k_5)) \oplus c^0 \quad (11)$$

$$k_{10} = k_2 \oplus H(S(k_6)) \oplus c^0 \quad (12)$$

$$k_{11} = k_3 \oplus H(S(k_7)) \oplus c^0 \quad (13)$$

Our method refers to the thought in KHAZAD algorithm. In order not to make the key generating algorithm more complicated, we only complicate the operations where the subscript is a multiple of 4. We replace the diffusion function *H* and substitution function *S* by Sub Word function and shift operation function Rot Word of the original S-box in AES algorithm, and replace the round constant c^i with $Rcon(i)$. For other elements which the subscript is not a multiple of 4 can be generated by the XOR of the former two corresponding elements. So the round keys from the 2nd round to the 10th round can be calculated by the former 2 round keys. The generating algorithm is as follows

$$k_i = k_{i-8} \oplus SubWord(RotWord(k_{i-4})) \oplus Rcon(i/4) \quad (i = 8, 12, \ldots, 40) \quad (14)$$

$$k_i = k_{i-8} \oplus k_{i-4} (8<i<44, \text{ and } i \text{ is not a multiple of } 4) \quad (15)$$

For the sub-key of the 1st round, it can be only generated from the original key. We hope it has "one way" character so that derivation can only be done from former to later. The de-

sign for the generating of the first round key is as follows

$$k_4 = k_0 \oplus k_2 \quad (16)$$

$$k_5 = k_1 \oplus k_3 \quad (17)$$

$$k_6 = k_4 \oplus k_5 \quad (18)$$

$$k_7 = k_5 \oplus SubWord(RotWord(k_6)) \oplus Rcon(1) \quad (19)$$

Supposing that attackers have known the key (k_4, k_5, k_6, k_7), and they can't deduce the original key (k_0, k_1, k_2, k_3) , because k_7 only depends on k_5 and k_6, k_6 only depends on k_4 and k_5,while k_5 depends only on k_1 and k_3. Even if they know k_5, they still need 2^{32} exhaustive attacks to get k_1 and k_3 (each character length is 32bit). For the same reason, if they want to get k_0 and k_2 from k_4, 2^{32} times attacks are needed. So after attackers get the first round sub-key, they still need 2^{64} times to guess the original key. So our algorithm can meet the safety requirement.

According to the analysis above, the attacker needs to crack two successive rounds of sub-key to get the whole key bits. So our algorithm has higher key security compared to the AES algorithm, but the complexity remains the same.

III. Performance Analysis and Simulation

As mentioned above, the LDPC-based error correcting cipher in paper [9] is a pretty good encryption and error correcting method. But the method described in this paper has an even better performance. In this section, we will discuss the security, key size, error correction capability and efficiency of the new method, and give the corresponding simulation results.

3.1 Security

The main idea of LDPC-based error correcting cipher is to replace the last 4 rounds of AES encryption operation with LDPC coding. As LDPC encoding is a linear operation, it has the diffusion properties which are equivalent to the AES diffusion layer, and can replace parts of round function to simplify the calculation. However, in the SPN structure of the block cipher algorithm, security mainly depends on the nonlinear part -- S-box, and the diffusion layer only has the effect of transmitting the anti-attack ability of S-box. Therefore, LDPC-based error correcting cipher actually reduces 4 rounds of the scramble operation, and its simplification of calculation is at the cost of reducing the security of the algorithm. However, our method preserves the 10 rounds of operation and keeps the same security.

Meanwhile, compared with the traditional method of encrypting and error correcting respectively, the security of our method is further improved by using error correction coding in the encryption process [17], while the security of the AES algorithm is guaranteed. Assuming that the channel is a BSC channel, encrypted transmission process is as follows

$$Y_n = X_n \oplus K \oplus E_n \quad (20)$$

Where X_n is the encoded codeword, K is the 10th round key and E_n is the channel errors. Obviously, the legitimate receiver can get round keys and calculate them

$$X_n' = Y_n \oplus K = X_n \oplus E_n \quad (21)$$

And the ciphertext before encoding can be obtained by error correction decoding. On the other hand, the attacker can't recover the ciphertext without knowing the round key K, even if he knows the full detail of encoding and decoding algorithms. Therefore, this method has more security than that in the traditional secure communication system.

In addition, the difficulty of attacking to the key is increased due to the new key generation algorithm proposed in this paper. You can deduce other round keys as long as you know one round key in the AES algorithm. Instead, only when you know two or more round keys, you can decrypt other round keys with the new method. At the same time, the first round key is unidirectional which can be only deduced from front to back.

