International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

Study of Clock Synchronized Hybrid Cryptographic Algorithm

Abhishek Singh[1], Jaishri Tiwari[2]
[1]*Asst. Professor, Electronics and Communication, GGITS Jabalpur*
[2]*Research Scholar (Embedded System & VLSI Design), GGITS Jabalpur*

***Abstract*— This paper discusses a new technique of cryptography which combines the DES and AES algorithm and also synchronize the key generation with this hybrid algorithm. The term cryptography represents the combination of encryption and decryption .In encryption the plain data converted into cipher with the help of key, this cipher is a unintelligible data which is converted into plain data in decryption process. In this hybrid cryptographic algorithm every DES round have one AES round. This algorithm has reinforced the previous standards and the clocked synchronization gives us highly secure algorithm. Therefore this encryption algorithm provides side channel attack protection. Its mean it secure the data from crack ,when both data and crack are running on the same server. In this algorithm 256 bit block cipher is encrypted with 128 bit key in 10 round .In every round the key generation and algorithm are synchronizes with same clock. This design has been implemented in Xilinx ISE Design Suite 12.1 platform using verilog.**

***Keywords*—AES, Block Cipher ,CHEA , Cipher, DES, FPGA, Key, Data Security, Verilog, Xilinx ISE Design Suite.**

I. INTRODUCTION

DES and AES are cryptographic algorithm . DES was introduced in early 1970s as a cryptographic algorithm for data protection . A DES algorithm have 64 binary bit of which 56 bits are randomly generated and used directly by algorithm as the key . It can be broken easily in few hours. For overcome the weakness of DES National Institute of Standards and Technology (NIST) introduced AES algorithm. In AES algorithm single key is used for encryption and decryption same as DES .But the algorithm of AES is more complex than DES. AES algorithm is capable of using cryptographic keys of 128,192 1nd 256 to encrypt and decrypt data of 128 bit.According to the research AES is not secure if crack and code both are running in same server .In other word AES algorithm is not secure from side channel attack.

In this paper , a Hybrid algorithm is proposed for data security , which has a unique feature of that only one register is used for storing the different keys for particular round .In AES standard before and after 10th round the power consumption of the circuit is changed.

Because the already stored in register so it is easy decrypt the information . But in this Hybrid cryptographic algorithm the key and the data both are generated at same clock. By which the data is protected by side channel attack .

II. HYBRID CRYPTOGRAPHIC ALGORITHM

A. *HYBRID ENCRYPTION*

The basic model of proposed algorithm is used for 256 bit data with 128 bit key . It integrates the AES in each round of DES . As shown in fig. II.

Mathematical Function :-

$$L_n = R_{n-1}$$
$$R_n' = (L_{n-1} \text{ XOR } R_{n-1} \text{ XOR } K_n)$$
$$R_n = \text{AES}(R_n' \text{ with } K_{n+1})$$

In first round of CHEA 256 bit input plain data is split into two halves of 128 bit ,the left and the right half . The next left is equal to previous right half and next right is generated after two operations .

(I) XOR operation between L_{n-1}, R_{n-1}, K_n (II) Perform n round of AES algorithm with K_{n+1} key (next key). CHEA has 10 rounds which are same as AES but in this algorithm the key generation and encryption rounds are synchronised with clock .Key is generated at particular time of instant when encryption requires. It do not use mixed Column in last round same as AES.

B. *Hybrid Decryption*

Decryption algorithm is same as encryption algorithm but in this the key is in reverse order . In first round 256 bit cipher data splits in two halves left and right 128 bit data. Next left half is equal to previous right half and next right half is generated after the operation . In first round mixed column operation is not perform ,after first round it follows the same algorithm as encryption but the key is in reverse order. As shown in fig.II

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

C. Key Generation

Key generation algorithm is same as AES algorithm. But in this algorithm generation of particular key is synchronized with particular round of hybrid encryption and decryption. In this algorithm both encryption and decryption use same key but the synchronization of generation of key with algorithm is different .

