COMPARATIVE STUDY OF SYMMETRIC CRYPTOGRAPHY ON FPGA

[1]Mayur Shah, [2]Ketan Bhavsar
[1]Electronics and Communication Engineer, [2]Project Coordinator
[1]VLSI & Embedded System Design, [2]VLSI & Embedded System
[1]GTU PG SCHOOL, Gandhinagar, Gujarat, India. [2]2BrainKlick Technologies, Gujarat, India

Abstract— With the rapid increase in computing and communication devices the need for security services has become crucial in information transfer. Protecting the digital information against security attacks is extremely important. Encipherment is the security mechanism that provides authenticity and confidentiality. Here FPGA is the best tool in market. This Paper contains the survey about some security algorithms for data security on FPGA.

Index Terms—Symmetric Cryptography, Speed, Security, AES

I. INTRODUCTION - Speech encryption has always been a very important part of secured communication [1]. Digital transmission is much more efficient than analog transmission and it is much easier for digital encryption techniques to achieve high degree of security. Modern cryptographic algorithms have potential to provide security services like data confidentiality, data integrity, authentication, non-repudiation and access control. With the advent of reconfigurable devices like FPGAs, hardware implementation of complex algorithms has become quite easy which makes it possible to achieve significant improvement in speed. AES is a cryptographic algorithm which needs large number of byte level and bit level operations.

1. IDEA ABOUT SYMMETRIC CRYPTOGRAPHY - Symmetric Cryptography has certain standards like DES, 3DES, AES, IDEA, Blowfish, RC4, RC5 & RC6.Symmetric key algorithms use same key for both encryption of plain text and decryption of cipher text. In Symmetric Cryptography AES (Advance Encryption Standard) is most widely used in industry because of its greater speed advantage.
Across the years, various comprehensive data encryption techniques have been developed. Some popular examples of symmetric key algorithms include RC4 (Rivest Cipher 4), DES (Data Encryption Standard), AES and triple DES [2]. AES cipher also known as Rijndael cipher is the most advanced cryptographic algorithm approved by National Institute of Standards and Technology (NIST) of the United States in 2001 [3].

II. STUDY OF SYMMETRIC CRYPTOGRAPHY & STANDARDS ON FPGA

1. Hash Function- AES - Key concept of cryptography is to hide the data just like putting valuables in a box protected by a lock-key pair. Key(s) are essential and crucial part of encryption algorithm, and number and length of keys vary depending upon the purpose. Here it's implemented a multi key algorithm with real time key updating functionality where keys get updated every time they get used up. Here is advantage Changing key at every cycle, which makes it tough to break. To reduce area, serial peripheral devices can be used. Real time requires least delay [1].

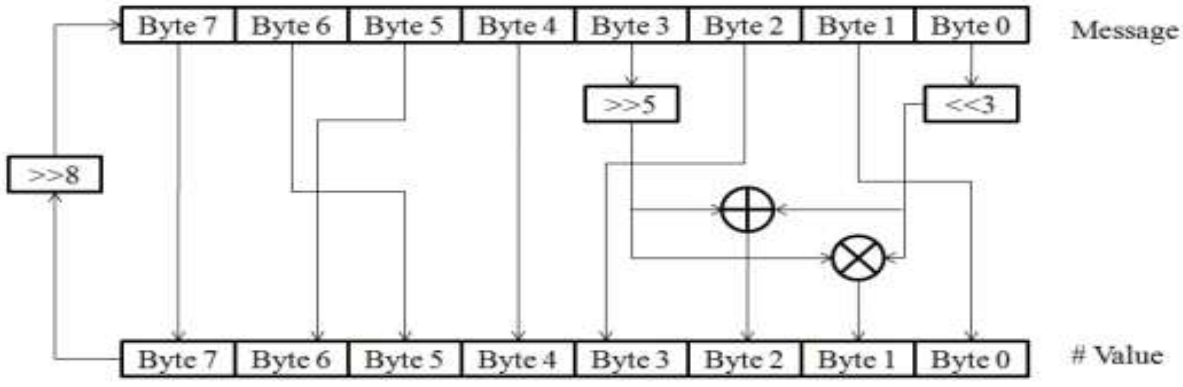

Figure 1. Hash function [1]

2. AES -Quartus II and Nios II 10.1 software - Implementation of AES algorithm for 128 bit data and 128 bit key in RTL (VHDL) and its software implementation using C. Application of Advanced Encryption Standard (AES) algorithm in UART for secure transfer data in software and hardware platform which are (RTL) VHDL and 'C' and further to decide suitably of its implementation of specific platform (software and hardware) depending on different baud rates supported by UART. Advantages are Hardware and software implementations of AES Algorithm in UART is carried out for data security [2].

