Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 3, No.9, 2012
www.iiste.org

A new approach to ward off Error Propagation Effect of AES – Redundancy Based Technique Redefined

Bikramjit Sarkar[1*], Chandan Tilak Bhunia[2], Ujjwal Maulik[3]

1. Dr. B. C. Roy Engineering College, Durgapur, West Bengal, India
2. National Institute of Technology, Yupia, Arunachal Pradesh, India
3. Jadavpur University, Kolkata, West Bengal, India

* E-mail of the corresponding author: sarkar.bikramjit@gmail.com

Abstract

Advanced Encryption Standard (AES) [1, 2] is a great research challenge. It has been developed to replace the Data Encryption Standard (DES). AES suffers from a major limitation of Error propagation effect. To tackle this limitation, two methods are available. One is Redundancy Based Technique and the other one is Bite Based Parity Technique. The first one has a significant advantage of correcting any error on definite term over the second one but at the cost of higher level of overhead and hence lowering the processing speed. In this paper we have proposed a new approach based on the Redundancy Based Technique that would certainly speed up the process of reliable encryption and hence the secured communication.

Keywords

Advanced Encryption Standard, Error Propagation Effect, Redundancy Based Technique, Longitudinal Redundancy Check Code

1. Introduction

The redundancy based technique [3 – 6] needs two modules: encryption module and decryption module for producing error-free cipher at the transmitter. The output cipher of the encryption module is decrypted by the decryption module. The decrypted output is compared with the plain text to check for error. If they match, the cipher is taken to be error-free and it is transmitted over the channel. The dual process of encryption and decryption by the technique make the encryption process slow and costly. Below is an example to clarify the process of Redundancy Based Technique.

128-bit Message (Plain Text): Bikramjit Sarkar

Corresponding Hexadecimal values: 42 69 6b 72 61 6d 6a 69 74 20 53 61 72 6b 61 72

128-bit Cipher key (Hex): 2B 28 AB 09 7E AE F7 CF 15 D2 15 4F 16 A6 88 3C

128-bit Cipher text (Hex): FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

If a one-bit error is now injected in the 8^{th} bit position of the intermediate cipher generated after 7^{th} round and the encryption process continues through 3 more rounds of AES encryption, an erroneous cipher text will be generated at the output as follows:

8A 88 3E 2D DC 16 77 90 4D B3 05 3E CA 04 4D 0C

Now on comparing the erroneous cipher with the error free cipher we get errors in 70 bits at the cipher text. It is, therefore, seen that a single bit error, if injected after 7^{th} round in 8^{th} bit position, leads to the generation of huge number of errors at the output cipher. Now if this erroneous cipher is decrypted back, we get a message (erroneous plain text) in the corresponding hexadecimal values as follows:

B2 C9 A7 34 CF 60 C6 24 75 F5 4B CD 9F 97 3C 62

Now on comparing the erroneous message with the error free message (plain text), we find errors in 57 bits in the erroneous message. This implies that that the message generated after decrypting the erroneous cipher text differs from the original message (plain text) and that the cipher text is not supposed to be sent to the receiver. This is basically the Redundancy Based Technique to ward off the error propagation effect of AES.

Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 3, No.9, 2012

It is clear that the Redundancy Based Technique requires the comparison of 128 bits since the plain text taken is of 128 bits. Here we propose to modify the Redundancy Based Technique that will reduce the overhead of comparison to only 16 bits.

2. Proposed Technique

We get the cipher text from the plain text after the AES encryption of 10 rounds. Here we consider that both the block size (plain text) and the key size are of 128 bits.

