A review on Crypto-Algorithm using Different Hardware

Inkee Chouhan[1], Dr. Monisha Sharma[2]

[1]M.Tech. scholar, Dept. of Electronics Communication Engineering, Shri Shankaracharya Technical Campus, Bhilai, C.G. India
[2]P.hD, Principal of Shri Shankaracharya Technical Campus, Bhilai, C.G. India

---***---

Abstract - *Cryptography is the field, which involves different algorithms utilized for anchoring information. It follows encryption strategies, which changes the plaintext (message to be transferred) into cipher content (encoded message) with the help of key. Today's hardware is used worldwide in various electronic items .Cryptography is the field, which involves different algorithms utilized for securing information. It follows encryption strategies, which changes the plaintext (message to be transferred) into cipher text (encoded message) with the help of key and decryption strategies, which changes cipher text into plaintext again. In this paper, we discuss various important algorithms used for the encryption and decryption of data in all fields, to make a study for most important algorithms in terms of data security effectiveness, key size, complexity, throughput and time, etc. This review paper focused on different types of cryptography algorithms implemented using hardware that are existing, like AES, DES, RSA, ECC, SHA-1 and RC6…etc.*

Key Words: - Cryptography, Encryption, Decryption, Hardware.

1. INTRODUCTION

Cryptology is the study of techniques for ensuring the secrecy and authenticity of information. The two main branches of the cryptology are Cryptography, which is the study of the design of such technically; and Cryptanalysis, which deals with the defeating such techniques, to recover information, or forging information that will be accepted as authentic. The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

Cryptography plays important role in information security. Many cryptographic algorithms have been proposed, such as the Advanced Encryption Standard (AES), Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), and other algorithms. Many researchers and hackers are always trying to break these algorithms using brute force and side channel attacks. Some attacks were successful as it was the cases for the Data Encryption Standard (DES), where the published cryptanalysis attack can be break the DES. Todays the Advanced Encryption Standard (AES) is one of the strongest cryptographic algorithms; therefore it was adopted by the National Institute for Standards and Technology (NIST) after the failing of the Data Encryption Standard (DES).

There are two types of encoding. These two types are the symmetric and asymmetric encoding algorithms. Several of those algorithms will be included here as: AES, DES, 3DES, E-DES, BLOW FISH, RC2, RC4 and RC6 which all have to do with bilateral algorithms. In contrast to RSA, ECC, EEE, DH, ELGAMAL ALGORITHM and DSA, are unilateral algorithm.

2. Survey on different type of Crypto-algorithm using different type of Hardware

1. **2000, Comparison of the hardware performance of the AES candidates using reconfigurable hardware**, Gaj. K et al : - In this paper, five types of AES cipher are used and comparing their results. These ciphers are two fish, RC6, serpent, mars and Rijndael. All five types cipher is implementing using Xilinx FPGA device. In which Twofish cipher is most suitable for the purpose of low cost and small area. Whereas Serpent and Rijindael both offers high speed.

2. **2004, High-speed VLSI Architectures for the AES algorithm**, Zhang. X et al : - In this paper an AES algorithm is implemented using high speed VLSI algorithm architecture. In this survey paper, also explore the advantages of sub pipeline. Moreover, fully sub-pipelined encrypts using 128 bit key implemented on FPGA devices and descriptors incorporated by Encryptor/decryptor round unit architecture, and throughput will be lower than encryptor only implementation. Furthermore reduces the number of round units in a loop.

3. **2005, successfully attacking masked AES hardware implementation**, Mangard. S et al : - In this paper, several masking schemes for AES are proposed to secure hardware implementation against DPA attacks. The Design might be susceptible to DPA attacks using simple power models. This survey paper said that the power consumption of the masked AES hardware implementation is correlated to the Hamming weight of the S-Box output.

4. **2005, Energy analysis of public key Cryptography on small wireless devices**, Arvinderpal S. Wander et al :- In this paper, key exchanged based on public key cryptography on an 8 bit microcontroller. This paper, compare two public-key algorithm RSA and ECC, and the paper concludes that ECC is better than RSA and the energy cost of public-key cryptography is minimum.

5. **2006**, **Desing and implementation of low area and low power AES encryption hardware core**, Alho. T et al : - In this paper, 8-bit AES ASIC encryption core hardware suited for devices in which low cost and low power consumption are desired. It compares previous 8-bit design and achieve higher throughput with corresponding area. It shows the distribution of area and power consumption of AES encryption core and energy consumption is low.

6. **2007, New Light-Weight Crypto Algorithms for RFID,** Poschmann A. et al :- In this paper, DESL provide more security against linear and differential cryptanalysis and the Davies-Murphy attack, more size-optimized and more power efficient than DES, So it especially suited for RFID applications. Moreover, DESL is used as an alternative for stream cipher.

7. **2007, Compact FPGA implementation of 32- bit AES algorithm using Block RAM,** Huang .c et al :-In this paper , AES implementation using BRAM feature in FPGA chip. In which AES hardware operations are shifted to BRAM and It uses 148 slice, 11 Block RAMs and gain the data stream of 647M bits per second, very low slice area and high throughput.