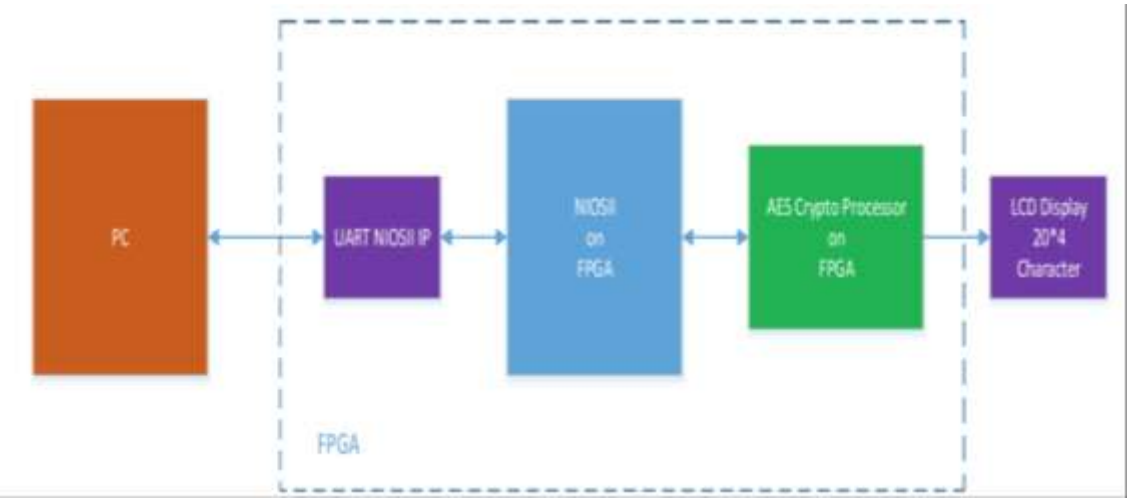

Figure 2. Block diagram [2]

3. AES Rijndael Encryption and Decryption Algorithm -Xilinx Virtex-7 FPGA - This paper presents the hardware implementation of AES Rijndael Encryption and Decryption Algorithm by using Xilinx Virtex-7 FPGA. Here architecture is found to be having good efficiency in terms of latency, throughput, speed/delay, area and power. Here the advantages have less complex architecture, than by providing high throughput and low latency, the overall delay is very less [3].