The ability to resist the three major attacks of AES with our method is illustrated as follows:

(1) Resistance to differential attack

Differential cryptanalysis is a chosen plaintext attack. It deduces the key by using the difference propagation property of a cipher. AES uses a wide trail strategy in the design of block cipher round function. It can achieve the provable upper bound of differential characteristic probability which is called trail. Reducing the probability of trail, that is to limit the differential propagation probability, is the design idea of the wide trail strategy. Since the differential trail prediction probability after 4 rounds of transformation in AES algorithm is not greater than 2^{-150}[18], it has a good performance against differential attack. Our system merely integrates the LDPC coding into the 10th round of the AES encryption, and does not change the fundamental principle of AES, so the encryption method in this system still has a good resistance to differential attack.

(2) Resistance to saturation attack

Saturation attack is also called square attack. Its main idea is to use the balance changes in the 4th round of AES algorithm to guess key bytes. It has higher efficiency than exhaustive search for the 4 to 6 rounds simplified version of AES with 128-bits key.

Current studies have shown that saturation attack of 6 rounds can be achieved in the complexity of 2^{63}. And 7 rounds or more of AES can be considered secure for saturation attack. Our method uses 10 rounds AES encryption, and improves the key generation algorithm. The attacker cannot further deduce the keys even with the last round key. Therefore, this method can resist the saturation attack.

(3) Resistance to power analysis attack

The main characteristic of power analysis attack is to use an appropriate instrument to measure the leaked energy information when the encryption devices are running. It speculates the key to decipher the encryption algorithm after the statistical analysis of a large amount of power curve [19].

Power analysis attack on AES, often choose to carry out at the output moment in a round of encryption (in order to prevent the initial key from being cracked in the first XOR operation, adding noise or masking when the initial key XOR operating). Even though the attack succeeds and gets a round key, the attacker cannot deduce the initial key due to the improvement of the key generation algorithm, which is more complicate and unidirectional, so the resistance to power analysis attack is also improved.

3.2 Key size

In the LDPC-based error correcting cipher, system keys consist of 128-bits AES encryption key and the 256*512 check matrix H of LDPC codes. However, the system key only depends on the 128-bits AES encryption key in this paper. As the LDPC encoding is operating during the encryption process, the encoding operation is under the protection of the round key, therefore, system can achieve the same security capability as LDPC-based error correcting cipher without the check matrix H. For block cipher algorithm, 128 bits key strength already has adequate security. In a word, this method saves 256*512 bits key space, greatly reduces the key size.

3.3 Error correcting capability

In this method, error correcting capability depends on the ability of selected LDPC codes. Since encoding and decoding processes of LDPC are public, we can choose the best code words to ensure the error correction performance. In the original method, the LDPC matrix is composed of key bytes which are chosen randomly. Considering the computation cost, they construct the LDPC matrix which is just without Girth-4 by simple method. Longer code words are available in this method than that in the original one, lead to a better performance. In the meantime, we can select appropriate LDPC code words according to different needs of satellite communications, which have good flexibility.

3.4 Efficiency

As mentioned in section 3.1, the reducing of the computation cost and time delay of LDPC-based error correcting cipher is actually

Fig.3 *Original image*

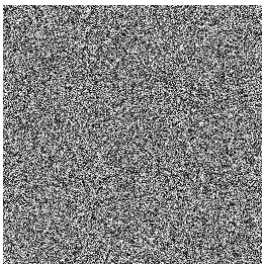

Fig.4 *Image with SEEC*

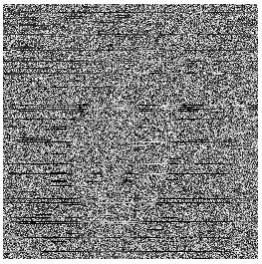

Fig.5 *Recovered image* (**SNR** *is 1dB*)

Fig.6 *Recovered image* (*SNR is 1.5dB*)

Fig.7 *Recovered image* (**SNR** *is 2dB*)

Fig.8 *Recovered image* (*SNR is 2.5dB*)

based on the reducing of four rounds of AES operation, the reduced AES degrades the security of AES. In addition, encryption in that method is followed by error correction. As the LDPC generator matrix consists of two vectors, parity vector and information vector, and the change of the generator matrix does not affect the information vector, an interleaving jammer would have to be added for confusing after the encoding completed. In our method, the security of encryption is already ensured and due to the inside process of encoding, it is unnecessary to confuse anymore and therefore improves the efficiency.

3.5 Simulations

To test the performance of encryption and error correction, simulations are conducted in MATLAB.

LDPC is now widely used in FEC of DVB-S2 system. Because DVB-S2 system communicates through geosynchronous satellite, and ground antenna with high gain is installed in an open place, the communication channel can be simulated as AWGN in sunny weather [20].

Parameters we selected are as follows:

Table I *Simulation parameters*

Parameter	Value
Block Length	128*4
Key Length	128
Number of Iterations	20
Code Length	1024
Code Rate	1/2
Decoding Algorithm	Min-Sum
Modulation	BPSK
Channel	AWGN

An image is used as the encryption data source to show the effects of encrypting and coding.

