ISTANBUL UNIVERSITY –
JOURNAL OF ELECTRICAL & ELECTRONICS ENGINEERING
YEAR : 2009 (891-896)
VOLUME : 9
NUMBER : 1

A COMBINED ENCRYPTION AND ERROR CORRECTION SCHEME:AES-TURBO

Hakan CAM[1] Volkan OZDURAN[2] Osman N. UCAN[2]

[1]Turkish Air Force Academy, Yesilyurt, Istanbul
h.cam@hho.edu.tr

[2]Istanbul University, Engineering Faculty, Electrical and Electronics Eng. Dept. 34320, Avcilar, Istanbul, Turkey
volkan@istanbul.edu.tr uosman@istanbul.edu.tr

ABSTRACT

In this paper, we introduced a new type of Encryption and Error Correction scheme, which is called "A Combined Encryption and Turbo Coding Scheme: AES-TURBO". Although in previous studies error correction and encryption are handled independently, we combined error correction and Encryption functionality into one single step. This combined System's performances are evaluated in AWGN (Additive White Gaussian Noise) channel type. The results are compared with the system employing ideal encryption and decryption.

Keywords: *Advanced Encryption Standard(AES), Turbo Coding, Encryption and Error Correction.*

1. INTRODUCTION

In this paper, we introduced a new type of Encryption and Error Correction scheme which is called "A Combined Encryption and Turbo Coding Scheme: AES-TURBO" In previous studies [1-2] error correction and encryption are handled independently. In the transmitter part of the system the data is encrypted by using one of the encryption techniques before it is sent through the wireless channel. After that, the encrypted data is sent to the Turbo encoder block [3]. The output of the turbo encoder block is sent to the wireless channel according to the channel model. In the receiver part of the system; The data taken from the wireless channel is sent to the turbo decoder block. The output of the turbo decoder block is sent to the decryption block. At the end of this process original plaintext can be obtained.

On the other hand, in this study we combined Error correction and Encryption functionality into one single step. In this proposed system we chose AES[4] for encryption and decryption process and turbo codes [3] for encoding and decoding.

According to general perspective of the system Turbo Encoder block is embedded in AES encryption block in the first round after subbytes block. The remaning steps of the AES encryption are followed normally .

Received Date: 10.10.2008
Accepted Date: 05.01.2009

In the decryption phase Turbo Decoder block is embedded in AES Decryption block in the last round before SubBytes block.

2. MATERIAL

2.1. AES (Advanced Encryption Standards)

The input and output for the AES algorithm each consist of sequences of 128 bits (Digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard [4].

The quantity of circles changes depending on the width of key. For 128 bit key , at the process of encryption in 10 circles , for the length of key 192 and 256 bites, the encryption process is done 12 and 14 circules subsequently. According to key size AES is named as "AES-128","AES-192", and"AES-256" [4-5].

2.1.1. AES Encryption Process

In the process of encryption, first, 128 bit is transfered to 4x4 byte matrix. Later, the bytes while changing their places in each circle, the table's mixing and before the key planing the XOR actions with definite keys are done for coming circle. In the process of byte's place changing, the value of 16 byte, 8 bit of entrance and 8 bit of exit are entered in S box. In the process of shiftrows, the row`s of 4x4 byte matrix shift and the process of Mixcolumns, columns values are mixed. At the end of the circle`s last layer, XOR process is done with the key which belongs to that circle.[4-5]

Below is presentation of AES Encryption Algorithm which chooses 128 bit key size.

2.1.2. AES Decryption Process

Decryption process of AES is reverse of Encryption process. The individual transformations used in the Decryption process - InvShiftRows, InvSubBytes, InvMixColumns and AddRoundKey [4]. Decryption process is presented in figure 2.