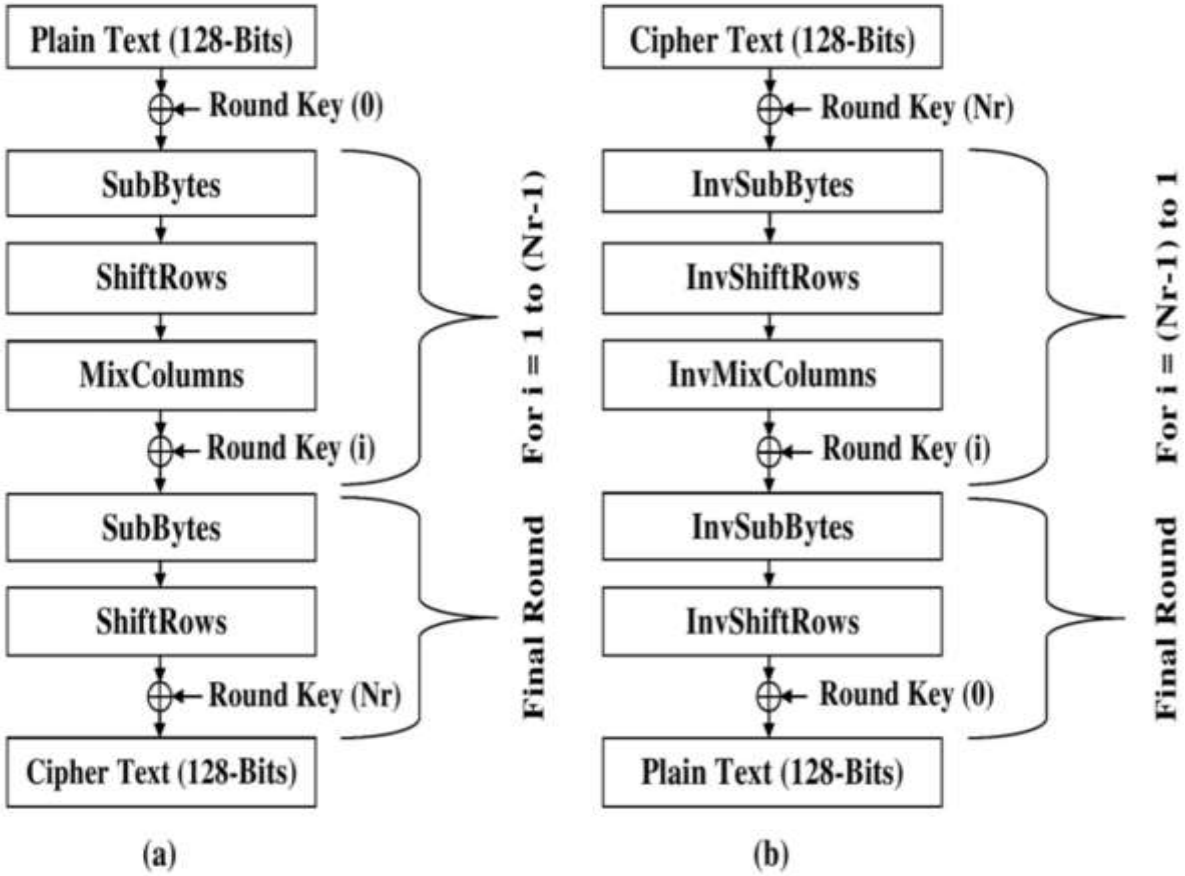

Figure 3. AES Rijndael Algorithm. (a) Encryption Block. (b) Decryption Block [3]

4. Unvoiced replacement- Xilinx xc2vp30- Real time processing system - An improvement unvoiced replacement technique based on real time processing using Field Programmable Gate Array (FPGA) board. The Virtex-II Pro board which consists of XC2VP30 chip as central processor unit is used in this research. The XC2VP30 chip consists of 30,816 logic cells and also it can operate with external memory for parallel buffers where sampling data are stored. Here the advantages of this it used only 4.17 ms to 50 ms for time processing which does not effect to delay time process on real time system. Moreover, the quality of the output speech signal is still similar to the original speech signal [4].

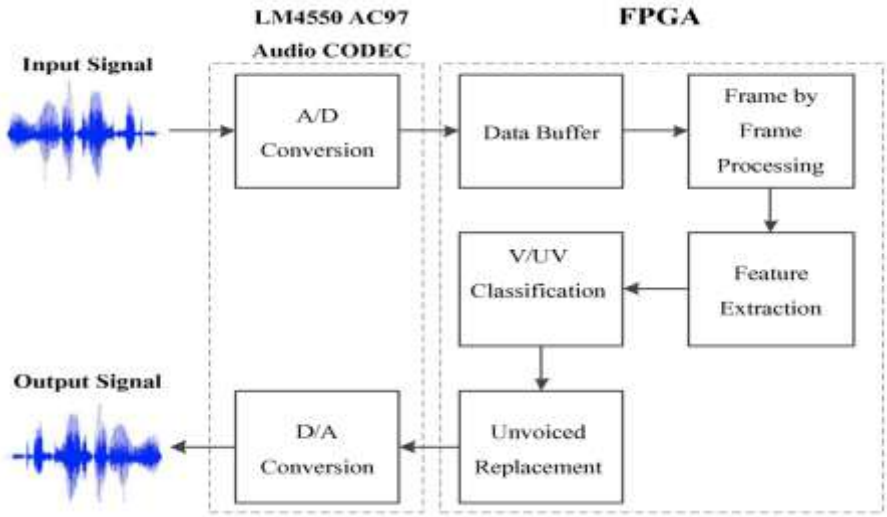

Figure 4. The diagram of unvoiced replacement system [4]

