International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

Design and implementation of Efficient embedded Cryptography algorithm using FPGA

Padmini.k, Leelavathi.G, UTL Technologies, Bangalore

Abstract

The traditional ideas and solutions focusing on network security problems are unsuitable for applications in which storage space and computing power are limited. In order to reduce cost in processor, this paper proposes a new embedded encryption algorithm based on linear feedback shift register. Because the algorithm is only composed by some basic operations such as the XOR and displacement, FPGA coprocessor with high performance and price ratio is adopted, through which our algorithm can achieve low cost and high speed in FPGA implementation. The experimental results show, compared with other known encryption algorithms, our algorithm has better performance on the whole, in particular the safety performance greatly outperforming other algorithms. Furthermore, FPGA-based hardware architecture of our proposed algorithm is presented in this paper and the architecture is synthesized and implemented on the Xilinx sapartan-3 FPGA. The design development is done in VHDL and simulates the results in modelsim 6.3 using Xilinx 12.2.

Index Terms—encryption algorithm, FPGA, LFSR.

Introduction

Encryption and decryption is the process of cryptography technique which should be provided secrecy of the data over the network. There are so many working areas which depend on large data bases over a public network like the banking sector, so there the security is of prime concern. Encryption is exhaustively used to keep confidential data. Other than encryption, there are so many cryptography techniques like digital signature, digital time-stamping, digital certificates etc. Used for security purpose. But encryption is the most used technique where transactions take place continuously between users [1, 2].

The communication skills have developed to the extent that the information passed must be at times concealed and protected for reasons such as integrity, authenticity and confidentiality.

Hence data can be transferred over one party to another party over insecure medium without fear of malicious practice. Cryptography algorithm encryption and decryption is an efficient scheme for both hardware and software implementation. As compare to software implementation, hardware implementation provides greater physical security and higher speed. Hardware implementation is useful in wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication.

Data Security is an important parameter for the industries. It can be achieved by Encryption algorithms which are used in the process called cryptography. It is a technique used to avoid an unauthorized access of data. It helps to provide accountability fairness and accuracy and also provide confidentiality. In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm.

The algorithm is efficient because the area utilization is optimized the used resource slice is less compared to other algorithm and in other algorithm key generation and sub key generation is done by using complex method like substitution, transformation and constant key is used in other algorithm .In this is algorithm key generation is done by using LFSR and security is more as key is changed till iteration of PN sequence completes. In all other algorithm the input plain text is specified to number of bits and also block size reduced into a particular no of bits but in this algorithm input plain text is not specified it can be any length and block size also can be done for any length because a generalized coding has been implemented for an input plain text and also for block size reduction this main advantage which overcomes from other algorithm.

In this paper, the main aim is to achieve security level and HDL coding is done to optimize the area utilization in Hardware and this algorithm can be used security purpose and also for communication purpose. Basis ideas of key management according to the principle based on linear feedback shift register (LFSR). The proposed embedded cryptography algorithm, adopts FPGA coprocessor to achieve and certify its correctness. In order to realize the algorithm, design with cryptogram library, and use it to choose all sorts of safety coefficient (operation mode, key length, cycle times etc.).

This paper is organized as follows. Section 2 gives a Brief analysis of the cryptography. Section 3 presents the implementation of proposed cryptography algorithm on FPGA. Simulation results are presented in Section 4. Comparison with previous algorithms in section 5. A conclusion is given in Section 6.

Overview of Cryptography

Cryptography can be defined as conversion of data plaintext (ordinary text) into cipher text (known as encryption), then back again (known as decryption) into plain text. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key, a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys.

Cryptography is the art of achieving security by encoding messages to make them non-readable [5].