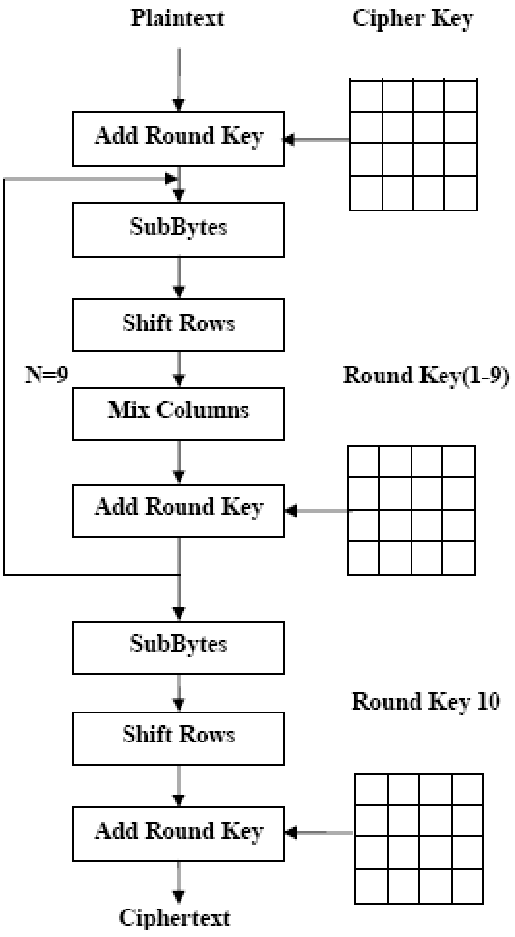

Figure 1. AES Encryption Process Scheme.

2.2 Turbo Coding

Turbo codes are a new class of error correction codes that were introduced a long with a practical decoding algorithm in [3]. The importance of turbo codes is that they enable reliable communications with power efficiencies close to the theoretical limit predicted by Claude Shannon [6]. Since their introduction, turbo codes have been proposed for low-power applications such as deep-space and satellite communications, as well as for interference limited applications such as third generation cellular and personal communication services [7].

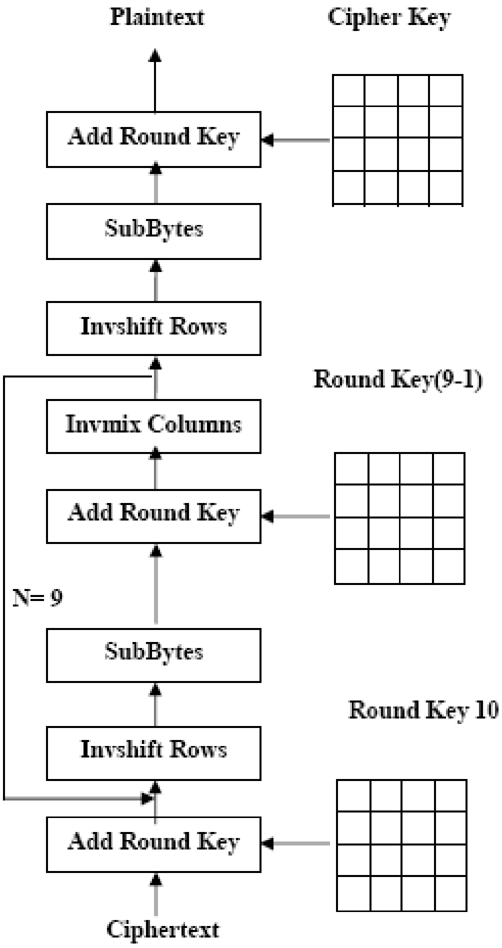

Figure 2. AES Decryption Process scheme.

2.2.1. Turbo Encoder

A Turbo encoder is a combination of two simple encoders. The input is a block of information bits. The two encoders generate parity symbols from two simple recursive convolutional codes, each with a small number of states. The information bits are also sent uncoded. The key innovation of turbo codes is an interleaver, which permutes the original information bits before input to the second encoder. The permutation allows that input sequences for which one encoder produces low-weight codewords will usually cause the other encoder to produce high-weight codewords. Thus, even though the constituent codes are individually weak, the combination is suprisingly powerful. The resulting code has features similar to a 'random' block code with information bits [8].

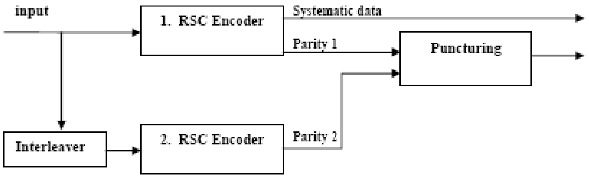

Figure 3. Turbo Encoder

2.2.2. Turbo Decoder

Random block codes are known to achieve Shannon-limit [6] performance as gets large, but at the price of a prohibitively complex decoding algorith. Turbo codes mimic the good performance of random codes using an iterative decoding algorithm based on simple decoders individualy matched to the simple constituent codes. Each constituent decoder sends a posteriori likelihood estimates of the decoded bits to the other decoder and uses the corresponding estimates from the other decoder as a priorilikelihoods. The uncoded information bits (corrupted by the noisy channel) are available to each decoder to initialize the priori likelihoods. The decoders use the `MAP` (Maximum a Posteriori) bitwise decoding algorithm, which requires the same number of states as the well-known viterbi algorithm. The turbo decoder iterates between the outputs of the two constituent decoders until reaching satisfactory convergence. The final output is a hard-quantized version of the likelihood estimates of either of the decoders [8].

