12th International Conference on Recent Innovations in Science, Engineering and Management
Sri Venkateswara College of Engineering & Technology,Etcherla, Srikakulam (ICRISEM'18)
17th February 2018 www.conferenceworld.in ISBN: 978-93-87793-01-9

Synthesis of Cellular Automata Cryptography using AES Algorithm

Ch. Janardanarao[1], K. Govindarao[2]

[1]*PG Scholar Dept. of ECE , SVCET ,Srikakulam, AP, (India)*

[2] *Asst.Professor Dept. of ECE , SVCET ,Srikakulam, AP, (India)*

ABSTRACT

Secure system is most important part in the data communication. A digital media can be transmitted easily in real time anywhere at any time due to the multimedia technology and internet, but to maintaining a security of information is a biggest problem now a days. Cryptography playing a major role to provide security. This paper presents an efficient reconfigurable implementation of Advance Encryption Standard (AES) algorithm on Field Programmable Gate Array (FPGA); using High Level Language (HLL) approach with lesser hardware resources. The mode of data transmission in the modified AES is 128-bit plaintext and keys which converted into four 32bit blocks and exclusion of shift row. Using this feature, not only area is optimized but also higher throughput is achieved. The proposed architecture can deliver higher throughput at both encryption and decryption operations. Design has been done using Verilog and Xilinx 14.5

Keywords: AES, FPGA, encryption, decryption, , block cipher, Cellular Automata

I.INTRODUCTION

Cryptographic techniques are very important in these times dominated by the growth of digital information storage and transmission. In fact, increasingly available communication networks and databases make the need for privacy and authentication a basic requirement in many areas, especially in electronic commerce transactions and for classified material. There exist many different cryptographic techniques, an excellent review is given in [9]. Here we will describe the potential uses of some types of cellular automata (CA) in this domain. CA have previously been suggested as encrypting devices by Wolfram [10] and by Nandi et al. [8]. Independently, Guam [3] and Gutowitz [4] also used CA for cryptographic purposes. We will not discuss Guam's and Gutowitz's works

here since the principles on which they are based are different from ours. In particular, Guam's work concerns public-key cryptography, while we will only discuss symmetric systems, where the encryption key and the decryption key are the same or can be calculated from each other. As in references [8, 10].

Advance encryption standard find its rout in cryptography and network security, Because of cryptography, doing business electronically is possible without worries of deceit and deception. Cryptography technology has changed the world today by being able to carry data found in the physical world to the electronic world with confidence. Nowadays, hundreds of thousands of people interact electronically every day, whether it is through email, E-commerce, E-bank or cellular phones. As the network transmission speed upgrades to the gigabits per

second (Gbps), the software-based implementations of cryptographic algorithms cannot meet its needs. The hardware-based implementations can greatly improve throughput and reduce the key generation time. Besides, the processes of cryptographic algorithms and the key generation packaged in chip, which cannot easily be read or changed by external attacker, so hardware-based implementations can get the higher physical security. In recent years, many hardware based Implementations use the field programmable gate arrays (FPGA) and the application specific integrated circuit (ASIC) ASIC lacks of flexibility and has high development costs and long development cycle. Reconfigurable devices such as FPGA, with hardware of security and high speed and software of flexibility and easy maintenance, have become hardware-based implementations research hotspots for block cipher algorithm.

II. BACKGROUND

As we know, the security strength of Data Encryption Standard (DES) [1] has been difficult to adapt to new needs. In October of 2000, the National Institute of Standards and Technology (NIST) selected the Rijndael algorithm as the advanced encryption standard (AES), which was developed by Joan Daemen and Vincent Rijmen, in order to replace the DES. At present, Rijndael is the most common and widely used symmetric cryptosystem to support bulk data encryption. It offers a good "combination of flexibility, efficiency and safety" AES is the abbreviation of Advanced Encryption Standard also known as Rijndael algorithm. It is symmetrical block cipher which uses the same key for both encryption and decryption. The minimum length specified can be 128, 192 and 256 bits.

Cryptography has long been of interest to intelligence gathering agencies and law enforcement agencies. Because of its facilitation of privacy, and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to civil rights supporters. Accordingly, there has been a history of controversial legal issues surrounding cryptography, especially since the advent of inexpensive computers has made possible widespread access to high quality cryptography.