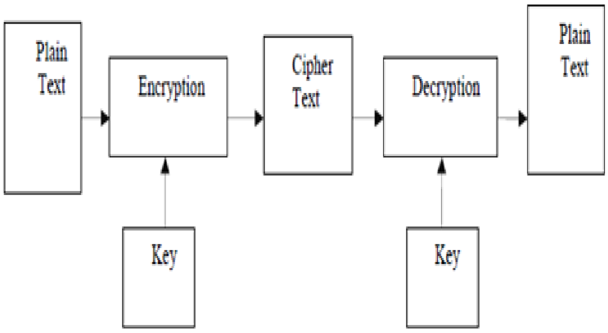

Figure 1 Basic Approach of Cryptography

The figure 1 gives an Basic approach of cryptography Where plain text is an original input and it is encrypted by using an suitable algorithm and key which is secret key which is an independent of an plain text and encrypted data which is known as cipher text and decrypted to obtain back the original data. Typically the sender and receiver agree upon a message scrambling protocol and methods for encrypting and decrypting the messages beforehand. The increasing need and interest in information protection have given rise to a new scientific field called cryptology. Cryptology is divided to two areas: cryptography and cryptanalysis.

Encryption is the process of transforming information (referred to as plaintext) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information in cryptography, referred to as cipher text. In many contexts, the word encryption also implicitly refers to reverse process. Encryption has long been used by militaries and governments to facilitate secret communication.

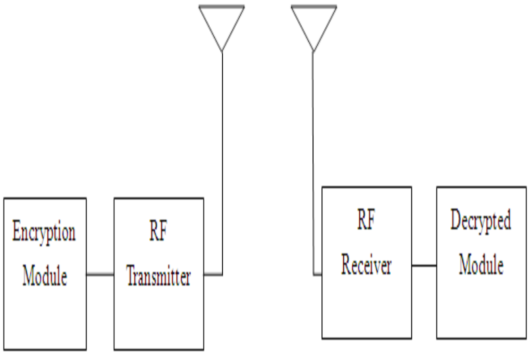

Figure 2 Block diagram of Transmitter and Receiver

Implementation of proposed system

In this section, we describe the hardware implementation of our proposed **efficient embedded Cryptography algorithm** on the Xilinx FPGA.

The block diagram consists of the transmitter and receiver section. The Figure 2 shows block diagram of overview of encryption and decryption where the data is transmitted by using RF transmitter and RF Receiver.

Encryption module*:* A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

RF Transmitter*:* This section transmits the encrypted data to space in a particular range based on the antenna used. This signal is received by the receiver.

The block diagram of the Receiver is given in Figure 2 the main parts in the receiver are Decryption module, RF Receiver

Decryption module*:* A decryption module which does the reverse of the encryption, so that the original information can be retrieved.

RF Receiver*:* The RF signal transmitted by the transmitter is detected and received by this section of the receiver. This encrypted data is sent to the decryption for decrypting the original data.

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text *;* encrypted data is referred to as cipher text.

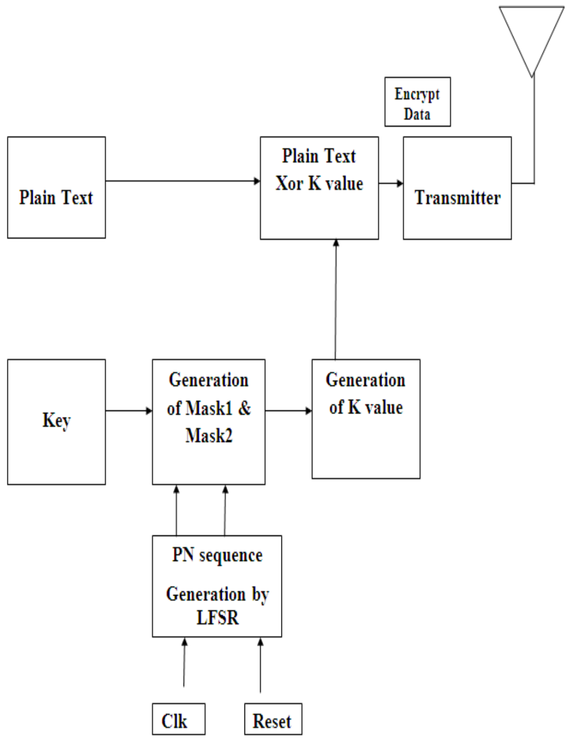

Figure 3 Block diagram of Encryption Module

The Figure 3 shows the block diagram where the encrypted data is transmitted when the receiver unit comes in the range of transmitter unit which continuously transmit RF signal, the whole receiver unit gets activated. The receiver unit receives the RF signal at a frequency range of 434 MHz's.