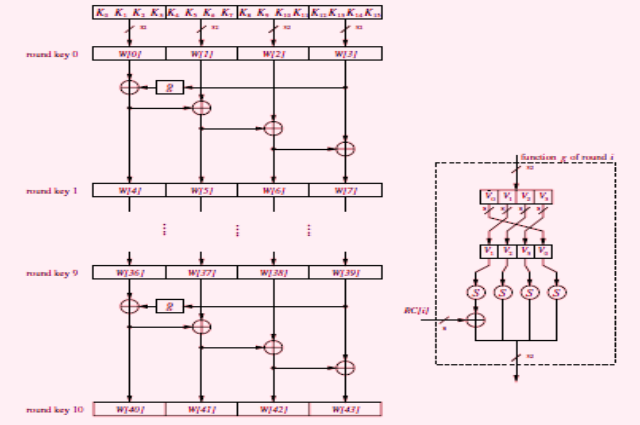


fig. I Synchronized Key Generation Algorithm [5]

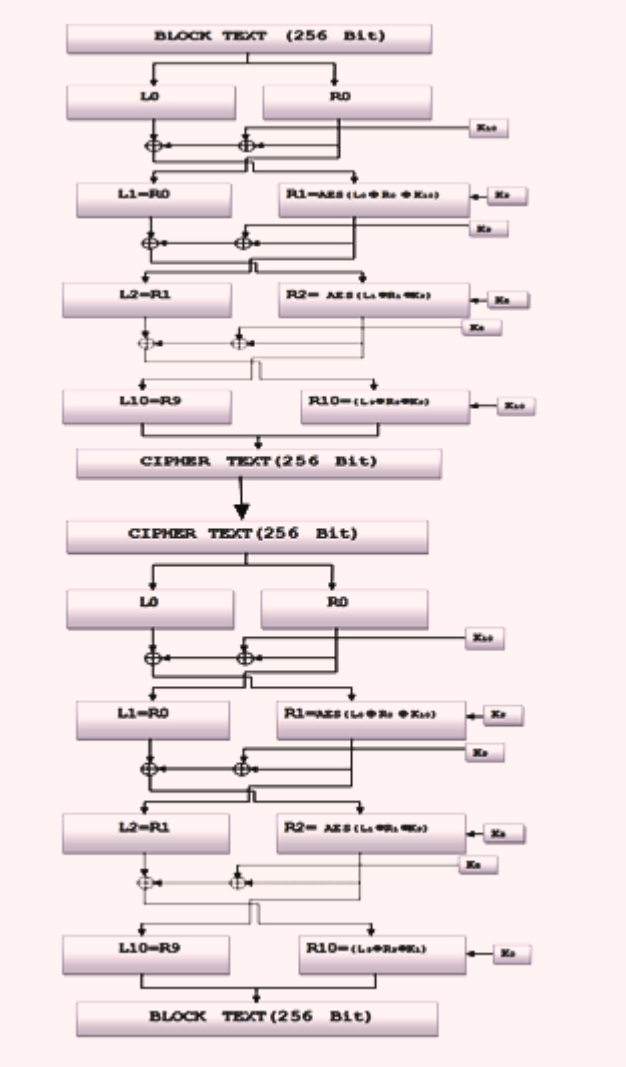
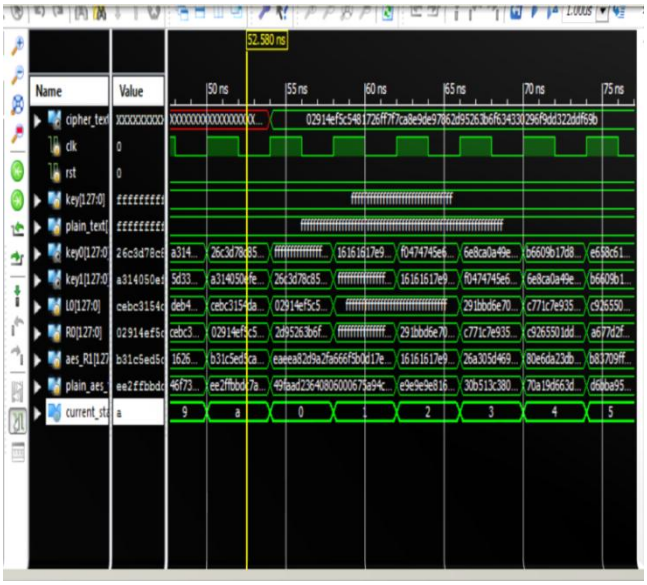


