IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

VLSI Implementation of AES Algorithm in Cryptography Developed in Xilinx

Mrs. M. Saritha[1], Ranjith. S[2], Vishvanth. R[3], Vijay. R[4]
Assistant Professor, Department of Electronics and Communication Engineering[1]
Students, Department of Electronics and Communication Engineering[2,3,4]
Dhanalakshmi Srinivasan Engineering College (Autonomous), Preambular, India
sarithamani91@gmail.com[1] and ranjith1704s@gmail.com[2], vasanthvishvanth33@gmail.com[3], vijaysparrow12@gmail.com[4]

Abstract: *In the present era of information processing through computers and access to private information over the internet like bank account information, even the transaction of money, and business deals through video conferencing, encryption of the messages in various forms has become inevitable. There are mainly two types of encryption algorithms, a private key (also called a symmetric key having a single key for encryption and decryption) and a public key(a separate key for encryption and decryption). In terms of computational complexity, a private key algorithm is less complex than a public key algorithm. The simple architecture of the private key algorithm attracts the VLSI implementation through the basic digital components like basic gates and flip-flops. Moreover, the high throughput architecture can be realized for the encryption of very large amounts of data, e.g., images and videos, in real-time. The National Institute of Standards and Technology (NIST) adopted Advanced Encryption Standard (AES) as the standard for the encryption and decryption of blocks of data. The draft is published under the name FIPS-197 (Federal Information Processing Standard number 197). AES is an asymmetric key block cipher. It encrypts data of block size 128 bits. The AES algorithm is used in diverse application fields like WWW servers, automated teller machines (ATMs), cellular phones, and digital video recorders.*

Keywords: VLSI

REFERENCES

[1]. B.A. Forouzan and D. Mukhopadhyay, Cryptography and Network Security,2nd Ed., Tata Mc Graw Hill, New Delhi, 2012.
[2]. M. I. Soliman, G. Y. Abozaid, "FPGA implementation and performance evaluation of a high throughput crypto coprocessor," Journal *of Parallel and Distributed Computing*, Vol.71 (8), pp.1075-1084, Aug.2011.
[3]. V. K. Pachghare, Cryptography, and information security, E. E. Ed., PHI Learning, New Delhi,2009.
[4]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields," *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems*, Vol. 19(1), pp.85-91, Jan.2011.
[5]. Federal Information Processing Standards Publication 197 (FIPS197), available online, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[6]. X. Zhang, K. K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm," IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, Vol. 12 (9), pp.957-967, Sep.2004.
[7]. M. Jridi and A. AlFalou, "A VLSI implementation of a new simultaneous images compression and encryption method,"2010 IEEE International Conference on Imaging Systems and Techniques (IST), pp.75-79, July 2010.
[8]. Chih-PinSu, Tsung-FuLin, ChihTsunHuang, and Cheng-WenWu, "A High-Throughput Low-Cost AES Processor," IEEE Communications Magazine, Vol.41(12), pp.86-91, Dec.2003.
[9]. L.Ali, I.Aris, F. S. Hossain and. Roy, "Design of an ultra-high speed AES processor for next-generation IT security," Computers and Electrical Engineering, Vol.37(6), pp.1160-1170, Nov.2011.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

[10]. K.H. Chang, Y.C. Chen, C. C. Hsieh, C. W. Huang, and C. J. Chang, "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application," IEEE International Symposium on Circuits and Systems, pp.1922-1925, May 2009.