If plain text of any length is considered and its block size is reduced any number of bits a generalised code is written for that. If block size is eight bit then input key length chosen is sixteen then an sub key is generated by splitting an sixteen bit key to mask1 of eight bit and mask2 of eight bit then Most significant bit (MSB) of mask1 is replaced by an PN sequence generated by LFSR and Least significant (LSB) of mask2 is replaced by PN sequence generated by LFSR and sub key is generated which is of eight bit .in case plain text where block size is reduced into sixteen bit then input key length will be thirthy two bit the input key is split into sixteen bit of mask1 and other sixteen bit of mask2 where again MSB of mask1 is replaced by pn sequence generated by LFSR mask2 is replaced by pn sequence generated by LFSR new mask1 which is known as temp1 and new mask2 which is known as temp2 where tepm1 is xored with temp2 to get an sub key value of sixteen bit sub key is generated to get an encrypted data.

Decryption is the reverse, moving from unintelligible cipher text to the plain text. This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plain text.

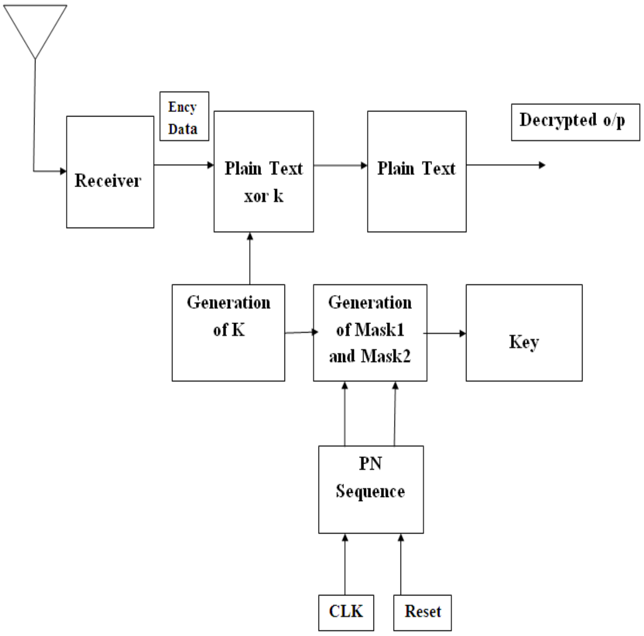

Figure 4 Block diagram of Decryption Module.

The Figure 4 shows the Decryption block diagram where it's used to retain the original message .The receiver receives the encrypted data where encrypted data is plain text xor with the sub key (K) for generation of sub key is done using the PN Sequence generated by LFSR and then original message is retained which of eight bit where decryption process completes in the proposed system the encryption of data has been discussed in paper the implemented the decryption of data is also implemented .

Simulation results and analysis

Proposed system is implementation in FPGA using Device Spartan-3 and Package PQ208.

Encryption top module is shown in Figure 5, the simulation results are shown in Figure 6

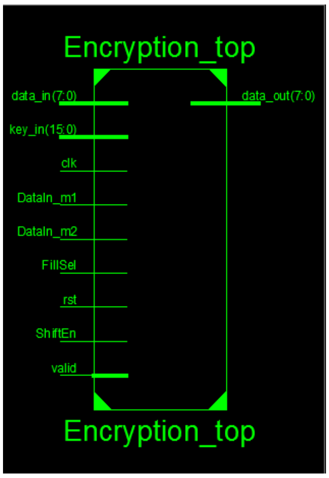

Figure 5 Encryption top Module

The encryption module contains clk, rst, valid, shiften, fillsel, data_m1, data_m2, key_in, 8-bit data_in are input ports and 8-bit data_out is output port.

