HIGH SECURITY VLSI DESIGN OF AESCRYPTO PROCESSOR FOR IMAGE ENCRYPTION

M.LAVANYA , S.SASIKALA

Abstract— The Advanced Encryption Standard (AES) is a data encryption specification. This standard has become one of the most extensively used encryption technology and has been implemented in both software and hardware. A high-security symmetric cryptography technique with field-programmable gate array implementation (FPGA). The suggested design contains an 8-bit data route as well as five main blocks. For storing plain text, keys, and intermediate data, we construct two specific register banks, Key-Register and State-Register. To decrease the area, Shift-Rows is inserted into the State-Register.We build an optimized 8-bit block for Mix-Columns with four internal registers that accept 8-bit and send out 8-bit to adapt the Mix-Column to an 8-bit datapath. Additionally, shared optimized Sub-Bytes are used during the key expansion and encryption phases. We consolidate and simplify various Sub-Bytes in order to optimize them. The clock gating technique is used in the design to reduce power consumption. This study provides a 128-bit AES architecture based on Image Cryptography. This design was implemented in an FPGA XC3S 200 TQ-144 using Verilog HDL, simulated with Modelsim 6.4 c, and synthesized with the Xilinx tool.

I. INTRODUCTION

The act of utilising a cryptosystem or cypher to prohibit anyone other than the intended recipient(s) from reading or using the encrypted data is known as cryptography, sometimes known as encryption. A message can be encoded using a cryptosystem. Only when the correct algorithm and keys are used to decode the message can the recipient see the encrypted content. The main application of cryptography is the transmission of confidential information through computer networks. A clear-text document is transformed into crypto-text during the encryption process by applying a key and a mathematical algorithm to it. If the reader doesn't have the key to decrypt the document, it cannot be read in crypto-text. Because to increases in computer processing capacity, it was widely acknowledged that DES was no longer secure. The purpose of NIST was to develop a replacement for DES that could be used by US government agencies for non-military information security applications. Of course, it was known that NIST's work would assist business and other non-government users, and that the work would be widely adopted as a commercial standard. The National Institute of Standards and Technology (NIST) invited cryptography and data security experts from around the world to participate in the discussion and selection process. Five encryption techniques were chosen for research. The encryption technique suggested by Belgian cryptographers Joan Daeman and Vincent Rijmen was chosen through a consensus-building process. Before choosing, Daeman and Rijnmen called the algorithm Pipelined, which is a combination of their names. The Advanced Encryption Standard (AES),

which is still widely used today, was given to the encryption algorithm when it was adopted. The AES encryption algorithm was formally adopted by the NIST in 2000 and published as a federal standard under the name FIPS-197. You can access the complete FIPS-197 standard on the NIST website (see the Resources section below). As was to be expected, numerous manufacturers of encryption hardware and software have included AES encryption to their offerings. The block cypher AES encryption algorithm employs multiple rounds of encryption and an encryption key. An encryption system known as a block cipher only encrypts one block of data at a time. The block in typical AES encryption has a length of 128 bits, or 16 bytes. The phrase "rounds" describes how the encryption process re-encrypts the data ten to fourteen times, depending on the size of the key. This is explained in the AES encryption article on Wikipedia. AES is

M.Lavanya , PG Scholar, Department of ECE , Sree Sakthi Engineering College.
S.Sasikala, M.E., (PhD) , Assistant Professor , Department of ECE , Sree Sakthi Engineering College.

neither a computer programme or source code in and of itself. It is a mathematical explanation of how to hide data.

II. EXISTING SYSTEM:

It utilizes the SDRR in an established Advanced Encryption Standard (AES)-128 design, enhancing the cryptographic hardware's resistance to modern PAAs. The combinational path in the AES-128 using SDRR analyses random data continuously during the clock cycle, and the interleaved processing of real and random data ensures the safety of both combinational and sequential logics.