Turbo encoder's structure is presented in figure 4.

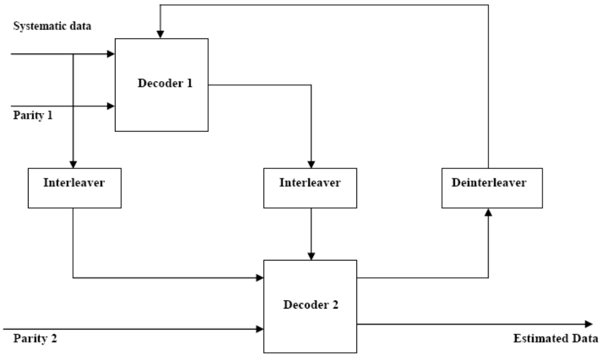

Figure 4. Turbo Decoder.

3. METHODS

We introduced a new type of Encryption and Error Correction scheme which is called “A Combined Encryption and Turbo Coding Scheme: AES-TURBO”. This combined system is presented in figure 5.

In the transmitter part of the system, Turbo Encoder block is embedded in AES encryption block in the first round after subbytes block. The remaning steps of the AES encryption are followed normally After that The bit stream is sent to the wireless channel

For simulation, we choose AWGN (Additive White Gausian Noise) channel model

In the receiver part of the system, the bit stream is taken from the wireless channel. The remaning steps of the AES decryption process are followed normally. Turbo Decoder block is embedded in AES in the last round before SubBytes block.

4. EXPERIMENTAL RESULTS

Frame size is chosen 128 bits and AWGN (Additive White Gaussian Noise) channel is considered . The bit error rate performance of overall system is investigated over mobile communication channel for various Signal to Noise Ratios (**SNR**s).

4.1. Bit Error Rate (Ber) Performance Over Awgn Channel Model

Frame size is 128 bite and Channel model is AWGN chosen. The bit error rate performance of overall system is figured in figure 6.

4.2. Bit Error Rate (Ber) Performance Over Ideal Channel Model

Frame size is 128 bit and Channel model is ideal chosen. The bit error rate performance of overall system is figured in figure 7.

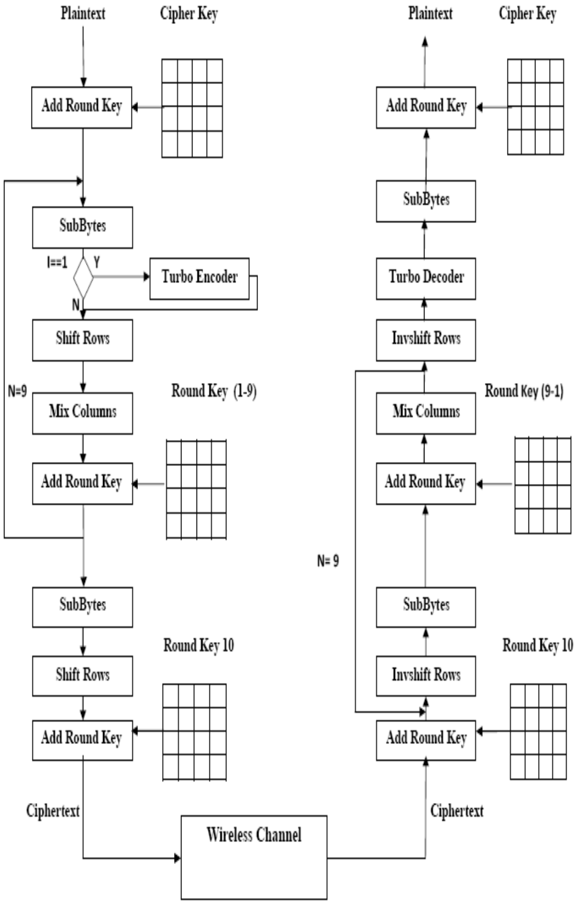

Figure 5. A Combined Encryption and Error Correction Scheme:AES-TURBO.

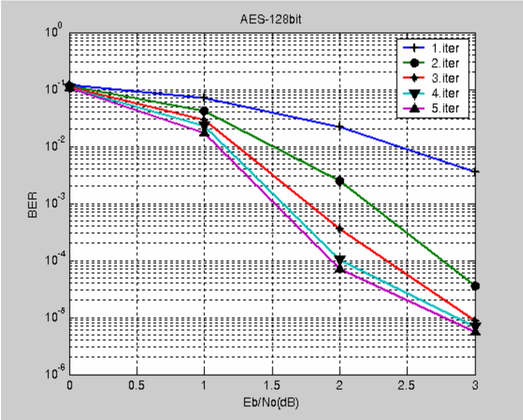

Figure 6. For N= 128, Bit Error Rate (BER) Performance over AWGN Channel.

