Efficient FPGA Implementation And Comprehensive Parameter Analysis of Advanced Cryptographic Techniques

Miss. Sonal S. Newaskar[1], Dr. Komal P. Kanojia[2], Dr. Bharti Chourasia[3]
[1]Dept of Electronics & Communication Engineering
[2, 3]Professor, Dept of Electronics & Communication Engineering
[1, 2, 3] SRK University, Bhopal, M.P., India

Abstract- *With the emergence of 5G, Internet of Things (IoT) has become a center of attraction for almost all industries due to its wide range of applications from various domains. The explosive growth of industrial control processes and the industrial IoT, imposes unprecedented vulnerability to cyber threats in critical infrastructure through the interconnected systems. This new security threats could be minimized by lightweight cryptography, a sub-branch of cryptography, especially derived for resource-constrained devices such as RFID tags, smart cards, wireless sensors, etc. More than four dozens of lightweight cryptography algorithms have been proposed, designed for specific application(s). These algorithms exhibit diverse hardware and software performances in different circumstances. Security and privacy are of prime concern in the emerging technologies like internet of things (IoT) and cyber-physical systems (CPS) based applications. Lightweight cryptography plays a major role in securing the data in this emerging pervasive computing environment. The objective of this thesis is to implement High performance and Area efficient VLSI architecture and to compare the results between present Ciphers. Cipher is an algorithm for encryption and decryption operation. The IoT concept has faced severe comments with regards to privacy and data security. These technologies have attain immense popularity and widespread use; hence, there is a dire need to restrict unauthorized access of data. Here, cryptography plays an important role in preserving data integrity, confidentiality and user privacy. This research presents implementation of cryptography technique for 5G application. Simulation is performed using the Xilinx ISE 14.7 software using .the Verilog code. The Proposed method gives better result as compare to previous work.*

Keywords- FPGA, VLSI architecture, light weight cryptography, rectangle block cipher, Internet of Things (IoT), etc.

I. INTRODUCTION

Communication is an act of conveying information between entities, it allows us to share information, understand one another and live together as a community. While there is information worth forwarding and sharing to the rest of the world, for instance cute kitten pictures1, there is also sensitive information, such as medical history or even military operations, which needs to be protected from unintended parties. However, transmission of information could be easily intercepted or observed by potential adversaries; hence private communication is not guaranteed. Instead, establishing a secure communication becomes the best option for protecting the information. Cryptology is the study of secure communications between two parties in the presence of unauthorized third parties. In cryptology, a cipher is an algorithm for encrypting and decrypting data. Symmetric key encryption, also known as secret key encryption, based on the use of ciphers, which operate symmetrically. A cipher convert's data by processing the original, plaintext characters (or other data) into cipher text, which should seems to be random data. Commonly, ciphers used two main types of transformation: transposition ciphers, which keep all the original bits of data in a byte but mix their order, and substitution ciphers, which replace specific data sequences with other specific data sequences. For example, one type of substitution would be to convert all bits with a value of 1 to a value of 0, and vice versa. The data output by either of the method is called the cipher text. Modern ciphers enable private communication in many different networking protocols, including the Transport Layer. Security (TLS) protocol also offers encryption of network traffic. Many communication technologies, including phones, digital television and ATMs, depends on ciphers to maintain security and privacy.

II. LITERATURE SURVEY

This chapter provides an in-depth look at the history of lightweight cryptography. It covers the theoretical and simulation work from several different types of cryptography approaches. In this chapter, we briefly discuss some of the recent improvements in performance. The following reviews provide an in-depth analysis of the current state of cryptographic security technologies around the world.