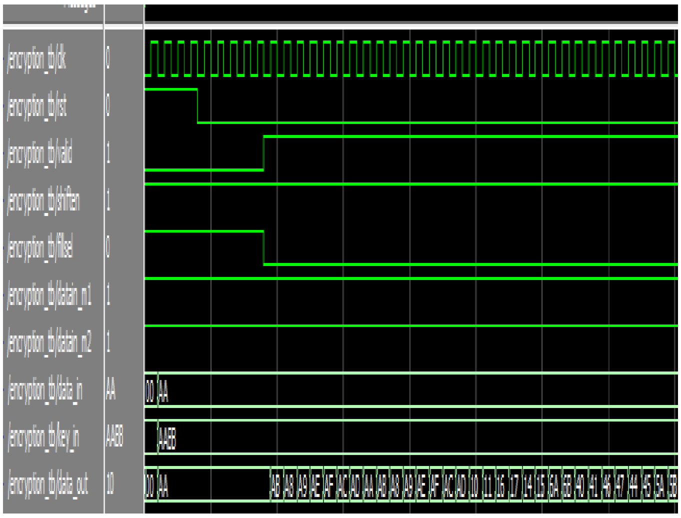
/encryption_tb/clk 0
/encryption_tb/rst 0
/encryption_tb/valid 1
/encryption_tb/shiften 1
/encryption_tb/fillsel 0
/encryption_tb/datain_m1 1
/encryption_tb/datain_m2 1
/encryption_tb/data_in AA
/encryption_tb/key_in AAEB
/encryption_tb/data_out 10
00 AA
AAEB
00 AA
AB A8 A9 AE AF AC AD AA AB A8 A9 AE AF AC AD 10 11 16 17 14 15 6A 6B 40 41 46 47 44 45 5A 5B

Figure 6 Encryption Module simulation results.

Decryption top module is shown in Figure 7 the simulation results are shown in Figure 8

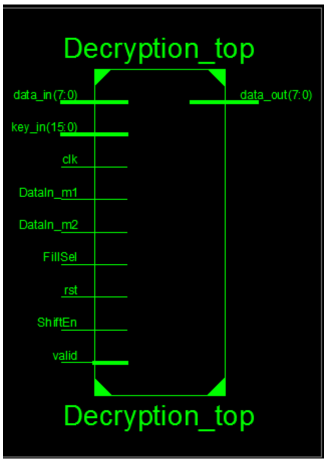

Figure 7 Decryption top Module

The decryption module contains clk, rst, valid, shiften, fillsel, data_m1, data_m2, key_in, 8-bit data_in are input ports and 8-bit data_out is output port.

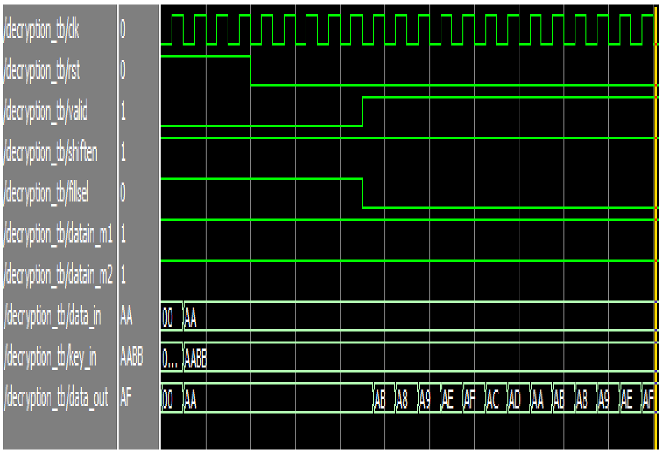
/decryption_tb/clk 0
/decryption_tb/rst 0
/decryption_tb/valid 1
/decryption_tb/shiften 1
/decryption_tb/fillsel 0
/decryption_tb/datain_m1 1
/decryption_tb/datain_m2 1
/decryption_tb/data_in AA
00 AA
/decryption_tb/key_in AABB
0... AABB
/decryption_tb/data_out AF
00 AA AB A8 A9 AE AF AC AD AA AB A8 A9 AE AF

Figure 8 Decryption Module simulation results.