Fig 1 Shows the Block diagram of Existing System

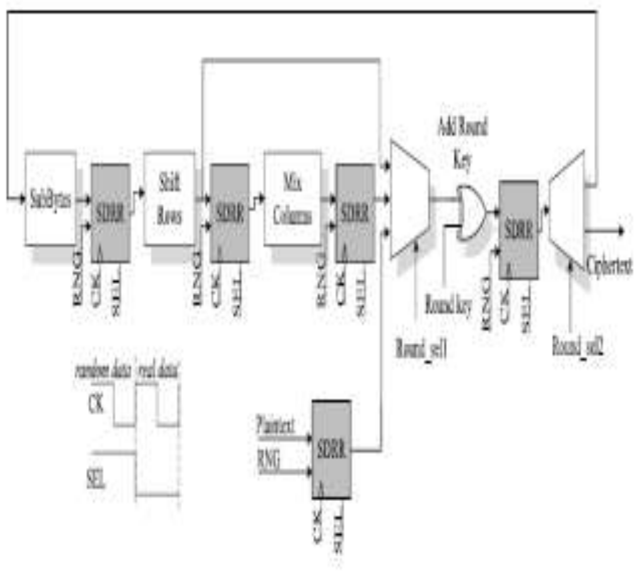


Figure 1: Block Diagram of Existing System

III.LITERATURE SURVEY:

Title: Differential power analysis: A serious threat for FPGA security

Authors: M. Masoumi

Publication: Int. J. Internet Technol. Secured Trans., vol. 4, no. 1, pp. 12–25

Year: 2012

This article explains the fundamentals of the differential power analysis (DPA) attack and shows how it can be applied successfully to an FPGA version of the advanced encryption standard (AES) algorithm. The findings of this study unequivocally show that DPA poses a severe threat to the implementation of encryption algorithms on SRAM-based FPGAs in the absence of appropriate defences.

Title: The research of DPA attacks against AES implementations

Authors: H. Yu, Z. Xue-Cheng, L. Zheng-Lin, and C. Yi-Chen

Publication: J. China Univ. Posts Telecommun. vol. 15, no. 4, pp. 101–106,

Year: Dec. 2008

The vulnerability of software and hardware implementations of cryptographic algorithms to power analysis attacks is examined in this article. To obtain power data, a simulation-based experimental environment is developed, and single-bit differential power analysis (DPA) and multi-bit DPA and correlation power analysis (CPA) attacks are performed on two implementations, respectively. The experimental results reveal that the hardware implementation has fewer data-dependent power leakages, making it more resistant to power attacks. In addition, an enhanced DPA technique is proposed.

Title: AES against first and second-order differential power analysis Applied Cryptography and Network Security

Authors: J. Zhou and M. Yung, Eds.

Publication: vol. 6123, Springer-Verlag, pp. 168–185. Berlin, Germany

Year: 2010

This paper present five fundamental concepts about DPA vulnerability in unprotected AES implementations and several general ideas regarding DPA vulnerability in protected AES implementations. These principles define which AES operations are susceptible to first- and second-order DPA. Finally, we conclude that for an AES software implementation to be resistant to first and second-order DPA in practise, at least the first two and a half rounds and the last three rounds of AES should be secured.

Title: High-speed VLSI architectures for the AES algorithm

Authors: X. Zhang and K. K. Parhi

Publication: IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 9, pp. 957–967

Year: Sep. 2004

New high-speed architectures for the hardware implementation of the Advanced Encryption Standard (AES) algorithm are presented in thiswork. The suggested solution exclusively uses combinational logic, unlike other efforts that also used look-up tables to achieve the AES algorithm's Sub Bytes and Inv Sub Bytes transformations. As a direct result, the insurmountable delay caused by look-up tables in conventional techniques is removed, allowing sub pipelining's advantages to be further investigated.

Title: Post-Quantum Crypto processors Optimized for Edge and Resource-Constrained Devices in IoT

Authors: ShahriarEbrahimi, SiavashBayat-Sarmadi, HatamehMosanaei-Boorani

Year: 2019

Publication: IEEE Internet of Things Journal PP(99):1-1

The suggested designs can accommodate various levels of security, and we present experimental findings for two iterations of the InvRBLWE scheme that offer 84 and 190 bits of conventional security. The best prior classic and post-quantum implementations are dominated by our FPGA implementation findings. Additionally, improvements can be shown in terms of speed, area, power, and/or energy in our two alternative ASIC implementations. We are, as far as we know, the first party to build LWE-based cryptosystems on an ASIC platform.

