Joint AES Encryption and LDPC Coding

C P Gupta, Shilpa Gautam

Abstract—For past many years secure and error free transmission of data has always been great challenge in conventional communication system. Traditionally error correction and encryption in communication networks have been addressed independently. Over 30 years discussion has been carried out to perform error correction and encryption in single step. In this paper we propose a Joint AES Encryption and LDPC coding scheme, which provides security comparable to AES and also exhibits good error correction capability. We show that performance of our proposed scheme is comparable to sequential approach of performing first encryption and then encoding and yet it turn out to be efficient in term of providing faster computation.

Index Terms— Encryption, Error Correcting Code, Advanced Encryption Standard (AES), LDPC code, Joint error correction and encryption, bit error rate (BER).

1 INTRODUCTION

AS the development of complex communication applications has increased rapidly in recent years, the need of secure and error free communication has also increased. In the past various separate developments [1], [2], [3] have been made to achieve security and reliability of communication. However security is achieved by applying cryptographic primitives on transmitted data, this also results in making transmitted data more sensitive towards channel noise and little errors in transmission may cause failure of encryption process. In order to prevent failure of encryption process, it is necessary to adopt coding scheme before transmission. Until recent years, the concatenate process (as shown in Figure 1) of encryption followed by encoding is being used to make transmission secure and error free.

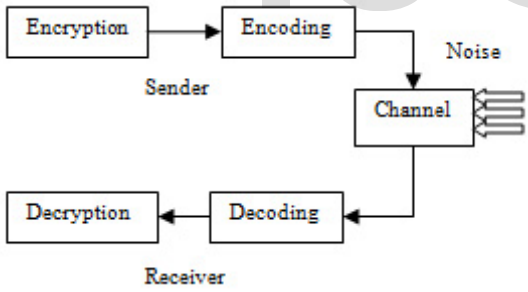

Fig.1. Traditional approach of first Encryption and then Encoding

This sequential process of encryption and then encoding consumes more computational time and resources; these separate primitives can be combined together as a single primitive and then applied on data to be transmitted.

- *C P Gupta is an associate professor in computer science engineering in Rajasthan Technical University, Kota, India. 324010 E-mail: guptacp2@rediffmail.com.*
- *Shilpa Gautam is pursuing masters degree in computer science engineering in Rajasthan Technical University, Kota, India. 324010 E-mail : shilpa.gautam18@gmail.com*

First such development was made by McEliece [4] almost 30 years ago and since then several successful attempts [5], [6], [7], [8], [9], [10] have been made to combine encryption and error correction process.

2 RELATED WORK

McEliece [4] proposed a public key cryptosystem based on algebraic codes which uses same hardware used for error correction to achieve security. The public key cryptosystem proposed by McEliece was hardware efficient but it was unable to protect cryptosystem against chosen-cipher text attack [11]. Later, S kak worked on method to show connection between decimal expansions and encryption in public key ciphers [5]. The method shows that the proposed cipher block generates a continuing D sequences, therefore sending more digits than the minimum necessary for uniquely defining cipher block provides a degree of redundancy that can be used for error correction. Unfortunately, his work has not been scalable and did not attract further attention. In the later years, private key cryptosystem remained preferable choice of researchers because of low resource requirement and implementation complexity in comparison to public key cryptosystem. One such private key cryptosystem scheme named Secret Error Correcting Codes (SECC) [6] is proposed by Rao et al. This scheme suffered from reduction in error correction capacity of codes used and in order to achieve meaningful error correction capacity, the parameters of the system have to be very large leading to high computation complexity [12]. Gilgoroski et al. proposed a joint error correction and encryption scheme based on quasigroup (Latin Square) string transformation [7]. The parameter used in this scheme is chosen from quasigroup (latin -square) of order 16,(Q,*) and for each combined primitive a quasigroup is chosen out of at least 2^{430} possibilities. This property makes Gilgoroski's scheme secure than previously proposed methods. The error correction is done by adding random redundant information to each message. But the decoding procedure turns out to be very complex to implement and thus consumes more resources in implementing.

