AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Zigbee Based Secured Wireless Transmission Using Advanced Blowfish Cryptographic Algorithm

[1]Kalaiarasi.D and [2]Prathipa.R, [3]Ranjana

[1]*Assistant Professor Department of Electronics and Communication Panimalar Institute of Technology.*
[2]*Assistant Professor Grade I Department of Electronics and Communication Panimalar Institute of Technology.*
[3]*Assistant Professor Department of Electronics and Communication Panimalar Institute of Technology.*

Address For Correspondence:
Kalaiarasi.D, Assistant Professor Department of Electronics and Communication Panimalar Institute of Technology

ARTICLE INFO

Article history:
Received 10 December 2015
Accepted 28 January 2016
Available online 10 February 2016

Keywords:
cryptography, ARM cortex 9, Blowfish, ULK, ZigBee, Graphics LCD

ABSTRACT

The project aims at implementation of secured data transmission system by means of encryption and decryption of data using advanced Blowfish algorithm in ULK(Unified Learning Kit) which has ARM cortex 9 as an OMAP 3530 chip and finally transmitting the cipher text through ZigBee and thereby enhancing the security of the transmitted data. The resulting output is the reliable, highly secured and inexpensive with decrease in delay of 0.15ns.

INTRODUCTION

This project aims at implementing secured data transmission using advanced Blowfish cryptographic algorithm. The Blowfish algorithm was based on X-OR operation of data with the encryption key, whereas the Advanced Blowfish algorithm uses X-NOR operation. The encrypted data from the transmitter ULK is decrypted by the receiver ULK enhancing the security of input data.Communication between each devices is done through ZigBee.ZigBee –a high level communication protocol plays important role in the transfer of encrypted data operating in the frequency range of 868MHz to 2.4GHz. Hence providing simple, inexpensive, reliable and responsive wireless communication mechanism.

The rest of the paper is represents as follows. Existing Blowfish algorithm and proposed algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

Proposed Algorithm:

A.Existing Blowfish algorithm –

1.Blowfish algorithm is a symmetric block cipher that uses Feistel network,iterating simple encryption, and decryption functions of 16times.

2. Blowfish has a 128-bit block size and a variable key length from 32 bits up to 448 bits.

3. The function splits the 64-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes.

4.The outputs are added modulo 2 and XORed to produce the final 32-bit output

5.The Blowfish encryption algorithm will run 521 times to generate all the sub keys - about 4KB of data is processed

Open Access Journal
Published BY AENSI Publication
© 2016 AENSI Publisher All rights reserved
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

Open Access

To Cite This Article: Kalaiarasi.D and Prathipa.R, Ranjana., Zigbee Based Secured Wireless Transmission Using Advanced Blowfish Cryptographic Algorithm. ***Aust. J. Basic & Appl. Sci.,*** *10(1): 332-336, 2016*