In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically. In China, a license is still required to use cryptography. Many countries have tight restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Russia, Singapore, Tunisia, Venezuela, and Vietnam. In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography. One particularly important

issue has been the export of cryptography and cryptographic software and hardware. Because of the importance of cryptanalysis in World War II and an expectation that cryptography would continue to be important for national security, many western governments have, at some point, strictly regulated export of cryptography. After World War II, it was illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was classified as a munition, like tanks and nuclear weapons. Until the advent of the personal computer and the Internet, this was not especially problematic. Good cryptography is indistinguishable from bad cryptography for nearly all users, and in any case, most of the cryptographic techniques generally available were slow and error prone whether good or bad. However, as the Internet grew and computers became more widely

available, high quality encryption techniques became well-known around the globe. As a result, export controls came to be seen to be an impediment to commerce and to research.

III.DESCRIPTION OF AES ALGORITHM

Advanced Encryption Standards (AES) is developed by two Belgian Cryptographers Vincent Rijmen and Joan Daemen. The Rijndael algorithm is selected for Advanced Encryption Standard over Data encryption standard [2], and was published by NIST-National Institute of Standards and Technology as FIPS PUB 197, in November 2001 [3]. The AES handles 128-bit block of data with variable length of the key size 128, 192, 256 bits. The number of rounds depends on the selection of key size i.e. 10, 12 or 14 rounds for key size 128, 192 and 256 bits, respectively. These bytes arranged in a 4x4 matrix. Substitute byte, Shift row, Mix-column and Add round key are major steps in AES encryption.

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

Figure 1: State-matrix arrangement for input text

A. Encryption Process

1) Byte substitution (SubBytes): This is a byte-by-byte substitution process. This processes substitution of bytes. The substitution byte for each input byte is found by using the S-Box lookup table. The size of the lookup table is 16×16. To find the substitute byte for a given input byte, we divide the input byte into two 4-bit patterns, each yielding an integer value between 0 and 15 which can represent these by hex values 0 through F. One of the hex values is used as a row index and the other as a column index for reaching into the 16×16 lookup table. The goal of the substitution step is to reduce the correlation between the input bits and the output bits.

2) Row-wise Permutation (Shift Rows): The Row-wise permutation transformation consists of (i) not shifting the first row of the state array at all (ii) circularly shifting the second row by one byte to the left (iii) circularly shifting the third row by two bytes to the left and (iv) circularly shifting the last row by three bytes to the left.

3) Column-wise mixing (Mix Column): This step replaces each byte of a column by a function of all the bytes in the same column. For the bytes in the first row of the state, operation can be stated as

$$S'0,c = (\{02\} \bullet S0,c) + (\{03\} \bullet S1,c) + S2,c + S3,c \quad (1)$$

For the bytes in the second row of the state can be stated as

$$S'1,c = S0,c + (\{02\} \bullet S1,c) + (\{03\} \bullet S2,c) + S3,c \quad (2)$$

For the bytes in the third row of the state can be stated as

$$S'2,c = S0,c + S1,c + (\{02\} \bullet S2,c) + (\{03\} \bullet S3,c) \quad (3)$$

And for the bytes in the fourth row of the state array can be stated as

$$S'3,c = (\{03\} \bullet S0,c) + S1,c + S2,c + (\{02\} \bullet S3,c) \quad (4)$$

A row of the leftmost matrix multiples a column of the state array matrix, additions involved are meant to be XOR operation.

4) Addition of round key: The key words are generated by key expansion process. Round Key is added to every State bya XOR operation where each Round Key consists of Nb words. Those Nb words are each added into the columns of the State, such that are the key schedule words and round is a value in the range 0 round Nr. In the Cipher, the initial Round Key addition occurs when round = 0, prior to the first application of the round function. Add Round Key transformation to the Nr rounds of the Cipher occurs when 1<round<Nr.

B. Decryption process :

Decryption is just the reverse operation of encryption that is cipher text which converted into plain text format. Inverse Substitute byte, Inverse shift row, Inverse Mix-column and Inverse Add round key are steps in AES decryption.

a) Inverse Sub Bytes Transformation: Each byte in a state matrix replaced with Inverse S-box table values. The Inverse S-box table contains 256 elements.

b) Inverse Shift Rows Transformation: In Inverse Shift Rows transformation, the rows of state matrix cyclically do right shift. Row 0 is kept as it is; Row1 is one byte shifted to right; Row 2 is two bytes shifted to right; Row 3 is three bytes shifted to right.

c) Inverse Mix Columns Transformation: Inverse mix column is just the inverse of the transformed Mix Columns. This transformation operates on the state matrix Column by column and each column is treated as a four term Polynomial.

d) Inverse Add Round Key Transformation: The round keys should select in a reverse order and combined with each byte of state matrix using inverse of XOR operation.

