Indonesian Journal of Electrical Engineering and Computer Science
Vol. 8, No. 3, December 2017, pp. 709 ~ 711
DOI: 10.11591/ijeecs.v8.i3.pp709-711

RTL Modelling for the Cipher Block Chaining Mode (CBC) for Data Security

Meenakshi RK*, A Arivazhagan
AMET University, Chennai

The demand of satellite communication, the security algorithms are to be designed in the board. The information from the satellite to the ground is required the data security with the cryptographic algorithms. Advanced encryption standard (AES) is one of the promising cryptographic algorithms for the terrestrial communication. In this paper, the encryption and decryption is mainly focused on the cipher block chaining (CBC) mode for achieving the high secured data transmission. For efficient data transmission, the AES algorithm is implemented by using CBC mode. The proposed work is designed by using RTL modeling and also the minimum numbers of logical elements are used for implementation.

Keywords*: Advanced Encryption Standard, Cipher block chaining, data security, Register transfer level, Data transmission*

1. Review Ofcipher Block Chaining Modes

The design is capable of maintaining throughput during key changes given a maximum of one change every 120 cycles. Another design has a throughput of 28.5 Gbps and supports key changes every cycle. The floor planning and a pipelined key expander were developed together with modifications to the mix columns and composite field implementation of Sub Bytes operation. AES secure channel of any feedback mode including cipher block chaining. Christy M A et al., [3] described the security data transmission algorithm in cryptography is advanced encryption algorithm. The pass transistor logic is used for the minimal power consumption and achieves the less number of transistor counts. Using a simple exclusive OR gate that is XOR gate pass transistor logic is used to minimize the power. The power consumption of mix column is reduced in AES. XOR gates are constructed by using six pass transistors which reduce the number of large transistor counts. The stream cipher algorithm based on modified AES block cipher concept to achieve high complexity in encryption and decryption processes. The stream cipher uses three functions, two of them are modified sub byte and one is modified mix column transformation of AES algorithm with an addition to the permutation function. Tiny blocks of sizes (2*2, 4*4, 6*6…) have been implemented in the algorithm. New cryptography algorithm with for effective data communication is discussed in [5]. Generating a digital signature based on new cryptographic scheme for user authentication and security. The new message digest algorithm is to provide high security, to transfer data by combination of digital signature algorithm and symmetric key cryptography algorithm is described in [6]. Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm is presented in [7].