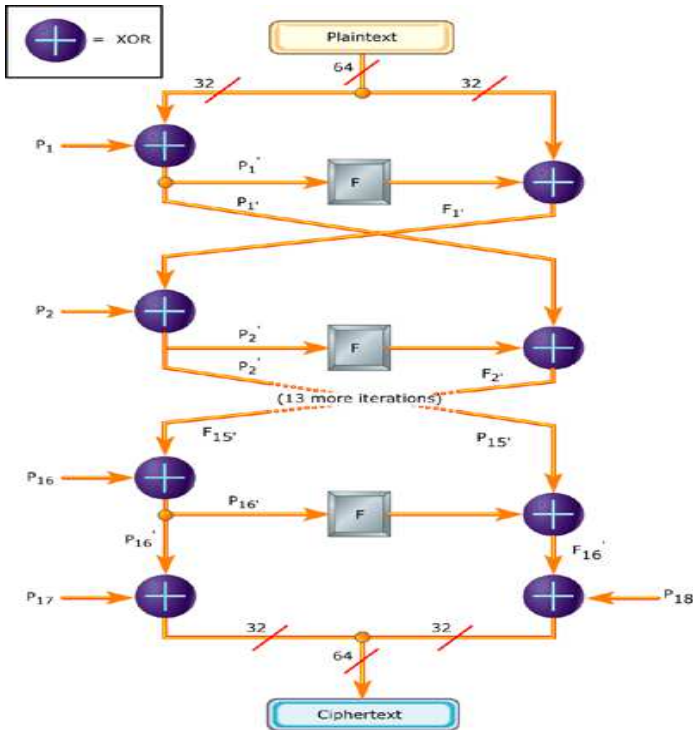

Fig. 1.1: A graphical representation of F appears

The key Expansion of BA begins with the P-array and S-boxes with the utilization of many sub-keys, which requires pre computation before data encryption or decryption. The P-array comprises eighteen 32-bit sub-keys: P1, P2… P18.

In this section a maximum key of 448 bits is converted into several sub-key arrays of up to a total of 4168 bytes.

There are 256 entries for each of the four 32-bit S-boxes:

S1,0, S1,1,..., S1,255
S2,0, S2,1,..., S2,255
S3,0, S3,1,..., S3,255
S4,0, S4,1,..., S4,255

Below is the explanation of how these sub-keys are calculated:

1.The P-array is initialized followed by the four S-boxes with a fixed string which has the hexadecimal digits of pi.

2. XOR P1 with the key's first 32 bits, XOR P2 with its second 32 bits, and so on until the key's bits are up to P14. The cycle is iterated through the key bits until the entire P-array has been XOR-ed with key bits.

3. The BA is then used for encrypting the all-zero string employing the described sub-keys in steps 1 and 2.

4. P1 and P2 are replaced with the step 3 output.

5. Encrypt the output of step 3 with the BA using the sub-keys that have been modified.

6. Output of step 5 is used to replace P3 and P4.

7. The process is continued, and all elements of the P-array are replaced, followed by all four S-Boxes, with the output continuously changing.

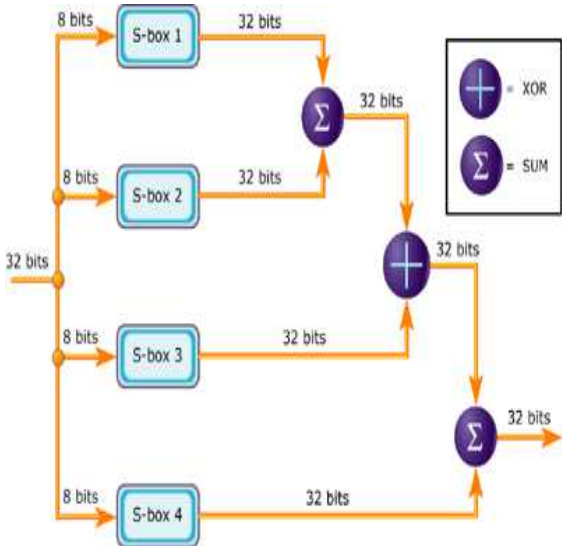

Fig. 1.2: Graphic representation of F appears

B.Advanced Blowfish algorithm:

1. The encryption on Blowfish algorithm was based on EX-OR operations of data bits with the encryption key, where the Advanced Blowfish algorithm will use EX-NOR operations.
2. The transmitted data from one ULK(Unified Learning Kit) with OMAP processor encrypted using blowfish cipher can be received and decrypted only by another ULK with the same algorithm which could decipher the transmitted data.
3. In the proposed system we use XNOR gate instead of XOR gate in the blowfish algorithm. X-NOR gate is the inverse of the exclusive XOR gate.
4. It uses less time to process the data than the XOR gate.
5. Thus encrypting input through advanced Blowfish cryptographic algorithm processed through python in the embedded system and transmitting through ZigBee protocol can made more effective security system.
6. Therefore it reduces the overall processing time in the algorithm by replacing XOR with XNOR.

Analysis of Algorithms:

The results which are obtained by running the simulation program using different data loads. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode used.

The superiority of Blowfish algorithm over
other algorithms in terms of the processing time. It shows also that AES consumes more
Resources when the data block size is relatively big.