IV. PROPOSED SYSTEM

AES cipher is operating on data blocks having the length of 128 bits with a symmetric key, which may have a length of 128, 196 or 256 bits. Operations are performed on a matrix of size 4 x 4 bytes called the state. The algorithm consists of successive steps. First, the data stored in the state array are added mod 2 with the master key by the operation Add Round Key. The next steps are rounds repeated Nr times. Each round performs 4 successive operations:

(1) substitution of bytes Sub Bytes,

(2) rows shifting Shift Rows,

(3) mixing of columns Mix Column, and

(4) Add Round Key. The number of rounds Nr depends on the key length;

for the 128-bit key Nr = 10. The last step performs 3 operations: Sub- Bytes, Shift Rows and Add Round Key. At each step another key generated as an extension by the procedure Key Expansion is added.

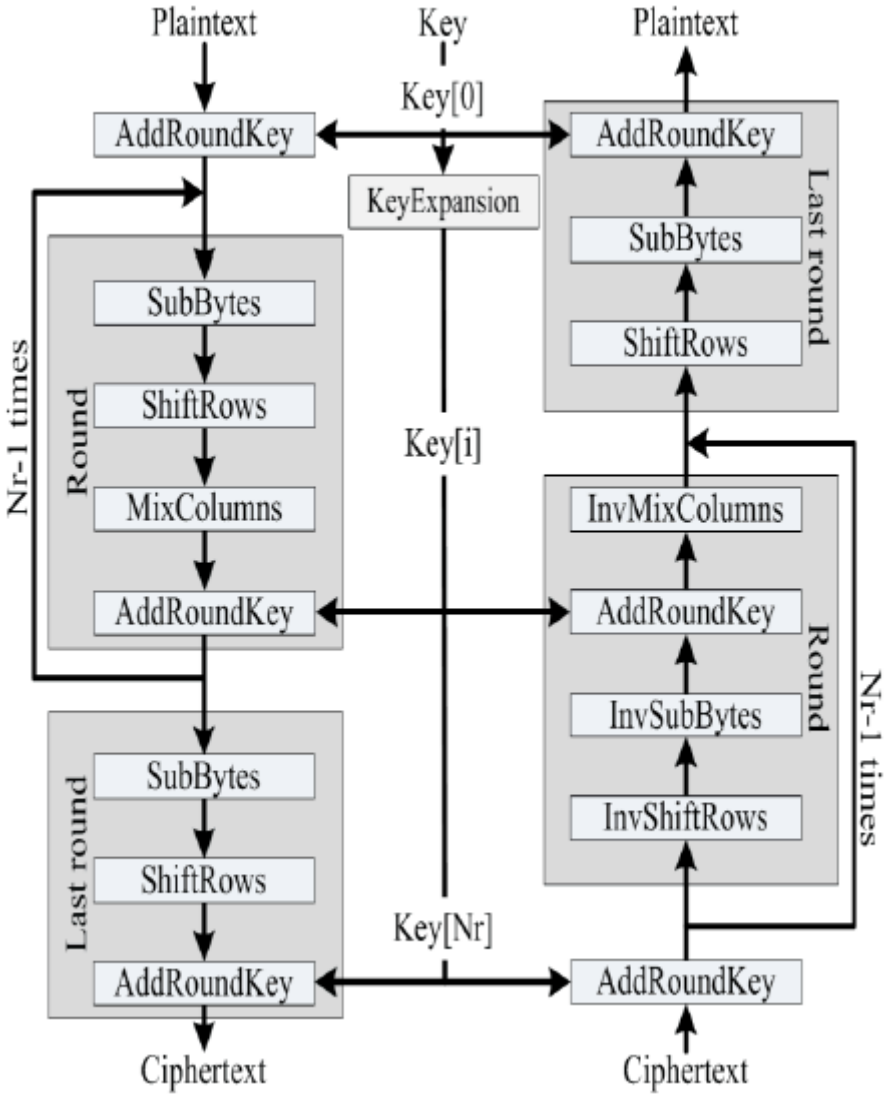

Figure 2. Block diagram of proposed system

Whereas the decryption process are relatively executing the same process as what encryption is doing except it is performing the inverse of the encryption process which are Inverse Sub bytes, Inverse Shift row, Inverse mix column and Inverse Add Round key[2]. This paper will describes both encryption and decryption process the block diagram of proposed system is shown in figure2.