5. AES – Speech encryption-decryption - Advanced Encryption Standard, a sophisticated cryptographic algorithm, which ensures that the transmitted data is protected from unauthorized disclosure. Here advantages a new hardware implementation has been developed for real time application of offline speech encryption and decryption using AES algorithm. Cryptanalytic attacks are less efficient for longer keys and hence 128-bit AES used in this work is definitely more secure. But disadvantages the algorithm is virtually indecipherable. Further optimization may need to be done for minimizing the required area on may need to be done for minimizing the required area on FPGA for high end applications [5].

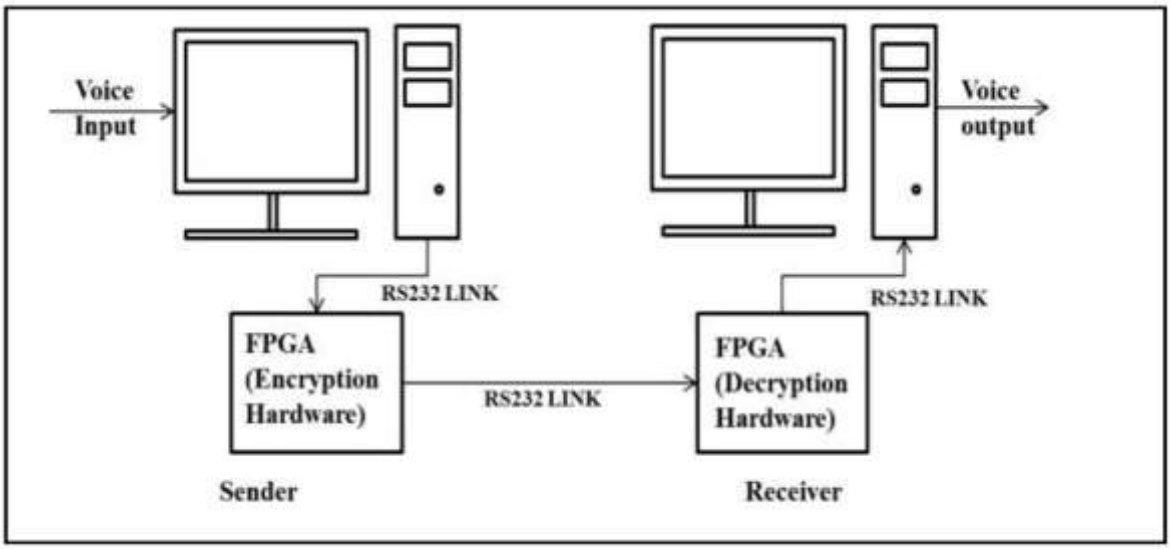

Figure 5. End to end Data transfer [5]

III. CONCLUSION - In Symmetric Cryptography, there is always a trade-off between security and performance (speed). As we increase in security then complexity of system also gradually increases which resultant in more area consuming, degradation in performance (speed) of system. The future work is to find a solution which can maintain greater Security with efficient way in terms of improves speed, reduction in power and area requirements.

REFERENCES

[1] Katkade, P., & Phade, G. M. (2016, August). Application of AES algorithm for data security in serial communication. In Inventive Computation Technologies (ICICT), International Conference on (Vol. 3, pp. 1-5). IEEE.

[2] Sharma, P., & Sharma, R. K. (2016, June). Design and implementation of encryption algorithm for real time speech signals. In Advances in Signal Processing (CASP), Conference on (pp. 237-241). IEEE.

[3] Sutacha, C., & Srinonchat, J. (2016, June). Improvement unvoiced replacement techniques base on real time processing using FPGA board. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2016 13th International Conference on (pp. 1-4). IEEE.

[4] Srinivas, N. S., & Akramuddin, M. (2016, March). FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption. In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on (pp. 1769-1776). IEEE.

[5] Kumar, L. P., & Gupta, A. K. (2016, May). Implementation of speech encryption and decryption using advanced encryption standard. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on (pp. 1497-1501). IEEE