With the matrix of satellite communications standard for LDPC coding, it makes the decoding algorithm achieve the optimized performance. Simulation results show that the method we proposed has a good encryption and error correction effect. After transmission in AWGN channel, when SNR is 1dB, the original image can hardly be recovered because of the error diffusion effect of AES; when SNR is 1.5dB, legal users are able to see the image basically; when SNR is 2.5dB, the original image can be recovered clearly by legal users.

Fig.9 illustrates the BER performances of our proposed method compared with LDPC-based error correcting cipher, which SNR varies from 0dB to 4dB. The performance of two methods is close when SNR is lower than 1dB. If SNR is higher than 2.5dB, the new method can completely recover the original image. However, the old method can recover full data only when SNR is higher than 3.6dB.

Fig.10 illustrates the PSNR performances

of our proposed method compared with LDPC-based error correcting cipher, which SNR varies from 0dB to 4dB. It is obviously that the original image can get a good visual effect when SNR is higher than 2.5dB. However, the old method can achieve the same effect only when SNR reaches at 3.5dB or above.

So the new method improves a lot on transmission performance. When it is used in satellite communications, the transmitting power can be reduced.

IV. Conclusions

In this paper, we propose a joint encryption and error correction coding method which applies to satellite communications domain. In this method the secret key of AES is adopted as the system key, the parallel encryption coding is implemented in order to take advantage of LDPC's excellent performance for long LDPC codes. At the same time, a new sub-key generation algorithm is proposed to keep the system more secure. The experimental results show that this method can accurately recover the original data in the condition that the signal-to-noise ratio is greater than or equal to 2.5dB.

Acknowledgement

This work was supported by the National 863 Project of China under Grant No.2012AA01A509, No.2012AA120800.

References

[1] MCELIECE R J. A Public-Key Cryptosystem based on Algebraic Coding Theory[R]. NASA Jet Propulsion Laboratory, Pasadena, Calif, USA, 1978.

[2] KORZHIK V I, TURKIN A I. Cryptanalysis of McEliece's Public-Key Cryptosystem[R]. Brighton, UK, 1991.

[3] RAO T. Joint Encryption and Error Correction Schemes[C]// In International Symposium on Computer Architecture (ISCA): June 1984. Ann Arbor, USA. 1984: 240 –241.

[4] WANG Xinmei. Generalization of M Public Key System and Analysis of Its Performance on Noisy Channel[J]. ACTA Electronica Sinica, 1986, 14(4): 84-90.

[5] WANG Xinmei. MC Error Correcting Block Cipher Systems [J]. Journal of China Institute of Communications, 1986, 7(5): 1-6.

[6] NIEDERREITER H. Knapsack-Type Cryptosystems and Algebraic Coding Theory[J]. Problems of Control and Information Theory, 1986, 15(2): 159-166.

[7] MATHUR C N, SUBBALAKSHMI K P. On the Design of Error-Correcting Ciphers[J]. EURASIP Journal on Wireless Communications and Networking, 2006: 1–12.

[8] ZUQUETE A, BARROS J. Physical-Layer Encryption with Stream Ciphers[C]// IEEE International Symposium on Information Theory, ISIT'08: July 6-11, 2008. Toronto, ON. 2008: 106–110.

[9] SU Qing, XIAO Yang. Design of LDPC-Based Error Correcting Cipher[C]// In Proc. of 2nd International Conference on Wireless Mobile and Multimedia Networks (ICWMMN): Oct 12-15, 2008. Beijing, CN. 2008: 470–474.

[10] LENG Wenyan, SANG Lin, XU Chengxin, *et al*.