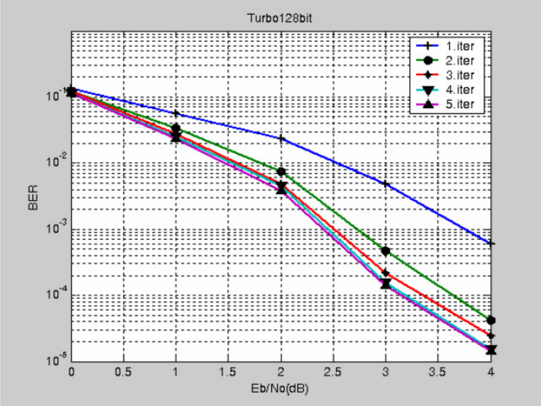

Figure 7. For N= 128, Bit Error Rate (BER) Performance over ideal channel.

5. CONCLUSION

In this study, we introduced a new type of Encryption and Error Correction scheme, which is called “A Combined Encryption and Turbo Coding Scheme: AES-TURBO”. This Combined systems will help to manufacturing Monoblocks in a single step.

6. AKNOWLEDGEMENT

We would like to thank to Asisst. Prof. Dr. Niyazi ODABAŞIOĞLU from University of Istanbul and Prof. Dr. Istvan VAJDA from Budapest University of Technology and Economics for their valuable comments.

7. REFERENCES

[1] V. OZDURAN,“Combined Encryption and Turbo Coding Systems (in Turkish)”, *Msc. Thesis, University of Istanbul*, February, 2008.

[2] V. OZDURAN, N.O. UCAN, M. GUREL, O. OSMAN, “Combined Encryption and Turbo Coding Systems”, *2nd Communication Technologies and Application Symposium (HABTEKUS)*, 22-23 October, 2008, Yildiz Technical University, Istanbul.

[3] C. BERROU, A. GLAVIEUX, P. THITIMASJSHIMA, “Near Shannon-limit error correcting coding and decoding: Turbo codes,” *Proc. ICC’93*, pp. 1064-1070, 1993.

[4] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, *U.S. Department of Commerce, Washington D.C.*, November 26, 2001.

[5] M.T. SAKALLI, 2006, Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi, *Doktora Tezi, Trakya Üniversitesi*.

[6] C.E. Shannon, “A mathematical Theory of communication”, *Bell Sys. Tech. J.*, Vol: 27, pp. 379-423 and 623-656, 1948.

[7] O. BAYAT , H. ALNAJJAR , O. N. UCAN, O. OSMAN, “Performance of Turbo Coded Signals Over fading channels”, *Istanbul University Journal of Electrical & Electronics*, Vol: 2, No. 1, 2002, pp. 417-422.

[8] http://www331.jpl.nasa.gov/public/TurboForce.GIF

BIOGRAPHIES

Hakan CAM is currently a Ph.D. student in Computer Engineering in ASTIN (Aeronautics and Space Technologies Institute), in Turkish Air Force Academy, Istanbul. He graduated from Yenimahalle Technical High School, Department of Computer, Ankara, in 1992. He received his B.Sc. Degree in Electronics Engineering from Turkish Air Force Academy, Istanbul, in 1996. He received M.Sc. Degree in Computer Engineering from ASTIN, Istanbul, in 2004.

Volkan OZDURAN graduated from Soke Technical High School, Department of Electronics in 1997. He Graduated from The Department of Industrial Electronics Program with high honors degree, Istanbul University, Istanbul, Turkey in 2002. He received the B.Sc. degree from the Department of Electrical and Electronics Engineering, College of Engineering, Istanbul University, Istanbul ,Turkey, in 2005. He received M.Sc. degree in Electrical and Electronics Engineering from the Institute of Science, Istanbul University in 2008.

Osman Nuri UCAN He received the BSEE, MSEE and PhD degrees in Electronics and Communication Engineering Department from the Istanbul Technical University (ITU) in 1985, 1988 and 1995, respectively. During 1986-1997 he worked as a research assistant in the same university. He became project manager at TUBITAK-Marmara Research Center in 1998. He is now Professor At Istanbul University (IU). His current research areas include: information theory, channel modeling, turbo coding and image processing. He is married and has one son and one daughter.