PREVIOUS WORK DONE

Jai Gopal Pandey, AyushLaddha, Sashwat Deb Samaddar (2020), Block ciphers are one of the most fundamental building blocks for information and network security. In recent years, the need for lightweight ciphers has dramatically been increased due to their wide use in low-cost cryptosystems, wireless networks and resource-constrained embedded devices including RFIDs, sensor nodes, smart cards etc. In this paper, an efficient lightweight architecture for RECTANGLE block cipher has been proposed. The architecture is suitable for extremely hardware constrained environments and multiple platforms due to its support of bit-slice technique. The proposed architecture has been synthesized and implemented on Xilinx Virtex-5 xc5vlx110t1ff1136 field programmable gate array (FPGA) device. Implementation results have been presented and compared with the existing architectures and have shown commensurable performance. Also, an application-specific integrated circuit (ASIC) implementation of the architecture is done on SCL 180 nm CMOS technology where it consumes 2362 gate equivalent (GE).

D. Malathi, S.Suvetha, S.Shanmuganathan ,K.Vignesh 2020, : Security and privacy are of prime concern in the emerging technologies like internet of things (IoT) and cyber-physical systems (CPS) based applications. Lightweight cryptography plays a major role in securing the data in this emerging pervasive computing environment. The main objective of this project is to implement High performance and Area efficient VLSI architecture with 64-bit data path for present Cipher and to compare the results between present Ciphers. Cipher is an algorithm for encryption and decryption operation. It is based on the concept of Substitution-Permutation network. These networks contains both S-boxes and P-boxes which has specified algorithm for each that converts input bits as blocks into output bits .The block runs for 9 clock cycles to get encrypted output and also to get decrypted output. Simulations is done on Model Sim software and synthesis is on Xilinx FPGA device. It gives the throughput of around 3712 Mbps and Efficiency of around 11.56%, this architecture gives the better results when compared to existing Cipher.

III. LIGHT WEIGHT CRYPTOGRAPHY

They are also designed for other miniature technologies such as implanted medical devices, stress detectors inside roads and bridges, and keyless entry fobs for vehicles. Devices like these need “lightweight cryptography” — protection that uses the limited amount of electronic resources they possess.

In cryptography, an adversary's advantage is a measure of how successfully it can attack a cryptographic algorithm, by distinguishing it from an idealized version of that type of algorithm.

LIGHTWEIGHT CRYPTOGRAPHY USED IN 5G

Lightweight cryptography (LWC) is an area of cryptographic techniques with low computational complexity and resource requirements. There must be a reason for using it in Internet of Things (IoT) network with a strict resource constraints environment. The key features of a 5G network are low latency, high throughput, heterogeneous network architecture, and massive connectivity

IV. PROPOSED METHODOLOGY

The main contribution of the proposed research work is as followings-

- To implement the VLSI architecture of the lightweight cryptography.
- To reduce the complexity of conventional lightweight cryptography algorithm.
- To simulate using Isim simulator and check the various parameter results using test bench.
- To calculate the performance parameters and compare with existing approach.

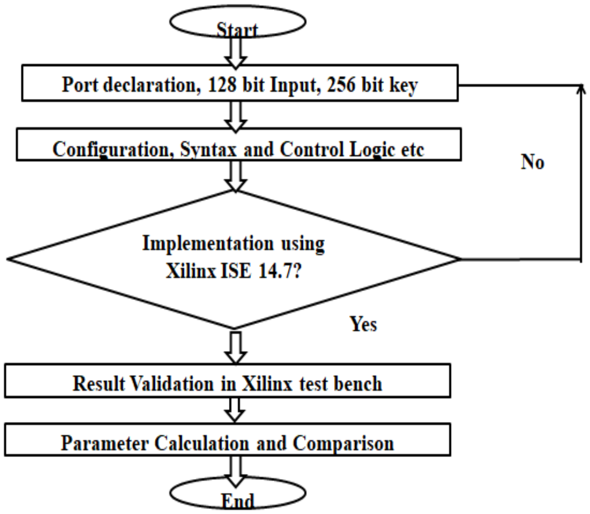
Start
Port declaration, 128 bit Input, 256 bit key
Configuration, Syntax and Control Logic etc
Implementation using Xilinx ISE 14.7?
No
Yes
Result Validation in Xilinx test bench
Parameter Calculation and Comparison
End

Figure 4.1: Flow Chart

Steps- Firstly assign the port declaration, 128 bit input and 256 bit key.