One common drawback found in above proposed schemes is that, they have compromised error correction over security. The codes used in previous schemes exhibit low error correc-

tion capacity. The High Diffusion Cipher proposed by C.Mathur et al. [8] is proven secure and exhibited high error correction capacity. The proposed High Diffusion (HD) Cipher uses structure of Advanced Encryption Standard AES where the diffusion operation of the AES is replaced with HD encoding operation of High-Diffusion codes [13]. Though HD cipher scheme provide data security and error correction, it is higher in complexity compared to McEliece based scheme and the AES. AES-TURBO [9] and Error Correction Based Cipher [10] are most recent proposed schemes. The combined AES and TURBO coding scheme AES-TURBO [9] also uses structure like AES. The error correction is done by emerging turbo code encoder after in first round on AES like structure and remaining steps of AES encryption are followed normally. In the decryption phase Turbo Decoder block is embedded in AES Decryption block in the last round. In another recent proposed scheme ECBC [10], Adamo et al. proposed a private key cryptosystem based on McEliece scheme. According to this scheme, an input k-bit plaintext block is enciphered into n-bit ciphertext block by first performing non linear substitution on input plaintext and then multiplying this substituted vector with generator matrix of error correction codes used. Although this scheme uses same hardware component available for error correction for security but security of system relies only on non-linear substitution function used. In order to evaluate security of ECBC, Chai and Gong revealed that ECBC scheme is vulnerable to chosen-plaintext attack and thus allows the secret generator matrix used for encoding to be recovered in O(1) [14]. In this paper, we have proposed a Joint AES Encryption and LDPC coding scheme that turn out to be as secure as AES [15] and also retains full error correction capability of LDPC codes [16] which are known for their capacity approaching performance [3].

3 PROPOSED JOINT AES ENCRYPTION AND LDPC CODING SCHEME

We have proposed a private key cryptosystem called Joint AES and LDPC Coding that combines encryption and error corretion into single primitive. Like standard block cipher [1], the proposed scheme is composed of iterative rounds. Our proposed scheme is consists of seven rounds and each round consists of three distinct layers key addition layer, non linear layer and linear diffusion layer. The structure of proposed Joint AES encryption and LDPC coding can be seen in Figure 2. As it can be seen from block diagram of proposed scheme, structure of first six rounds is same as Advance Encryption Standard and the last round incorporate error correction capability to the scheme. Our proposed scheme encrypts 128-bit plaintext into 256-bit ciphertext after completion of seven rounds. The 128-bit block is divided into 16 bytes to form a 4x4 array called state which is further passed to following round operations.

3.1 Key Adiition Layer

The first operation performed on input plaintext state is the key addition operation. First the 128-bit secret is expanded into 32 words (word size 16) using a key expansion algorithm, which is similar to that of the AES key expansion algorithm