Title: A High Data Rate Pipelined Architecture of AES Encryption/Decryption in Storage Area Networks

Authors: HosseinKouzehgar, MeisamNesaryMoghadam and PooyaTorkzadeh

Year: 2018

Publication: 26th Iranian Conference on Electrical Engineering (ICEE2018)

A combined strategy of memory utilisation and GF(24) is used to achieve the target throughput rate for the AES algorithm in the data storage network. To get the fewest slices feasible, a special multiplexer-based design is used below the S-Box block. The combined output of the Xilinx Virtex5-based encryption and decryption system, with its 60 Gbps throughput and 460 MHz operating frequency, shows improved performance compared to the best earlier studies.

IV. PROPOSED SYSTEM:

The masked AES core and clock gating are used in the AES implementation to create the encryption masks. 128 bit encryption is performed using the maskedAES core. In order to save space compared to a fully unrolled implementation, the procedure is carried out in 10 cycles, computing 1 round every cycle. The suggested masked AES is depicted in the figure below. where a randommask is used to first mask the original data (plaintext). The "Nano AES core" is then fed the mask and the masked plaintext, encrypting the masked data using the secret key. The module receives result masked cipher-text and outputs the desired cipher-text.

1) The Shift-Rows are contained into the State-Register in order to minimise the necessary logic.

2) We share the Sub-Bytes block with the key expansion and encryption phases after optimising it.

3) We create an 8-bit block that is optimal for Mix-Columns with 8-bit input and output based on the 8-bit data path's structure, which is then followed by Add-Round-Key. As a result, the results are sent byte-by-byte to Add-Round-Key. It is not essential to save the results in the registers or make the data path for the Key-Register 32 bits longer than it is for 32-bit Mix-columns.

4) The clock gating approach is used in various portions of the design to lower the power consumption, which results in a lower power consumption.

To reduce dynamic power usage, we use the clock gating technique in several aspects of the design. Clock gating is done individually to State-Register, Mix-Columns' internal registers, Key-Register, and RCON. For example, the key expansion phase saves the most power; the clock of State-Register and Mix-Columns is disabled to save power because these two blocks are not used during the key expansion phase.Figure 2 shows the block diagram of proposed system.

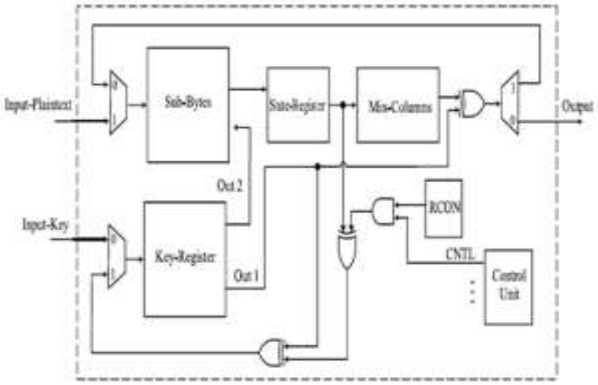


Figure 2: Block diagram of proposed System

1)Algorithm

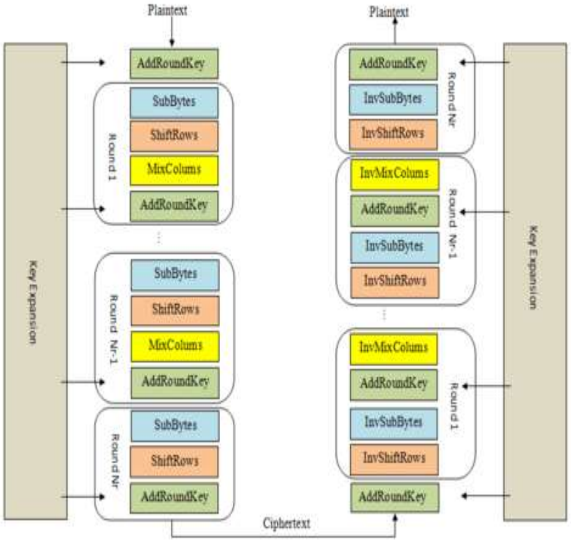
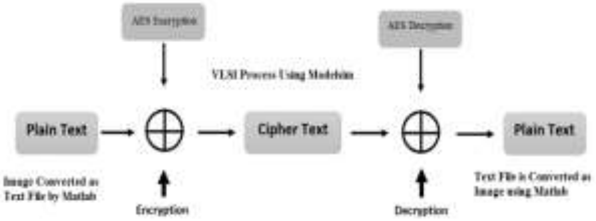