Comparisonof encryption algorithm:

In the below table the comparison of Literature of [9, 10] ,proposed system, Implemented system is shown between the device used and usage of resource slice and data stream transmitted seeing the comparison the implemented system is efficient which has advantage of less usage of area and resource slice and same data stream is transmitted .

Table 1. Performance Comparisons for other algorithm

Comparsion	Apparatus	Resource slice	Data stream G bits/s
Pair wise key predistribution scheme for wireless Sensor networks. Literature [9]	XCV300E	832	1.21
key predistribution assignment schemes for sensor networks" Literature[10]	XCV300E	775	0.89
AEEA(Proposed algorithm)	XCV300E	717	1.18
AEEA(Implemented algorithm)	XC3S400	157	0.8

Conclusion

The Implemented an efficient embedded encryption algorithm (AEEA) based on LFSR, which includes merely basic operations of XOR and shift, is suitable for realizing safety communication of wireless communication. There is no complex method for generation of Key and sub key Generation. Generalized VHDL coding is implemented to select the block size of a plaintext. Adopting FPGA technique, it has fulfilled timing simulation of several optional encryptions and AEEA on the platform of FPGA the area utilization is optimized usage of resource slice is also less compare to previous works. The result proves that: the algorithm with the advantages of low design cost, high speed and strong antiattack security compare to

Acknowledgments

We the authors would like to thank the reviewers of journal for the completion of this paper..

References

[1] Shanta Mandal1 and Rituparna Chaki, "A secure encryption logic for communication in wireless sensor networks", in International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[2] Khushboo Sewak, Praveena Rajput and Amit Kumar Panda" FPGA Implementation of 16 bit BBS and LFSR PN Sequence Generator: A Comparative Study", IEEE Students' Conference on Electrical, Electronics and Computer Science 2012.

[3] Ben Othman, Soufiene; Trad, Abdel basset; Youssef, Habib "Performance evaluation of encryption algorithm for wireless sensor networks" Information Technology and e-Services (ICITeS),International Conference 2012, PP1 – 8.

[4] Gaochang Zhao Xiaolin Yang Bin Zhou Wei Wei "RSA-based digital image encryption algorithm in wireless sensor networks" Signal Processing Systems (ICSPS), 2nd International Conference on Volume:2,2010, V2-640 - V2-643

[5] William Stallings "Cryptography and network security",Pearson ,Fifth Edition 2011.

[6] Wei-Ming Lang, Zong-Kai Yang, Shi- Zhong Wu etc. "WSNsafety investigation.", Computer Science 2005, 32(5):PP.54-58.

[7] Zu-Chang Ma, Yi-NingSun,Tao Mei. "WSN summarize",CommunicationTransaction,2004,25(4):PP. 114-124.

[8] Zhong Su, Chuang Lin, Fu-Jun Feng, Feng-Yuan Ren. "Key and Solution in WSN", Software Transaction, 2007, Vol.18 No.5 PP.1218-1232.

[9] Du w, Deng J, Han Y S,Varshney P.A pair wise key predistribution scheme for wireless Sensor networks. In: proc of the 10th ACM Conf. on Computer and

Communications security (CCs), Washington: ACM Press, 2003, PP.1-10.

[10] Chan H, perring A, Song D.Random “key predistribution assignment schemes for sensor networks”, In:IEEE Symposium on Research in Security and Privacy, 2003.

[11] Amparo Fúster-Sabater and Dolores de la Guía-Martínez.“Modelling nonlinear sequence generators in terms of linear cellular automata”, Applied Mathematical Modelling, Volume 31, Issue 2, February 2007, PP. 226-235.

Biographies

Padmini.k received the B.E. degree in Telecommunication from the visvesvaraya technological university, Belgaum, Karnataka, in 2004.