- Configuration of the system using VLSI syntax, and various control logic.
- The input byte process with the s-box or sub byte operation.
- The next step process with the shift rows operation.
- The mix columns process is applied where use XOR operation.
- At last the data value round with various numbers or it is known as add round Key operation.
- The VLSI architecture RTL view is generated after the simulation process.
- In the simulation step, the results are validated or tested with the test bench.
- The various performance parameters like latency, area, power, frequency and throughput are calculated and compare with the existing work.

V. SIMULATION AND RESULTS

5.1 SIMULATION

Xilinx ISE (Integrated Software Environment) is a software tool produced by Xilinx for synthesis and analysis of HDL designs, enabling the developer to synthesize their designs, perform timing analysis, examine RTL diagrams, simulate a design's reaction to different stimuli, and configure the target device with the programmer.

Framework level testing may be conducted utilizing ISIM or the Modalism way of reasoning test framework, and such test projects need to likewise be developed in HDL vernaculars. Test seat activities may comprise mirrored input signal waveforms, or displays which observe and confirm the yields of the contraption under test. Modalism or ISIM may be applied to play out the going with types of diversions.

5.2RESULTS

Sr No	Parameter	Value
1	Area	6213 LUT, 512 I/O box
2	Delay or Latency	43.398ns total, logic delay is 3.526ns
3	Power	0.18mW
4	Frequency	23 MHz
5	Throughput	2949 Mbps
6	Memory	4726336 kilobytes

Table 5.1: Simulation Parameters

In table 5.1, simulation parameters are showing which is taken during the execution of Xilinx Verilog script.

Sr No.	Parameters	Previous Work	Proposed Work
1	Input bit	80	128
2	Frequency	10 MHz	23 MHz
3	Area	28860.580	13017
4	Total Power	0.2535 mW	0.18mW
5	Throughput	250 Mbps	2949 Mbps
6	Delay or Latency	100 ns	43.398ns

Table 5.2: Result Comparison

Table 5.2 is representing the result comparison of the previous and the proposed work. The previous work is based on the 80 bit data input while proposed work is based on the 128 bit data input with 256 bit key so that it provide better security. The value of frequency is 23 MHz in the proposed work while 10 MHz in the previous work. The total throughput is 2949 Mbps in the proposed work while 250 Mbps in the existing and the total latency is 43.39ns in the proposed and 100ns in the previous work.

VI. CONCLUSION AND FUTURE SCOPE

CONCLUSION

Lightweight cryptography, often known as lightweight encryption, is a kind of encryption developed for resource-constrained systems. Lightweight encryption technology employs less memory, fewer computational resources, and a lesser amount of electricity to offer secure solutions for restricted resources in a network.

While AES and SHA are extremely good together at the interface of computing, they are unable to deal with an IoT context where they use extra computational resources. In recent years various lightweight, cryptographic basic devices have been created and deployed to satisfy constrained resource needs. Both worldwide and NIST organizations have defined numerous ways that are feasible for lightweight cryptography and they are suitable for IoT/RFID devices.

This dissertation provides implementation of lightweight crypto VLSI architecture for 5G-IOT application. Simulation is conducted using the Xilinx ISE 14.7 software utilizing the Verilog code. The simulation results reveals that the prior work is based on the 80 bit data input while suggested work is based on the 128 bit data input with 256 bit key so that it give higher security. The value of frequency is 23 MHz in the proposed work whereas 10 MHz in the preceding work. The overall throughput is 2949 Mbps in the proposed work whereas 250 Mbps in the existing and the total latency is 43.39ns in the proposed and 100ns in the previous work.

VII. FUTURE SCOPE

In Future we can use hybrid techniques for cryptography to improve more security using IOT application. Our work is based on the 128 bit data input with 256 bit key so that it give higher security further we can increases size of key upto 512 as data bit increases and we can send data more securely with less power.