Figure 3: Algorithm of Proposed system

2)Application Block Diagram

As shown Fig 3 we will design a Decryption Scheme based on Proposed Scheme. We are going to Make Encryption & Decryption Based on Images. We are going to merge the Matlab& VLSI for this Process.


AES Encryption
AES Decryption
VLSI Process Using Modelsim
Plain Text
Cipher Text
Plain Text
Image Converted as Text File by Matlab
Encryption
Decryption
Text File is Converted as Image using Matlab

3)Software Requirements

This paper presents an Image Cryptography based 128-bit AES design. This Design is implemented in FPGA XC3S 200 TQ-144 using Verilog HDL and simulated by Modelsim 6.4 c and Synthesized by Xilinx tool. In Syntheis Process will generate RTL Viewer and Technology Viewer. Power calculation is done by Xpower Tool. Image Processing is made by Matlab **Tool.**

V. RESULTS

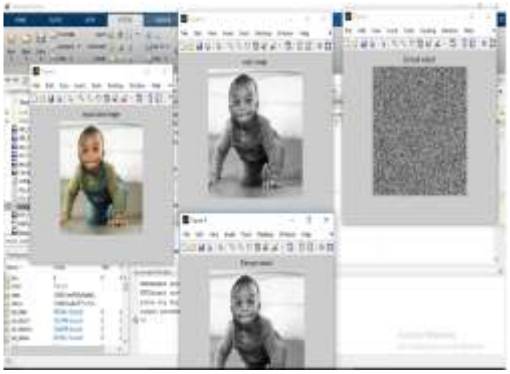
1)Simulation result of Encryption & Decryption:

This is Encryption & Decryption Simulation Result. Plain_Test is Primary Input Data and Key is Key for Encryption Process. Cipher_Test is Encrypted Output. Key1 to Key 10 are the Generated key for Each Round by Key Generation Unit. This waveform Simulated by Modelsim Tool and we can give the Input based on Binary Number and we Showed op as Hexa Decimal format in the Figure

.

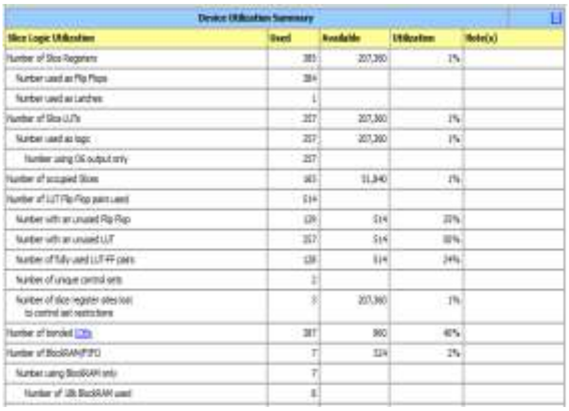
2) IMAGE PROCESSING OUTPUT

We done image Processing Image Cryptography using our proposed design. Here Matlab will convert the image into text and Verilog AES Code will make Cryptography Process. Finally the Decrypted text data will convert back as Image using Matlab.



3)Xilinx device utilization summary of encryption module:

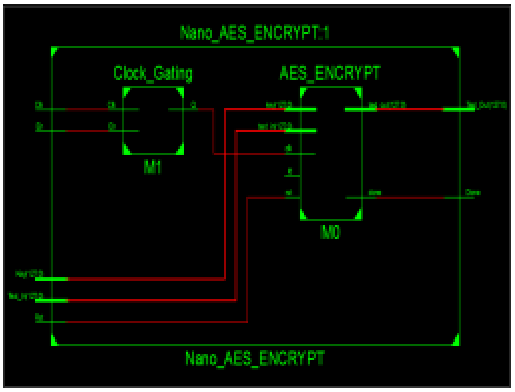
This is Devise utilization Summary for the Proposed Encryption algorithm, Here We show no of Register used, No of LUT occupied, Slices and all.