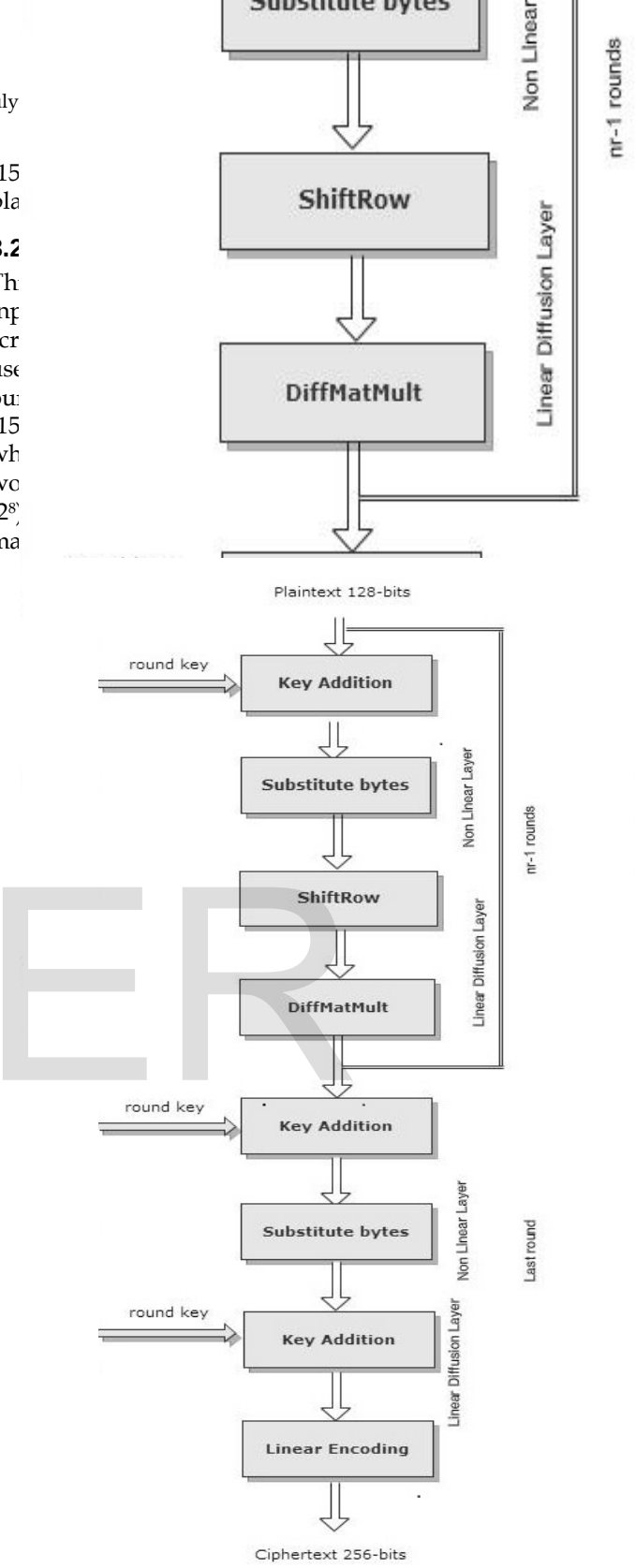

Fig. 2. Proposed Joint AES Encryption and LDPC Codng

3.3 Linear Diffusion Layer

In this layer we use operations like diffusion matrix multiplication and LDPC encoding to jointly attain maximal diffusion and error correction capability. For initial six rounds, the input state goes through two operations, ShiftRow and DiffMatMult.

First operation cyclically shifts bytes of each row of state and second operation provides diffusion by multiplying cipher-state with diffusion matrix. The ShiftRow operation and DiffMatMult operation performed in first six rounds is similar to ShiftRow operation and MixColumns of AES algorithm [15]. In ShiftRow operation, the rows (first row to fourth row) of state is circular shift by zero, one, two and three bytes respectively. In MixColumns, state is multiplied with a predefined matrix. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. In the last round state Linear Diffusion layer is consists of key addition and encoding operation of state with the Low Density Parity Check codes [16], [17].

As diffusion is consider as quantitative measure of security of a cipher [15]. The diffusion property of cipher can be define as a charactric where one bit of ciphertext depends on plaintextbits in a very complex way, such that if one bit of the plaintext is changed then it will affect long range of cipher bits. In the scheme we presented, we examined bit propagation rate (Rp) to measure diffusion provided by our proposed scheme. In a single round of AES, a single change in bytes of state can cause in change in four bytes of state due to ShiftRow and MixColumn operations of round. Thus for ten rounds of AES this propagation rate can be summed as 4^9 (last round does not add into diffusion as MixColumn operation is not present). Similarly propagation rate of six rounds of proposed scheme is 4^6 while the last round of scheme consists of LDPC encoding whose propagation rate is 128 ($4^{3.5}$). The propagation rate of seven rounds of proposed scheme is summed as ($4^{9.5}$) which is greater than bit propagation rate of AES. This shows that our proposed scheme is more secure and efficient than AES as it takes fewer rounds to obtain more disperse ciphertext than the AES.

In order to decrypt received cipphertext, the layer operations of scheme are replaced with corresponding reverse operations. In decryption process of proposed scheme, ciphertext is decoded in the first round using iterative sum product decoding algorithm (SPA) [18]. The channel error induces by noisy channel is corrected by this layer of decryption scheme, now error free 128-bit data is passed to Inverse Non Linear Layer(Inverse S-Box), Key Mixing Layer. Now result from first round passed to next rounds which consist of inverse operation of ShiftRow, Inverse MixColumn and Inverse Non Linear Layer (Inverse S-Box) and then Key Mixing Layer.

4 Simulation Results

In our simulation, we construct a seven round Joint AES Encryption and LDPC coding cryptosystem with input plaintext data and secret key of size 128-bits and output ciphertext obtained is of size 256-bits. This is achieved by using regular [128, 256, 3] low density parity check (LDPC) code at the last round. Initial six rounds of proposed scheme contribute in security while last round contribute in achieving both security as well error correction capability. The parity check matrix [128, 256, 3] H used in order to perform LDPC encoding is a randomly constructed sparse matrix of size 128x256 having only 3 non-zero values in its column and 6 non-zero values in its rows. In our simulations, The H is constructed by random construction method proposed by McKay [19]. The performance of our proposed joint AES encryption and LDPC coding scheme is evaluated by calculating bit error rate (BER) over additive white Gaussian noise channel. In results presented here, we compared performance of proposed scheme with performance of sequential process of encryption followed by encoding. It can be observed from Figure 3 that proposed joint AES encryption and LDPC coding scheme and the sequential system are comparable in terms of error correction capacity over a range of signal to noise power spectral density Eb/N0. The sequential system exhibit such results after running ten rounds of AES encryption/decryption process first and then error correcting coding/decoding is done. However, as error correction coding is performed within seven rounds of encryption /decryption process of our proposed joint scheme we are roughly saving three rounds per encryption/decryption performed compared to sequential system. This results in faster simulation and takes significantly less time than sequential system.