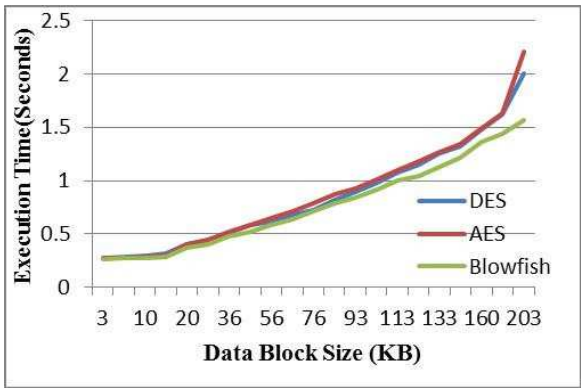

Fig. 1.3: Performance Results with ECB

As expected CBC require more processing time than ECB because of its keychaining nature. The results indicate that CBC is much better than ECB in terms of protection. The difference between the two modes is hard to identify by the naked eye because it is relatively small. Again the results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time.

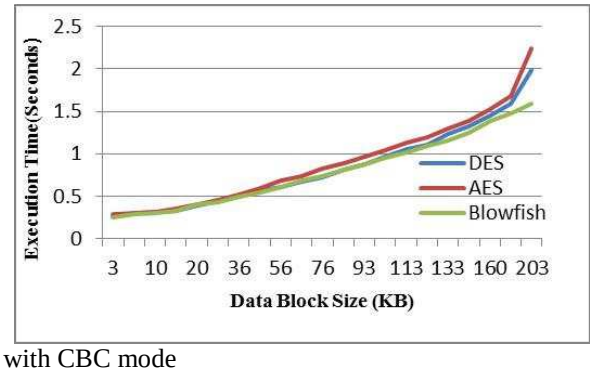

Fig. 1.4: Performance Results with CBC mode

The results indicate that the OFB is better for applications requiring output feedback and require less processing time than other modes. The difference between the three modes is hard to identify by the naked eye because it is relatively small. Again the results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time.

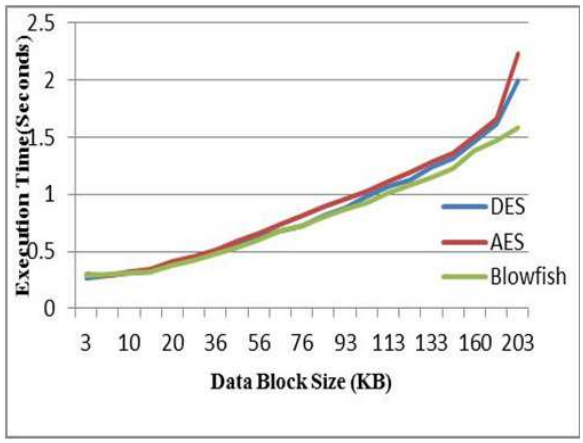

Fig. 1.5: Performance Results with OFB mode

As expected CFB require less processing time than ECB & CBC. The results indicate that the OFB is better than CFB in terms of processing time. The difference between the four modes is hard to identify by the naked eye because it is relatively small. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time.

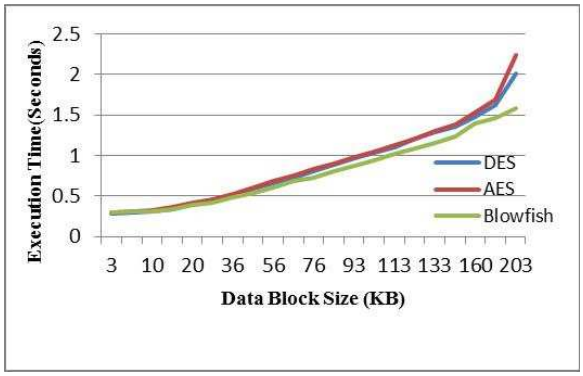

Fig. 1.6: Performance Results with CFB mode

Experiment And Result:

The experimental result as shifted from the existing Blowfish to advanced Blowfish algorithm with the replacement of Ex-or gates with Ex-nor gates are for the following reasons

On comparison the delay calculated between the existing and proposed system using Xilinx software is given as

1. The delay produced by each Ex-or gate in the existing system is found to be 2.68ns.

2. And the delay produced by each Ex-Nor gate of the advanced system is found to be 2.53ns
3. On comparison it has been calculated that difference in delay of 0.15ns has been decrease which increase the transmission speed of operation.