Device Utilization Summary				
Slice Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Registers	385	207,360	1%	
Number used as Flip Flops	384			
Number used as Latches	1			
Number of Slice LUTs	257	207,360	1%	
Number used as logic	257	207,360	1%	
Number using O6 output only	257			
Number of occupied Slices	163	51,840	1%	
Number of LUT Flip Flop pairs used	514			
Number with an unused Flip Flop	129	514	25%	
Number with an unused LUT	257	514	50%	
Number of fully used LUT-FF pairs	128	514	24%	
Number of unique control sets	2			
Number of slice register sites lost to control set restrictions	0	207,360	1%	
Number of bonded IOBs	387	960	40%	
Number of BlockRAM/FIFO	7	324	2%	
Number using BlockRAM only	7			
Number of 18k BlockRAM used	8			

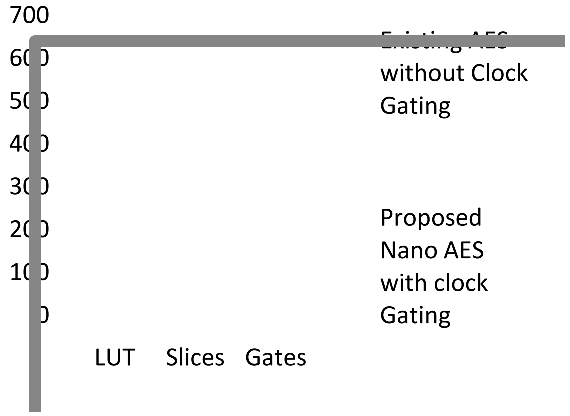
4) RTL View of AES MAIN Module

This is RTL View of Proposed Design. RTL Means Register transfer Level. Here the Verilog HDL Code is converted as Schematic View. It shows Each and Every individualModuleas internal modules.

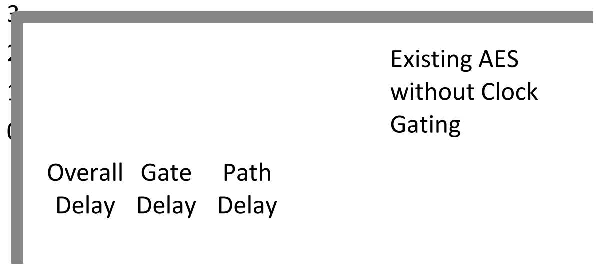


VI. COMPARISON RESULT

1) AREA:



2)DELAY:



VII. CONCLUSION:

With a high level of security, the widely utilized Nano AES symmetric cryptography method is employed in several applications and networks. AES is a viable algorithm for small IoT devices as a result. In this paper, we developed a compact AES architecture for IoT devices with limited resources. The architecture had an 8-bit datapath and two designated register banks for storing keys, intermediate results, and plain text. Shift-Rows were executed inside of the State- Register to lessen the amount of logic needed. Additionally, the design shared optimized Sub-Bytes with the encryption and key expansion phases. In addition, we created mix-Columns, a suitable block for low-area design, with 8-bit input and output. We used the clock gating technique in several design blocks to reduce the area and power consumption, which resulted in a 30% area reduction on the Spartan 3 xc3s 200 tq144 boards. We done image Processing Image Cryptography using our proposed 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] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of things,” Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[8] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, “Challenges in access right assignment for secure home networks,” in Proc. USENIX Conf. Hot Topics Secur., 2010, pp.1-6.

[9] M. Mozaffari-Kermani and A. Reyhani-Masoleh, “Concurrent structure independent fault detection schemes for the Advanced Encryption Standard,” IEEE Trans. Comput., vol. 59, no. 5, May 2010.

[10] M. Mozaffari-Kermani and A. Reyhani-Masoleh, “A low-power high performance concurrent fault detection approach for the composite field S-box and inverse S-box,” IEEE Trans. Comput., vol. 60, no. 9, pp. 1327–1340, Sep. 2011.