8. **2009, Efficient hardware realization of AES using VIRTEX-5 FPGA**, Rais MH. et al :- In this paper, a high performance and highly optimized hardware realization of Rijndael AES algorithm has been designed and implemented using Xilinx virtex-5 XC5VLX50 FPGA device. This paper calculates, speed, timing, devices utilization and throughput.

9. **2009, Efficient software implementation of Public- Key cryptography on sensor network using the MSP430X microcontroller,** Leonardo B. et al :- In this paper, ECC and PCB are presented in the MSP430 family of microcontroller. In this research paper obtained a prime field multiplication that is faster than 160 and 256- bit prime reduction. It also improves the timing of ECDSA and ZSS signature using the GLV method.

10. **2010, Efficient hardware design and implementation of AES cryptosystem**, Ghewari PB. et al :-In this paper , cryptographic algorithm can be implemented with FPGA which offers quicker solution and upgrade to incorporate any protocol change. In the paper optimized and synthesizable VHDL code is developed for the implementation of both 128 bit encryption and decryption process and minimizes the hardware consumption.

11. **2011, The LED block cipher**, Guo J. et al :- In this paper, block cipher LED is presented with AES algorithm for security purpose . It provide two implementation of LED; 1st for reference and other being optomized for performance. The proposed method, provide one of the smallest block cipher and maintain a competitive performance in software.

12. **2012, Effective implementation and avalanche effect of AES,** Kumar A. et al :- In this paper, implementation of AES algorithm using MATLAB. This paper explains the avalanche effect with the use of AES and MATLAB. One purpose for the avalanche effect is that by changing only one bit there is large change so it is difficult to analysis of cipher text. Hence the purposed method provides high security to information.

13. **2012, an efficient hardware model for RSA Encryption system using Vedic mathematics,** Bhasker. R et al :- In this research paper, RSA

algorithm is used with vedic multiplier and improved division algorithm is used to increase computation speed. Vedic maths gives advantage to calculate partial fraction in a single step.

14. **2013, Implementation of Secure Hash Algorithm-1 using FPGA,** Iyer NC. et al :- In this paper, VHDL is used to design and crypto SHA-1 algorithm is used with Xilinx ISE software. The design is implemented on Xilinx FPGA and test vectors are used and observed that the design generates correct hash values. This proposed SHA-1 architecture gives a higher working frequency and higher throughput.

15. **2014, A Tiny RSA Cryptosystem based on Arduino microcontroller useful for small scale network,** Al-Haija.QA et al :- In this paper, RSA crypto algorithm has been successfully implemented using Arduino MCU along with double keypad and screen touch. Here tested 32-bit encryption and decryption key which is provide small key size to infrastructure. If it is supported rechargeable battery along with a small solar cell than it can be used for the Ad-hoc sensory network.

16. **2015,An experimental realization of a Chaos-Based Secure communication using Arduino Microcontroller,** Acho.L et al :- In this paper, Communication system based on chaotic logistic map. In proposed system simple delta modulator is used for encryption. In this method no need of synchronization on receiver side and it can transmit signals whose bandwidth is 500Hz approximately.

17. **2016, Smart as a Cryptographic processor,** Kanchi S. et al :- In this paper, security algorithm and smart card are to be used for providing security to the ATM card and Smart card. This paper said that on comparing implementation of DES on HC12 we found that Smart code is only 14% longer in terms of static no. of instructions, and it is faster in term of clock cycle and smaller in terms of code size.

18. **2016, A compact 446Gbps/w AES accelerator for mobile SoC and IoT in 40 nm,** Zhang Y. et al :- In this paper, for security AES algorithm is used for mobile and IOT application which is fabricated in 40nm CMOS. Along this glitch reduction technique is used that provides low throughput output.

19. **2017, Design end to end Encryption based Biometric system for Security,** Chiranjeevi C. et al :- In this paper, A cloud based biometric system architecture is proposed which gives efficient and economical result for remote enrollment. It is low cost computer based system which is capable of capturing multimodal biometric traits.

20. **2018, Prediction of cardiovascular disease using sensor and technique of data mining,** Sangeetha G. et al :- In this paper, proposed method is used to secure the health related data and disease is predicted using the physical value of that patient using J48, RANDOM FOREST, LOGISTIC and NA�VE BAYES, In which NA�VE BAYES gives more accuracy.

21. **2018, FPGA based Implementation of AES algorithm using MIX-Column,** S. Neelima et al : - In this paper , modified AES-128-bit algorithm can be personalized, To improve this technique, introduced the high level increased parallelism scheme Mix-columns is used with FPGA device. In this paper increase the throughput efficiency, increase the stack usage with minimum reduction of area.

22. **2019, Compact circuits for combined AES Encryption / Decryption ,** Banik.S et al : -In this paper, the two reports of construction of AES circuit is provided , In the first one is 8-bit serialized implementation which provide both encryption and decryption both and second is optimize the above architecture to provide the dual encryption and decryption function. This paper concludes that required number of cycles reduces and save the gate area.