REFERENCES

[1] Jai Gopal Pandey, AyushLaddha, Sashwat Deb Samaddar, A Lightweight VLSI Architecture for RECTANGLE Cipher and its Implementation on an FPGA, October 04,2020 at 09:08:45 UTC from IEEE Xplore

[2] D. Malathi , S.Suvetha, S.Shanmuganathan ,K.Vignesh VLSI Architecture For Cipher In 5G New Radio, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 02, FEBRUARY 2020 ISSN 2277-8616 861 IJSTR©2020 www.ijstr.org

[3] Malathi, D., S.Suvetha, S.Shanmuganathan, &K.Vignesh (2020). VLSI Architecture For Cipher In 5G New Radio. International Journal of Scientific & Technology Research, 9, 861-864.

[4] Xu, T., Wendt, J.B., &Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 417-423.

[5] Gulzar, M., & Abbas, G. (2019). Internet of Things Security: A Survey and Taxonomy. 2019 International Conference on Engineering and Emerging Technologies (ICEET), 1-6.

[6] Chandrajeet Singh and Prof. Ashish Raghuwanshi, “VLSI Implementation of Modified AES System for FPGA-IOT Application”, International Journal of Mechanical Engineering,I SSN: 0974-5823 Vol. 7 No. 4 April, 2022.

[7] AyoubMhaouch, W. Elhamzi, Mohamed Atri, Lightweight Hardware Architectures for the Piccolo Block Cipher in FPGA,Computer Science, Mathematics, 5th International Conference on Advanced,2020.

[8] Naidu, T., &Kumari, A.K. (2020). A High-Performance VLSI Architecture for the PRESENT Lightweight Cryptography. International Journal of Engineering Research and, 9.

[9] Singh, P., Acharya, B., &Chaurasiya, R.K. (2022). Low-area and high-speed hardware architectures of LBlock cipher for Internet of Things image encryption. Journal of Electronic Imaging, 31, 033012 - 033012.

[10] Kumari, M., Singh, P., & Acharya, B. (2022). Secure image encryption using high throughput architectures of PRINT cipher for radio frequency identification applications. Journal of Electronic Imaging, 31, 063036 - 063036.

[11] Mishra, Z., & Acharya, B. (2020). High throughput and low area architectures of secure IoT algorithm for medical image encryption. J. Inf. Secur. Appl., 53, 102533.

[12] J. G. Pandey, A. Laddha and S. D. Samaddar, "A Lightweight VLSI Architecture for RECTANGLE Cipher and its Implementation on an FPGA," 2020 24th International Symposium on VLSI Design and Test (VDAT), 2020, pp. 1-6, doi: 10.1109/VDAT50263.2020.9190623.

[13] P. B.S, N. K.J and N. J. C.M, "MEC S-box based PRESENT Lightweight Cipher for Enhanced Security and Throughput," 2020 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 2020, pp. 212-217, doi: 10.1109/DISCOVER50404.2020.9278038.

[14] B. Hajri, M. M. Mansour, A. Chehab and H. Aziza, "A Lightweight Reconfigurable RRAM-based PUF for Highly Secure Applications," 2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2020, pp. 1-4, doi: 10.1109/DFT50435.2020.9250829.

[15] B. Richter and A. Moradi, "Lightweight Ciphers on a 65 nm ASIC A Comparative Study on Energy

Consumption," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020, pp. 530-535, doi: 10.1109/ISVLSI49217.2020.000-2.

[16] P. Singh, B. Acharya and R. K. Chaurasiya, "Efficient VLSI Architectures of LILLIPUT Block Cipher for Resource constrained RFID Devices," 2019 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2019, pp. 1-6, doi: 10.1109/CONECCT47791.2019.9012869.

[17] R. Sadhukhan, N. Datta and D. Mukhopadhyay, "Power Efficiency of S-Boxes: From a Machine-Learning-Based Tool to a Deterministic Model," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2829- 2841, Dec. 2019, doi: 10.1109/TVLSI.2019.2925421.

[18] T. Chen, K. Hou, W. Beh and A. Wu, "Low-Complexity Compressed-Sensing-Based Watermark Cryptosystem and Circuits Implementation for Wireless Sensor Networks," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 11, pp. 2485-2497, Nov. 2019, doi: 10.1109/TVLSI.2019.2933722