2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-7024-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCCNT61001.2024.10724160

Area-Efficient VLSI Architecture for Advanced Encryption Standard

1st Anbumani V
Electronics and Communication Engineering
Kongu Engineering College
perundurai,Erode
anbumanivenkat@gmail.com

2nd Vikram N
Electronics and Communication Engineering
Sona College of Technology Salem
vikram.malliga@gmail.com

3rd R. RajaRaja
Electronics and Communication Engineering
PSG Institute of Technology and Applied Research
Neelambur,Coimbatore
rajaraja@psgitech.ac.in

4 th Sanjeev G P
Electronics and Communication Engineering
kongu Engineering College
perundurai,Erode
sanjeevgp.20ece@kongu.edu

5th Varunesh M J
Electronics and Communication Engineering
Kongu Engineering College
perundurai,Erode
varuneshmj.20ece@kongu.edu

6th Suhas D K
Electronics and Communication Engineering
Kongu Engineering College
perundurai,Erode
suhasdk.20ece@kongu.edu

***Abstract* — This paper describes an area-efficient AES design method that takes into account the implementation features of application-specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) . The majority of the AES hardware area is occupied by Sub bytes and MixColumns, hence this paper concentrates on optimizing and assessing their design approach. This short examines the trade-off connection between area and clock cycles based on data channel changes and proposes an area-efficient AES intellectual property (IP) design. This paper provides a 128-bit AES design based on text data cryptography. Verilog HDL program is used for implement the design, in addition to that Modelsim is used here to simulate the results. With the help of Synthesis Process of the Xilinx is used for measuring the performance. This work provides a 128-bit AES design based on text data cryptography. The designed architecture has been implemented in FPGA -XC3S 200 TQ-144 using Verilog HDL.**

Keywords— AES, FPGA, ASIC, IP, HDL

I. INTRODUCTION

The procedure of developing and utilizing a cryptosystem or cipher to keep the information or application encrypted unreadable or usable by anybody other than the intended receiver or recipients is known as cryptography, sometimes abbreviated as encryption. A message can be encoded using a technique called a cryptosystem. Only after decoding the encrypted message using the appropriate keys and algorithm can the recipient see it. Sensitive information is mainly communicated over computer networks using cryptography [1]. An encrypted document is one that has been created by applying a mathematical method and a key to a clear-text document. When a document is encrypted with crypto-text, it cannot be read by anyone without the key to decrypt it.

A substitute for the Data Encryption Standard (DES) was sought after by the US government's National Institute of Standards and Technology (NIST) in 1997. The prevailing consensus was that DES was insecure due to the advancements in computer processing power. NIST set out to define a substitute to DES that US government agencies may suited for non-military based communication security applications. Naturally, it was acknowledged that NIST's work would be advantageous to commercial and other nongovernment users and that the results would eventually be widely embraced as industry standards. Experts in data security and cryptography from all around the world were asked by the NIST to take part in the selection and discussion process. For this paper, five encryption techniques were chosen. The encryption technique put out by Belgian cryptographers Joan Daeman and Vincent Rijmen was chosen through a consensus-building procedure. Daeman and Rijnmen called the algorithm Pipelined, which was a combination of their names, prior to selection [2].

Upon its implementation, the encryption technique became known as Advanced Encryption Standard (AES) and it is still widely used today. The AES encryption algorithm was officially adopted by the NIST in 2000 and it was then published as a federal standard with the name FIPS-197. The NIST website has the complete FIPS-197. As could be expected, a wide no of manufacturers of software and hardware for encryption have included AES-encryption in their offerings.

II. RELATED WORK

Lee et al (2023) proposed a research tackles the urgent need for an area-efficient design of the Advanced Encryption Standard (AES) by taking into account the implementation

strengthened. In order to achieve high throughput and efficiency, it is crucial to reduce the design delay by combining and swapping AES operations, optimize the Sub-Bytes using Mix-Columns and shorten the composite field arithmetic's critical path. An almost similar delay between various sub-pipeline stages has been made in an effort to achieve the low delay and high frequency of the design.

REFERENCES

[1]. K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2]. D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[3]. M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security and utility in medical devices?" in Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom., May/Jun. 2013, pp. 1–6.

[4]. M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[5]. H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[6]. M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in Proc. 26th Int. Conf. VLSI Design,Jan.2013,pp.203–208

[7]. Kim H. K, Sunwoo M.H. (2019),' Low Power AES Using 8-Bit and 32-Bit Datapath Optimization for Small Internet-of-Things', Journal of Signal Processing Systems, Vol. 91, No. 11, pp.1283–1289.

[8]. Kaps P. and Sunar B. (2006), 'Energy comparison of AES and SHA- 1 for ubiquitous computing', International Conference on Embedded Ubiquitous Computers, Vol. 23, pp. 372–381.

[9]. Lee U. and Kim H. K. (2023), 'Area-Efficient Intellectual Property Design of Advanced Encryption Standard', IEEE Transactions on Circuits and Systems II, Vol. 70, No. 10, pp. 3797-3801.

[10]. Liu Z. and Grossschadl J. (2018), 'Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography', IEEE Communications Magazine, Vol. 56, No. 2, pp. 158-162.

[11] Masoumi M. (2012), 'Differential power analysis: a serious threat for FPGA security', International Journal of Internet Technology and Secured Transactions, Vol.4, No.1, pp. 12-25.

[12]. Mathew S. (2015), 'NanoAES hardware accelerator with area-optimized Encrypt and Decrypt in 22 nm tri-gate CMOS', IEEE Journal on Solid-State Circuits, Vol. 50, No. 4, pp. 1048–1058.