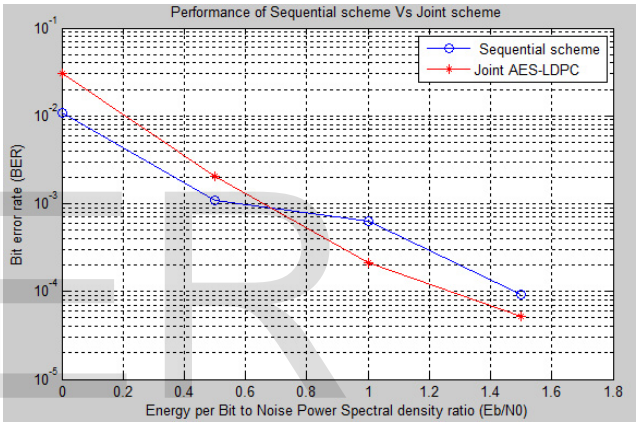

Fig. 3. Performance of Sequential Vs Proposed Joint scheme

We also compared performance of our proposed scheme in terms of error correction capacity with earlier proposed combined encryption and error correction scheme AES-TURBO [9]. Here, the result presented in figure 4 shows error correction capacity of AES-TURBO scheme for different number of iterations used in iterative decoding.

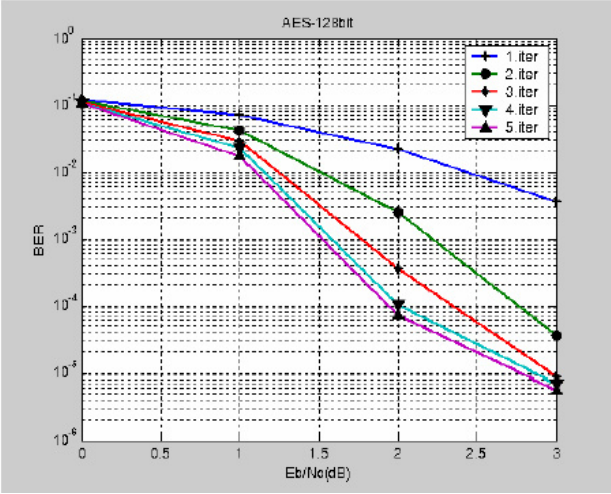

Fig. 4. For N=128, Bit Error Rate (BER) Performance over AWGN channel of AES-TURBO

In order to compare our proposed scheme with results prsented in AES-TURBO [9], we also simulated our proposed joint scheme for different iteration values varying from one to five numbers of iterations. From the results presented in figure 5, it can be observed that error correction capacity of our proposed Joint AES Encryption and LDPC coding scheme is comparable to results of AESTURBO scheme. Unlike other previously proposed schemes, our scheme retains full error correction capacity of codes used in scheme. The Low Density Parity Check coding is one of the practical coding schemes that could approach Shannon's channel capacity [19], [3]. In contrast to this, our result shows that our joint scheme achieves reliability by attaining bit error rate of 10^{-5} at E_b/N_0 within 1.31 dB of the Shannon limit for E_b/N_0=0.188dB needed for reliable communication over additive white Gaussian noise channel.