23. **2019, Triathlon of lightweight Block Ciphers for the Internet of Things** Dinu D. et a**l :-** In this paper, light weight block cipher is used with embedded platform. This paper work evaluates the execution time, memory size and code size. In this paper compares the different type of block cipher. The benchmarking framework provides cipher designers with easy to use and allow standardization.

3. CONCLUSIONS

This paper presents a survey of the most important cryptography algorithms implemented using different type of hardware like microcontroller (VLSI, FPGA, IoT, Arduino and S-boxes), and provide low cost and area of implementation. These cryptographic algorithms are studied and analysed well in order to help in enhancing the performance of the current cryptographic methods by using hardware. This paper shows the techniques that are useful for real-time encryption. All encryption methods have proven to have their advantages and setbacks and have proven to be appropriate for different applications. In this research paper, after investigation we found that AES is better than the other form of cryptography technology using with hardware as well as software. With the help of this research paper many student, teachers and developers will get help to easily found that which type of crypto-algorithm is already implemented with which type of hardware's. Also we found that in all these research papers none of research paper used to implement AES algorithm using STM32-bit microcontroller. So, our future work based on to implement AES algorithm using STM32 microcontroller.

REFERENCES

1. 2000, Gaj.k and Chodowiec.P, "**Comparison of the hardware performance of the AES candidates using reconfigurable hardware",** AES candidate conference, 40-54
2. 2004, Zhang. X et al, "**HIGH-speed VLSI Architectures for the AES algorithm**", IEEE transaction on very large scale integration system, 12(9): 957-967
3. 2005, Mangard.S et al, "**Successfully attacking masked AES hardware implementation",** International workshop on cryptographic hardware and embedded system, 157-171
4. 2006, Alho. T et al, "**Desing and implementation of low area and low power AES encryption hardware core**", 9th EUROMICRO conference on digital system design , 577-583
5. 2009, Rais MH. Et al," **Efficient hardware realization of AES using VIRTEX-5 FPGA"** , International journal of computer science and network security , 9(9):59-63
6. 2007, Huang .c et al**, "Compact FPGA implementation of 32- bit AES algorithm using Block RAM",** TENCON IEEE region 10 conference, 1-4
7. 2010, Ghewari PB. Et al, **"Efficient hardware design and implementation of AES cryptosystem"**, International journal of engg. Science and technology,2(3):213-219
8. 2011, Guo J. et al, **"The LED block cipher"**, International workshop on cryptographic hardware and embedded system, 326-341
9. 2012, Kumar A. et al, **"Effective implementation and avalanche effect of AES",** International journal of security, privacy and trust management, 1(3/4):31-35
10. 2016, Zhang Y. et al, **"A compact 446Gbps/w AES accelerator for mobile SoC and IoT in 40 nm",** IEEE symposium on VLSI circuit, 1-2
11. 2018, S. Neelima et al, "**FPGA based Implementation of AES algorithm using MIX-Column",** Microelectronics, Electromagnetics and Telecommunications, 233-245
12. 2019, Banik.S et al, "**Compact circuits for combined AES Encryption / Decryption"** , Journal of Cryptographic Engineering , 9(1): 69-83
13. 2007, Poschmann.A et al, "**New Light-Weight Crypto Algorithms for RFID**", IEEE International symposium on circuit and systems, 1843-1846
14. 2012, Bhaskar.R et al, **"An efficient hardware model for RSA Encryption system using Vedic mathematics"**, International Conference on Communication Technology and System Design, 30: 124-128
15. 2013, Iyer NC. et al**, "Implementation of Secure Hash Algorithm-1 using FPGA"**, International Journal of Information and Computation Technology, 3(8):757-764
16. 2014, Al-Haija.QA et al, **"A Tiny RSA Cryptosystem based on Arduino microcontroller useful for small scale network"**, Procedia computer science, 34:639-646
17. 2015 , Acho.L et al, **"An experimental realization of a Chaos-Based Secure communication using Arduino Microcontroller"**, The scientific world journal, 9:1-11
18. 2016, Kanchi S. et al, **"Smart as a Cryptographic processor"**, Proceeding of the SIXTH Internationalconference on computer science, Engg. And Information technology, 1-11
19. 2017, Chiranjeevi C. et al, **"Design end to end Encryption based Biometric system for Security"**, International journal of research, 4(2):838-843
20. 2018, Sangeetha G. et al, **"Prediction of cardiovascular disease using sensor and technique of data mining"**, IRJET, 5(9):1539-1542
21. 2019, Dinu D. et al, **"Triathlon of lightweight Block Ciphers for the Internet of Things"** , Journal of Cryptographic engineering , 9(3):238-302
22. 2012, Sharma M. et al, **"Analysis and comparison between AES and DES Cryptographic Algorithm"**, International Journal of Engg. And Innovative Technology, 2(6):362-365