Now we carry on the experiment on Redundancy Based Technique to ward off the error propagation effect of AES. Here we require both the Encryption Module and the Decryption Module at the transmitter end. First the Longitudinal redundancy Check (LRC) code (Odd) L_1 is generated from the input state (plain text) P and then P is encrypted through the encryption module to generate the cipher text C which is then again decrypted to find P'. Again another LRC code (Odd) L_2 is generated from P'. L_1 and L_2 are then compared. If the comparison proves L_1 and L_2 to be same, it means, there is no error injected / generated in the intermediate states of the encryption process, assuming that the entire decryption process is free from any error. The cipher text is hence considered to be error-free and is transmitted. It should be noted that the introduction of LRC Code Generator leads to comparisons amongst only 16 pairs of bits instead of 128 pairs of bits. The block diagram of the proposed scheme is shown in Figure 1.

2.1. Experimental results

Character wise Binary Equivalent is first generated from the plain text.

42	69	6b	72	61	6d	6a	69	74	20	53	61	72	6b	61	72
								↓							
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	1
0	1	1	0	0	1	1	1	0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
1	0	1	1	0	0	1	0	0	0	1	0	1	1	0	1
0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0

Generated Odd LRC Code (L_1): 1 1 0 1 0 0 1 1 1 0 1 0 1 0 0 1.

Character wise Binary Equivalent is then generated from the Decrypted Message (generated from the Original Message after encryption and then again decryption) as before:

B2	C9	A7	34	CF	60	C6	24	75	F5	4B	CD	9F	97	3C	62
								↓							
1	1	1	0	1	0	1	0	0	1	1	1	1	1	0	0
0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	1
1	0	1	1	0	1	0	1	1	1	0	0	0	0	1	1
1	0	0	1	0	0	0	0	1	1	0	0	1	1	1	0
0	1	0	1	1	0	0	1	0	0	1	1	1	0	1	0
0	0	1	0	1	0	1	0	1	1	0	1	1	1	1	0
1	0	1	0	1	0	1	0	0	0	1	0	1	1	0	1
0	1	1	0	1	0	0	0	1	1	1	1	1	1	0	0

Generated Odd LRC Code (L_2): 1 1 0 0 1 1 1 1 0 1 1 0 1 0 1 0.

Now L_1 and L_2, both of 16 bits, are compared with each other and the comparison reveals that L_2 differs L_1 by 7 bits, which implies that there were error(s) injected in the encryption process and the cipher generated is erroneous. So the input state is again left for further processing to generate the error free cipher text to be transmitted. It should be noted that if P and P' be equal, L_1 and L_2 are also equal, indicating that no error has been injected / generated in the encryption process assuming that the decryption process is entirely free from errors.

3. Conclusion

In this paper we have proposed a new approach based on the Redundancy Based Technique to tackle the error propagation effect of AES. Redundancy Based Technique has a limitation of lower speed of encryption. According to this method, there is a particular step of comparison of 128 pairs of bits. Our approach has minimized the overhead of comparison from 128 pairs of bits to 16 pairs of bits. Although an additional module of LRC Code Generator that has been introduced in our approach causes an extra overhead of the new approach, yet the proposed technique is superior.

References

Allen Household et al. (2002), "Computer Attack Trends and Challenges", Internet Security and Privacy, IEEE Computer Society, pp 5-7.

NIST (2001), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication, No. 197.

Chandan T Bhunia (2005), "Information Technology , Networks and Internet" , New Age International Publishers , New Delhi.

Guido Bertoni et al. (2004), "Error analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard", IEEE Trans on Computers, Vol-52, No. 4, pp 492-504.

Chandan T Bhunia et al (2004). Project Work on AES Error Propagation, Indian School of Mines, Deemed University, Dhanbad, India.

B. Sarkar et al. (2008), "Study and Analysis of Error Propagation Effect of Advanced Encryption Standard", Int'l J HIT Transaction on ECCN, Vol.–2, No. 7.

Mr. Bikramjit Sarkar started his career with teaching profession in 2004. Currently he has been working as an Assistant Professor in the dept. of Computer Science and Engineering in Dr. B. C. Roy Engineering College, Durgapur, India. Previously he worked in different Institutes, both Private and Government. He has worked as the Head of the Departments for more than 3 years. Currently he is pursuing Doctor of Philosophy (Engineering) in Jadavpur University, Kolkata, India under the joint supervision of Prof. (Dr.) Chandan Tilak Bhunia and Prof. (Dr.) Ujjwal Maulik.