V. RESULTS

The verification was done using the test vector and the expected output as described in the fips-197, Appendix B section [1]. The architecture of this AES works as expected for each process as described in Figure A. The cipher is progressed using the round key value and the input shown in Table 1, when the ready signal is high the data is fully encrypted, i.e. the output/data_out as shown in Figure 3.the decryption data data_out is shown in Fig 4

Table -1: Example test vector

Key	2b7e151628aed2a6abf7158809cf4f3c
Plain text	6bc1bee22e409f96e93d7e117393172a
Cipher text	3ad77bb40d7a3660a89ecaf32466ef97

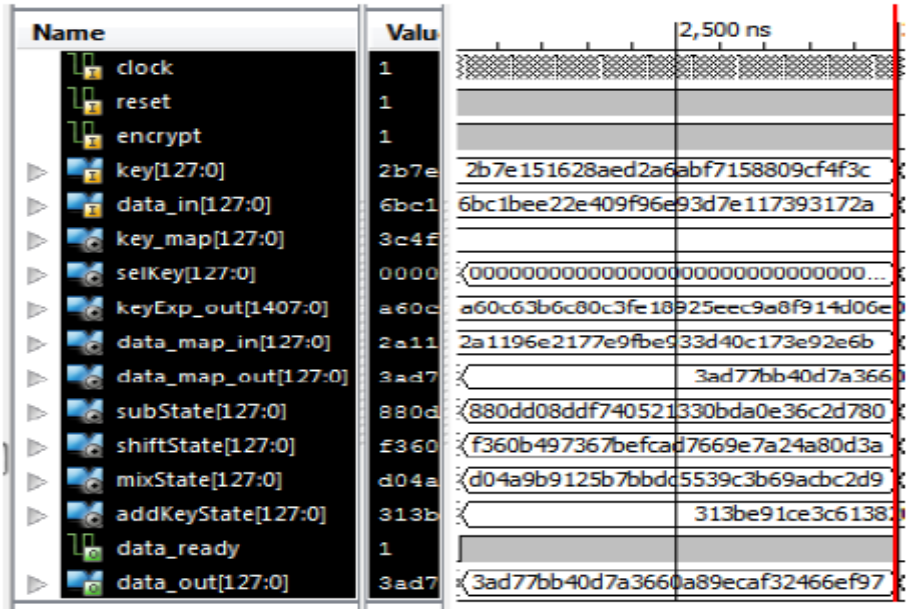

Fig 3. Encryption simulation waveforms

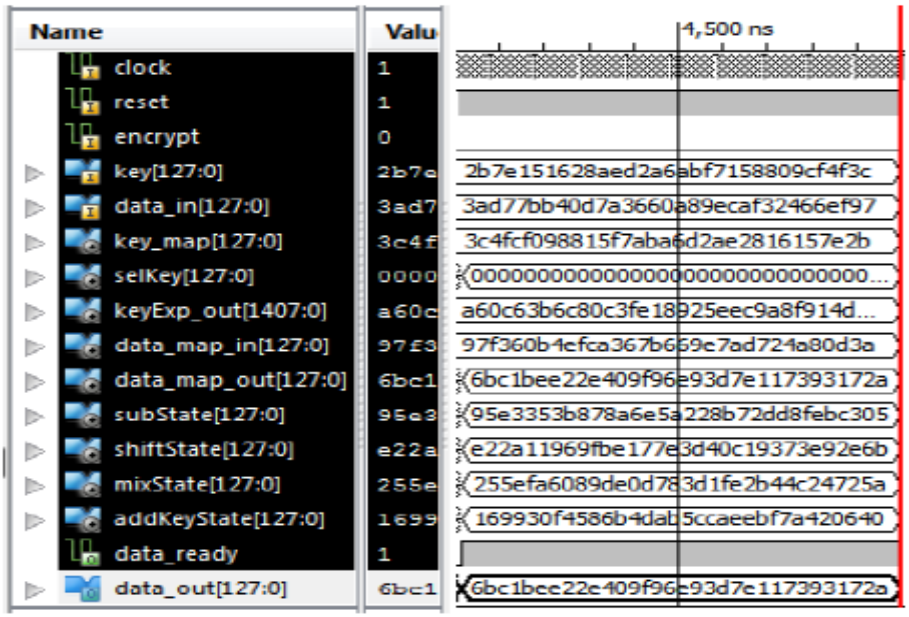

Fig 4. Decryption simulation waveforms

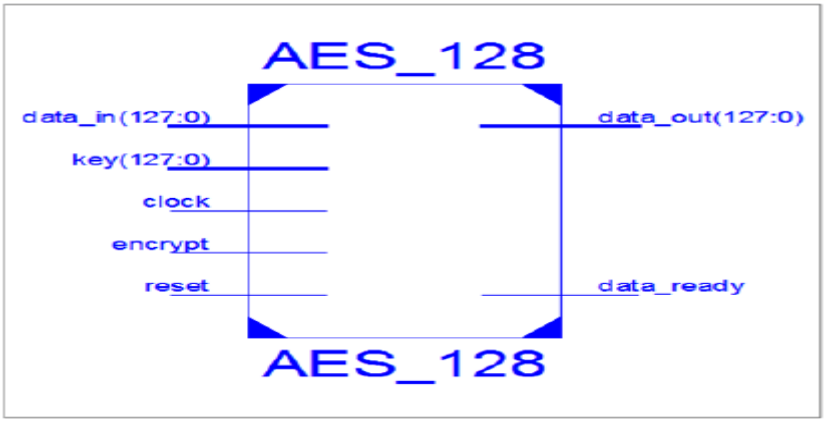

Fig 5. RTL Schematic of AES

VI.CONCLUSION

An implementation of 128 bit AES algorithm in hardware is discussed in the paper. The cipher has been synthesized using Xilinx 13.4, simulated using ISim .87xd and result is verified using standard test vectors .the algorithm is implemented by Verilog HDL. Implementation of AES algorithm in hardware is without a doubt increases efficiency of the throughput, however when it comes to hardware implementation the trade-off between area saving and high speed always needs to be compromised.

REFERENCES

[1] William Stalling, Cryptography and Network Security Principles and Practices‖ , Prentice Hall, sixth edition, 2013.

[2] Data Encryption Standard (DES), FIPS PUB 46-3, October 1999.

[3] National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.Advanced Encryption Standard (AES) (FIPS PUB 197).

[4] S. M. Umar Talha, Mir Asif, Hammad Hussain, Ali Asghar, Hadi Ameen. Efficient Advance Encryption Standard (AES) Implementation on FPGA Using Xilinx System Generator, 978-1-5090-0845-2/16[IEEE]

[5] Sumedh H. Nagdeve, Ujwala S. Ghodeswar Synthesis of Advanced Encryption Standards using Xilinx 13.4, IEEE ICCSP 2015 conference, 978-1-4799-8081-9/15[IEEE], pp.1204-1208