fig. II Hybrid Cryptographic Algorithm

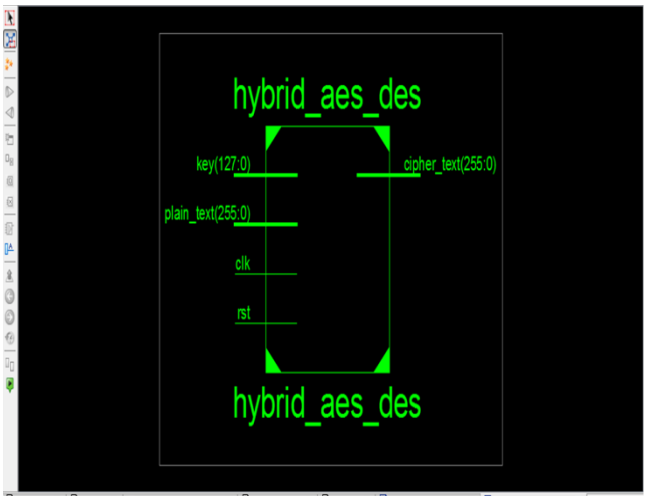
International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

III. Simulation

After detail study of AES and DES write the program in verilog for CHEA and Key generation . The coding of CHEA calls the key function for every round . Xilinx ISE Design Suite 12.1 platform used for simulation and implementation .



IV. Implementation



V. Result

With this concept of cryptography we can generated a highly secure code in which the key pattern changed with clock and this same clock process the encryption and decryption algorithm .

VI. Future Scope

Clocked Synchronized Hybrid Cryptographic Algorithm will be more secure if the no. of rounds will increased. The no of rounds can be increased and decreased according to the security purpose. We can also improve the security with increase the key length.

VII. Conclusion

This paper introduces a side channel attack proof algorithm for data security . CHE Algorithm can be used in various applications where security is primary importance.

References

[1] M.Pitchaiah, Philemon Deniel , Praveen 2012 "Implementation Of Advanced Encryption Algorithm" International Journal Of Scientific & Engineering Research ISSN 2229-5518.

[2] Behrouz A. Forouzan , "Cryptography and Network Security" TMH.

[3] Data Encryption Standard (DES) ,Federal Information Processing Standards Publication (FIPS PUB 46-3)Reaffirmed 1999oct 25

[4] Advanced Encryption Standard , Federal Information Processing Standard Publication 197 Nov 26 2001

[5] Christof Paar.Jan Pelzl "Understanding Cryptography" Springer

[6] Gireesh Kumar P. ,P. Mahesh Kumar 2013 "Implementation Of AES Algorithm Using Verilig " International Journal of Embedded systems ISSN 2249-6556.

[7] Kenekayoro Patrick T. 2010. "The data encryption standard thirty four years cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems .

[8] B.Sujitha , Dr.B.Karthikeyan 2014 "Study, Simulation and Analysis of AES Algorithm" IJIRSET ISO 3249:2007, International conference on engineering technology and science 14.

[9] William Stallings Fifth Edition "Cryptography And Network Security " Pearson Publication

[10] M. Natheera Banu April 2014 "FPGA Based Hardware Implementation Of Encryption Algorithm" IJEAT ISSN :2249-8958.

[11] Douglas Selent 2010"Advanced Encryption Standard" Rivier Academic Journal Vol. 6 Nov. 2 Fall 2010.

[12] http://www.xilinx.com

[13] Wikipedia