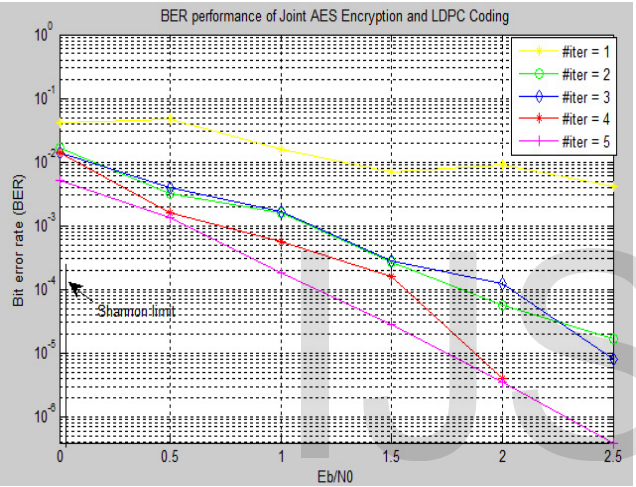

Fig. 5. BER performance of Joint AES and LDPC Coding over AWGN Channel

From the simulation results presented here, it is observed that our proposed joint AES Encryption and LDPC coding scheme exhibits good bit error rate performance comparable to traditional sequential scheme and also results in faster implementation than the sequential process. The result presented here shows that, the error correction capacity of joint AES encryption and LDPC coding has not been compromised and the scheme achieves reliable communication at E_b/N_0 just 1.31 dB near to Shannon's limit.

5 Conclusions

With the recent invention of joint schemes for encryption and encoding, achieving secure and error free transmission has become faster and efficient. However, combining encryption and encoding as single primitive becomes challenging as process of encryption and encoding work at cross purpose with each other, in the work presented here we tried to combine both on common characteristic of diffusion exhibited by both primitives. We proposed a joint AES encryption and LDPC coding which takes only seven rounds and yet provide same degree of diffusion as ten rounds of AES. The proposed joint scheme overcomes the trade-off between security and error correction capability of earlier proposed schemes. The simulation result shows that joint AES encryption and LDPC coding shows performance comparable to traditional sequential scheme and yet it is faster in computation. The proposed joint scheme here used low density parity check codes for error correction and LDPC codes are best known for their capacity approaching performance i.e. LDPC codes gives very low probability of error (10^{-5}) at SNR value close to Shannon limit of given channel. Our simulation results shows that proposed joint scheme retains error correction capacity of LDPC codes used and can achieve reliable transmission (error probability 10^{-5}) within 1.31 dB near to Shannon limit of additive white Gaussian channel.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. Prentice-Hall Press, 2006. (Book style)

[2] S. Gravano, *Introduction to Error Control Codes*. Oxford University Press, 2010. (Book style)

[3] G. Forney and D. Costello, "Channel coding: The road to channel capacity," Proceedings of the IEEE, vol. 95, no. 6, pp. 1150–1177, 2007.

[4] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, vol. 42-44, pp. 114–116, 1978.

[5] S. Kak, "Encryption and error-correction coding using d sequences," *IEEE Transactions on Computers*, vol. 100, no. 9, pp. 803–809, 1985.

[6] T. Hwang and T. Rao, "Secret error-correcting codes (secc)," in *Advances in Cryptology-CRYPTO'88*. Springer, 1990, pp. 540–563.

[7] D. Gligoroski, S. Knapskog, and S. Andova, "Cryptcoding-encryption and error correction coding in a single step," in *Proceedings of International Conference on Security and Management*. Citeseer, pp.1–7, 2006. (Conference proceedings)

[8] C. Mathur, K. Narayan, and K. Subbalakshmi, "High diffusion cipher: Encryption and error correction in a single cryptographic primitive," in *Applied Cryptography and Network Security. Springer*, pp. 309–324, 2006.

[9] H. Cam, "A combined encryption and error correction scheme: Aes-turbo," *ISTANBUL University-Journal of Electrical & Electronics Engineering*, vol. 9, no. 1, 2012.

[10] O. Adamo and M. Varanasi, "Joint scheme for physical layer error-correction and security," *ISRN Communications and Networking*, vol. 2011, 2011.

[11] H. Sun, "Further cryptanalysis of the mceliece public-key cryptosystem," *Communications Letters, IEEE*, vol. 4, no. 1, pp. 18–19, 2000.

[12] K. Zeng, C. Yang, and T. Rao, "Cryptanalysis of the hwang-rao secret error-correcting code schemes," *Information and Communications Security*, pp. 419–428, 2001.

[13] C. Mathur, "A mathematical framework for combining error correction and encryption," Ph.D. dissertation, Stevens Institute of Technology, 2007. (Thesis)

[14] Q. Chai and G. Gong, "Differential cryptanalysis of two joint encryption and error correction schemes," in *Global Telecommunications Conference (GLOBECOM 2011). IEEE*, pp. 1–6, 2011.

[15] J. Daemen and V. Rijmen, "The block cipher rijndael," in *Smart Card Research and Applications, Springer*, pp. 277–284, 2000.

[16] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[17] D. MacKay and R. Neal, "Good codes based on very sparse matrices," *Cryptography and Coding*, pp. 100–111, 1995.

[18] D. MacKay, Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2003.

[19] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, 1999.