[6] D. Rahul Gandh, V. Kamalakannan, R. Balamurugan, S. Tamilselvan ―FPGA Implementation of Enhanced Key Expansion Algorithm for Advanced Encryption Standard, International Conference on Contemporary Computing and Informatics [2014], 978-1-4799-6629-5/14/[IEEE], pp.409- 413

[7] A. E. Rohiem, S. Elagooz and H. Dahshan, A Novel Approach for Designing the S-Box of Advanced Encryption Standard Algorithm (AES) Using Chaotic Map, ‖ in Proc. Twenty second National Radio Science Conference, 2005, pp. 455-464

[8] K. Sakamura, W.X. Dong and H. Ishikawa, A Study on Linear Cryptanalysis of AES Cipher, ‖ J. Faculty of Environmental Science and Technology, vol 9, no. 1, Feb 2004, pp. 19-26

[9] K. J. Jegadish Kumar, V. Karthick, AES S-Box Construction using One Dimensional Cellular Automata Rules, || Int. J. Computer Applications (IJCA), vol. 110, no. 12, Jan 2015, pp. 35-39

[10] M. Szaban and F. Seredynski, Dynamic Cellular Automata- Based S-Boxes, || in Proc. Computer Aided Systems Theory- EUROCAST '11, Springer-Verlag, 2012, pp. 184-19.

[11] NIST, Advanced Encryption Standard (AES), (FIP PUB 197) http://csrc.nist.gov/publications

[12] Rozita Borhan, Raja Mohd Fuad Tengku Aziz,"Successful Implementation of AES Algorithm in Hardware" 2012 IEEE International conference on Electronics Design, system and application(ICEDSA)

[13] William Stallings "Cryptography and network Security" Principles and practise Fourth Edition

[14] Morris Dworkin, "Recommendation for n BlockCipher Modes of Operation" Methods and Techniques. NIST Special Publication 800-38A 2001 Edition

Ch.Janardana pursuing his M.Tech in the department of Electronics and Communication Engineering (VLSI), Sri Venkateswara College of Engineering & Technology, Etcherla, Srikakulam, A.P., India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. He obtained his B.Tech(ECE) from Akula Gopayya College of Engineering, West godavari.

K. Govinda Rao working as Assistant Professor, in the Department of Electronics and Communication Engineering(VLSI), Sri Venkateswara College of Engineering & Technology, Etcherla, Srikakulam. He obtained his M.Tech from Gokul Institute of Technology and Sciences.