Dr. Chandan Tilak Bhunia took up the teaching profession by choice. He joined the University on resigning the lucrative job of Engineer of a public sector. He worked as Professor, Head of the Departments, Deans and Dy. Director / Director of several institutes and universities for above 16 years out of which a considerable period is on nomination and invitation. He visited different corners of the globe on several assignments including chairing Technical Sessions, BOYSCAST Fellowship and delivering Invited Talks. Currently he has been working in the capacity of Director of the National Institute of Technology, Arunachal Pradesh, established by the MHRD, Govt. of India. He is also attached to the International Centre for Theoretical Physics, Italy as a Senior Associate.

Dr. Ujjwal Maulik is a Professor in the Department of Computer Science and Engineering, Jadavpur University, Kolkata, India since 2004. He was the Head of the Department of Computer Science and Technology Department of Kalyani Govt. Engineering College, Kalyani, India during 1996-1999. Dr. Maulik has worked in Los Alamos National Laboratory, Los Alamos, New Mexico, USA, University of New South Wales, Sydney, Australia, University of Texas at Arlington, USA, University of Maryland Baltimore Country, USA, Fraunhofer Institute AiS, St. Augustin, Germany, Tsinghua University, China, University of Rome, Italy, University of Heidelberg, Germany, German Cancer Research Center (DKFZ). He has also visited many Institutes / Universities around the globe for invited lectures and collaborative research. He is the recipient of the Govt. of India BOYSCAST fellowship and Alexander von Humboldt Fellowship for Experienced Researchers and senior associate of ICTP, Italy. Dr. Maulik has been the Program Chair, Tutorial Chair and the Member of the program committee of many international conferences and workshops.

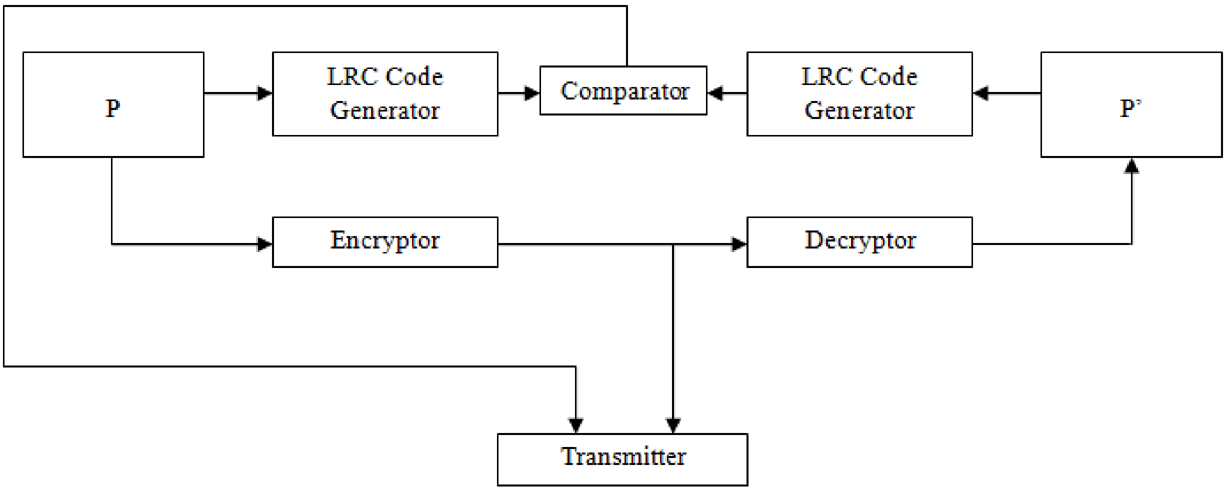

Figure 1. Block diagram of the proposed scheme