Theoretical Calculation:

For Delay:

Single Ex-or gate uses a delay of 2.68s as per the basepaper
Similarly single ex-nor gate uses delay of 2.53ns
Total delay difference = (0.15)ns
For 1 64bit operation=difference in delay * no.of x-nor gates used
For one 64bit (8byte operation) =0.15ns*50
One 64bit =8byte =7.5ns
Hence for 1Kbyte (8*128=1024byte) operation =7.5*128ns=960ns
For 1Mbyte(1024*1024byte)=960*1024ps=983040ns
Therefore for 1Mbyte transmission of data 0.983040ms delay has been produced.

Result:

Table 1.1: Delay per gate

TYPE	NO. OF TRANSISTORS	DELAY(ns)
EX-OR	6	2.68
EX-NOR	6	2.53

Reduction in the transmission delay of the system increases the speed of operation. Example: Transmission of secured video conferencing where several Giga to Terabytes are used.

Security Analysis of The System:

Security is the most important factor in the evaluation of cryptographic algorithms. Security encompassed features such as randomness of the algorithm output, avalanche effect, correlation coefficient resistance of the algorithm cryptanalysis, and relative security as compared to other candidates. Blowfish possess better performance when compared to AES,DES and 3DES algorithms with 2^448 combinations to examine all keys. Usage of ZigBee is less expensive and provides long battery life low power consumption comparative to other algorithms. Highly responsive and transmission of data over long distance using intermediate devices and mesh networks. Bluetooth has a wakeup delay of 3 seconds where Zigbee does not have possess any wakeup delays. Applicable for military applications sharing information for security of the country. Effective communication method for higher officials of different countries helpful for providing peace and security. Avoids tracking of information from unauthorized access. Also suited for passwords, banking applications etc.

Conclusion:

Thus by implementing our project we establish a most secure algorithm suitable and effective for hardware implementations which is license free and unpatented.In our advanced algorithm we reduce the major factor delay involved in the process which obviously increases the speed of operation.Zigbee uses long distance transmission with advantage of frequency sharing technique satisfying the needs of the future generations.

REFERENCES

"An implementation of data encryption standard using blowfish algorithm on FPGA" IEEE 2014 by Kurniawan Nur Prasetyo ST, Department of Computer System,University, Bandung, Indonesia, Yudha Purwanto, ST., MT.Departement of Computer System,School of Engineering Telkom University, Bandung, Indonesia And Denny Darlis, S.Si., MT.Diploma of TelecommunicationEngineering, School of Applied Science, Telkom University,Bandung, Indonesia

Ashwak ALabaichi, Faudziah Ahmad and Ramlan Mahmod, "Security Analysis of Blowfish algorithm", IEEE 2013 Universiti Utara Malaysia Kedah, Malaysia, Faculty of Sciences, Kerbala University and Universiti Putra Malaysia Serdang, Malaysia.

"A Study of DES and Blowfish Encryption Algorithm" TENCON 2009 byTingyuan Nie,Communication and Electronic Engineering Institute,Qingdao Technological UniversityQingdao, Chinatynie@qtech.edu.cn Teng Zhang Communication and Electronic Engineering Institute Qingdao Technological UniversityQingdao, China

"An Implementation of the Blowfish Cryptosystem" IEEE 2008 by Russell K. Meyers and Ahmed H. Desoky Computer Engineering and Computer Science Department Speed School of Engineering University of Louisville

"A VLSI Implementation of the Blowfish Encryption/Decryption Algorithm" by Michael C.-J. Lin, Youn-Long Lin Department of Computer Science National Tsing Hua University Hsin-Chu, Taiwan 30043, R.O.C. IEE 2000

"Data Encryption Performance Based on Blowfish Allam "47th International Symposium ELMAR-2005.08-1 0 June 2005. Zadar. Croatia by Mousa Electrical Engineering Department An-Najah N