Received June 29, 2017; Revised August 15, 2017; Accepted September 23, 2017

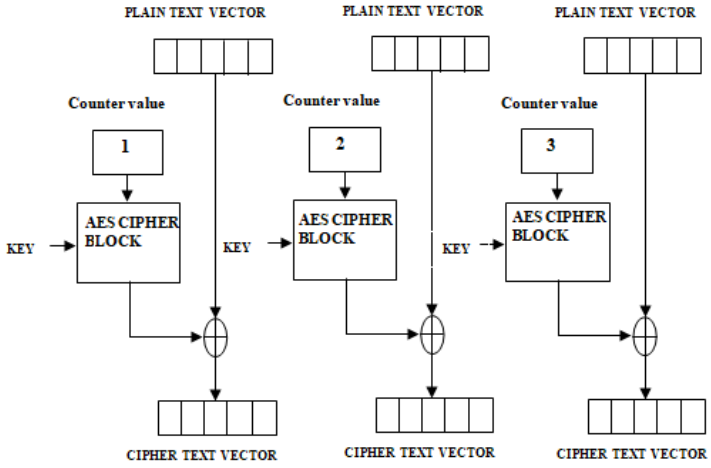

Figure 1. Cipher Block Chaining Mode Structure

2. Simulation Results

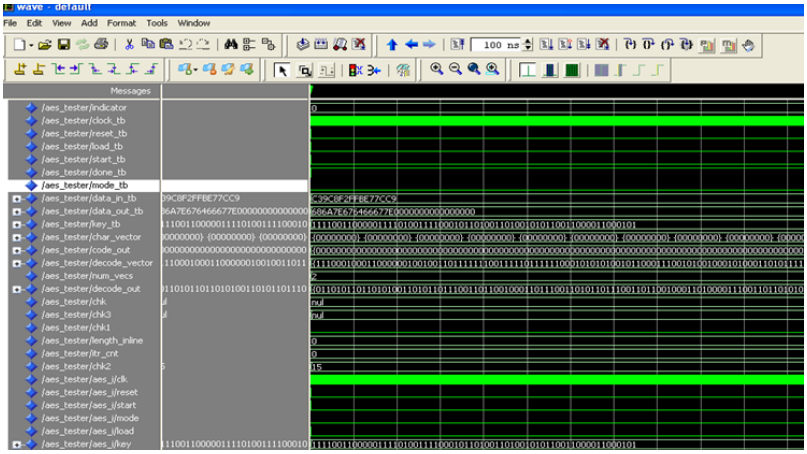

Figure 2. Simulation Result for the Encryption

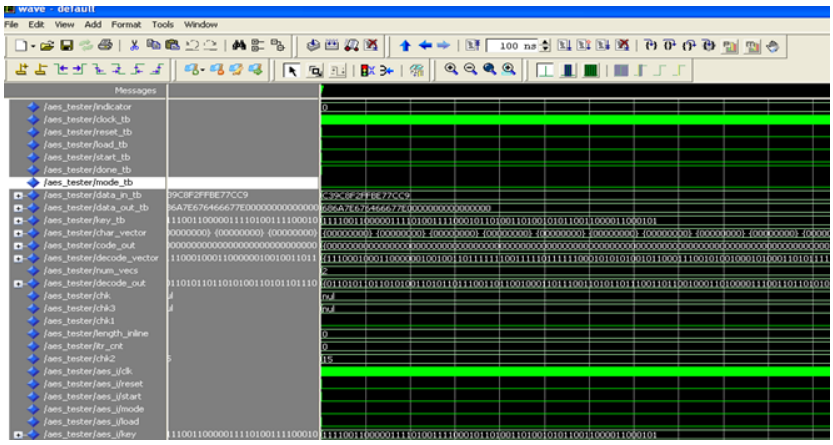

Figure 3. Simulation Result for the Decryption

3. Synthesis Results Analysis

In order to achieve the high secured data transmission, the Cipher block chaining mode is to be implemented instead of the counter mode. By using counter mode is increasing the LUT counts and the power utilizations. The CBC mode is implemented in the encryption and decryption to achieve the high efficiency level in terms of VLSI design environment. The synthesis results are carried out by using the Xilinx ISE design suite.

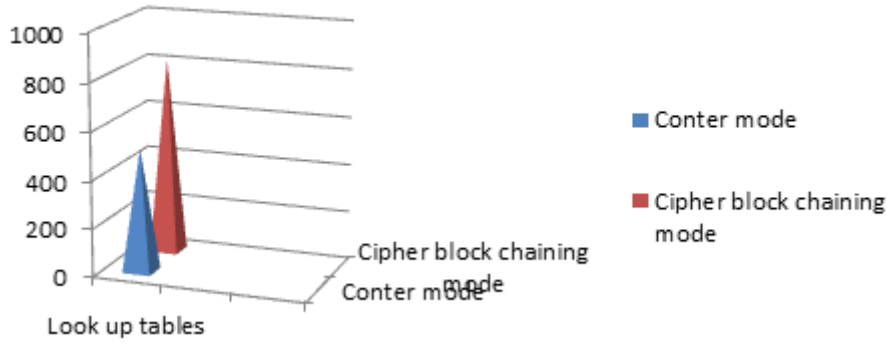

Figure 4. Synthesis results for the Look-Up-Tables utilizations

4. Conclusion

The proposed Cipher block chaining (CBC) mode based encryption and decryption is improving the area utilizations compare than the traditional method. The proposed work is designed by using Verilog HDL language. The simulation is evaluated by suing the ModelSim XE and the synthesis results are generated by using the Xilinx ISE.

References

[1] High Speed Low Cost Implementation of Advanced Encryption Standard on FPGA. *International Journal of Electronics & Telecommunication and Instrumentation Engineering (IJETIE)*. 2010.
[2] Scalable 128-bit AES-CM Crypto-Core Reconfigurable Implementation for Secure Communications. *IEEE conference* on 2010.
[3] Implementation and Performance Analysis ofAES-128 CBCalgorithmin WSNs. Hyeopgeon Lee, Kyounghwa Lee, Yongtae Shin Departmentof Computingt, Soongsil University, Korea.
[4] High-Speed VLSI Architectures for the AES Algorithm. *EEE Transactions on Very Large Scale Integration (VLSI) Systems.* 2004; 12(9).
[5] GaneshKumar K, Arivazhagan D. New cryptography algorithm with for effective data communication. *Indian Journal of Science and Technology*. 2016; 9(48): 108970.
[6] Ganeshkumar K and Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. *Indian Journal of Science and Technology*. 2014; 7(S6): 1-5.
[7] Vennila G, Arivazhagan D & Manickasankari N. Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm. *International Journal of Engineering and Technology (IJET).* 2014; 6(5): 2401.