Data Security with CHEA (Clocked Hybrid Encryption Algorithm)

Jaishri Tiwari

M.Tech (Embedded System & VLSI Design) GGITS Jabalpur

Abstract— In this era of communication Data Security is primary concern. This paper introduce the concept of Clocked Hybrid Encryption .The term clocked hybrid represent DES & AES hybrid algorithm which is synchronized with key. In this algorithm every DES round have one AES round. This hybrid 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 .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.

I. INTRODUCTION

DES was introduced in early 1970s as a cryptographic algorithm for data protection .DES algorithm have 56 bit key length which 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. 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 ,CHE algorithm is proposed for data security. A unique feature of this algorithm is 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 Clocked Hybrid Encryption Standard algorithm the key and the data both are generated at same time which can prevent the information from side channel attack.

II. CLOCKED HYBRID ENCRYPTION

The basic model of proposed algorithm is to integrate AES into each round of DES. As shown in fig. I.

Mathematical Function :-

\[ Ln = Rn-1 \]
\[ Rn = (Ln\text{-}1 \text{ XOR} Rn \text{-}1 \text{ XOR} Kn) \]
\[ Rn = AES ( Rn' \text{ with } Kn+1) \]

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.

III. CLOCKED 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
IV. 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.

V. IMPLEMENTATION
VI. RESULT

Clocked Hybrid Encryption 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.

VII. FUTURE SCOPE

VIII. 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