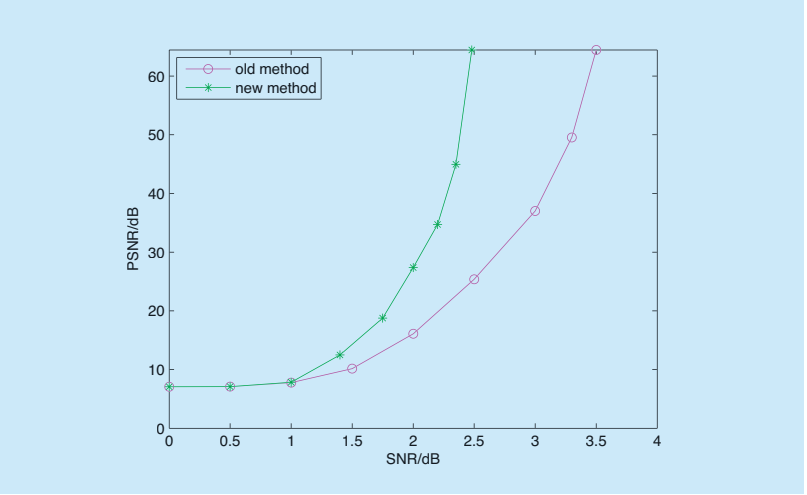

Fig.9 *BER performance*

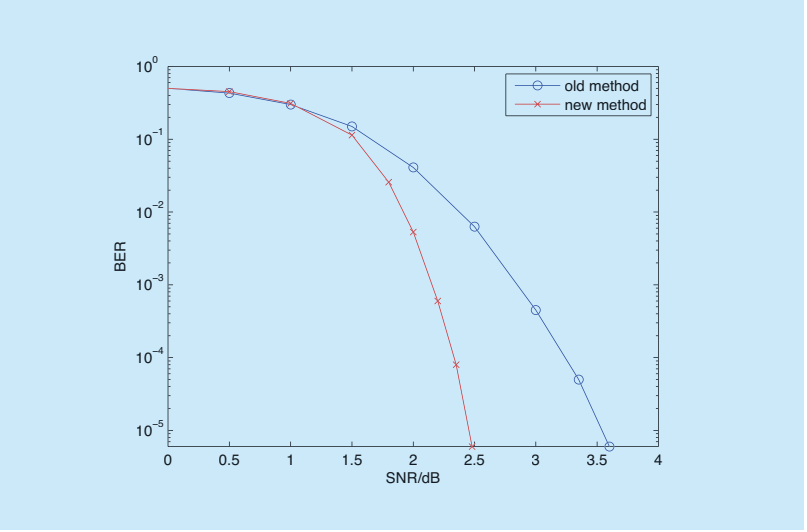

Fig.10 *PSNR performance*

Applications of Modulation in a McEliece-Like Symmetric-Key Scheme[C]// Vehicular Technology, IEEE Conference - VTC -Spring: May 16-19, 2010. Taipei, TW. 2010: 1-4.
[11] ADAMO O, VARANASI M R. Joint Scheme for Physical Layer Error Correction and Security[J]. ISRN Communications and Networking, 2011: 1–9.
[12] ADAMO O, AYEH E, VARANASI M. Joint Encryption Error Correction and Modulation (JEEM) Scheme[C]// Communications Quality and Reliability (CQR), 2012 IEEE International Workshop Technical Committee on: May 15-17, 2012. San Diego, CA. 2012: 1–5.
[13] CCSDS 131.1-O-2. Low Density Parity Check Codes for Use in Near-Earth and Deep Space Applications[S]. 2007.
[14] ZHANG Zuotao, FANG Yibo, LIU Guanghui. Two Efficient Algorithms Based on Majority-Logic and Min-Sum Algorithms for LDPC Codes[C]// Wireless Communications, Networking and Mobile Computing (WICOM): Sept 21-23, 2012. Shanghai, CN. 2012: 1–4.
[15] CHARI S, JUTLA C, RAO J R, *et al*. A Cautionary Note Regarding Evaluation of AES Candidates on Smart Cards[C]// The 2nd AES Candidate Conference: Mar 22-23, 1999. Rome, IT. 1999: 133-150.
[16] YANG Yixian, SUN wei, NIU XinYi. Modern Cryptography Theory[M]. Beijing, CN: Science Press, 2002.
[17] GUO Jin, WANG Jian, YUAN Jian, *et al*. Physical Layer Encryption Communication Systems with Block Ciphers[J]. Journal of Tsinghua University (Sci & Tech), 2011, 51(11): 1733-1737.
[18] ZENG Xiangyong, ZHANG Huanguo, LIU Heguo. Differential Characters of the Advanced Encryption Standard[J]. Journal of Wuhan University (Nat Sci. Ed), 2004, 50(1): 60-64.
[19] SMITH K, LUKOWIAK M. Methodology for Simulated Power Analysis Attacks on AES[C]// Military Communications Conference: Oct 31-Nov 3, 2010. San Jose, CA. 2010: 1292-1297.
[20] MA Qi, LAN Xing, CHENG Zengpin. Variable-Rate Low-Density Check Codes for Satellite Communication System[J]. Signal Processing, 2009, 25(5): 729-734.

Biographies

LI Ning, female, Ph.D., associate professor at the School of Electronic Engineering, Beijing University of Posts and Telecommunications. Research Interests: Information Security, Satellite Communications. E-mail:lnmmdsy@bupt.edu.cn

LIN Kanfeng, male, graduate student at the school of Electronic Engineering, Beijing University of posts and telecommunications. Research Interest: Satellite Communications, Information Security. E-mail: 18810534397@139.com

LIN Wenliang, male, PhD student at the School of Electronic Engineering, Beijing University of Posts and Telecommunications. Research Interest: Satellite communications, Information security.

DENG Zhongliang, male, Ph.D., professor at the School of Electronic Engineering, Beijing University of Posts and Telecommunications. Research Interests: Satellite Navigation and Communications.