RESEARCH ARTICLE OPEN ACCESS

HIGH SECURITY AND LOW POWER AES CRYPTO PROCESSOR SECURITY ALGORITHM FOR IMAGE ENCRYPTION

Vino.T*, Dr. V.Kalaipoonguzhali,**

*(PG Scholar VLSI/Sembodai Rukmani Varatharajan Engineering College, and Sembodai, Email: vinobe1989@gmail.com)

**(Professor and HOD of ECE, /Sembodai Rukmani Varatharajan Engineering College, and Sembodai, Email: hodeeesrvec@gmail.com)

----------**********----------

Abstract:

Advanced Encryption Standard (AES) is a specification for electronic data encryption. This standard has become one of the most widely used encrypt method and has implemented in both software & hardware. A high-secure symmetric cryptography algorithm, implementation on field-programmable gate array (FPGA). The proposed architecture includes 8-bit data path and five main blocks. We design two specified register banks, Key-Register and State-Register, for storing the plain text, keys, and intermediate data. To decrease the area, Shift-Rows is embedded inside the State Record. To adapt the Mix-Column to 8-bit datapath, we design an optimized 8-bit block for Mix-Columns with four inside registers, which accept 8 bit and send back 8-bit. Also, shared enhanced Sub-Bytes are employed for the key expansion phase and encryption phase. To optimize Sub-Bytes, we merge and simplify some parts of the Sub-Bytes. To reduce power feeding, we apply the clock gating system to the design. This paper presents and 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.

Keywords —Encryption,Decryption,AES,FPGA,HDL.

----------**********----------

I. INTRODUCTION

This document is a template. An electronic copy can bedownloaded from the conference website.Cryptography, often called encryption, is the practice of creating and using a cryptosystem or cipher to prevent all but the intended recipient(s) from reading or using the information or application encrypted. A cryptosystem is a technique used to encode a message. The recipient can view the encrypted message only by decoding it with the correct algorithm and keys. Cryptography used mostly for communicating sensitive physical across computer networks. The process of encryption takes a clear-text document and applies a key and a mathematical algorithm to it, converting it into crypto-text. In crypto-text, the document is unreadable unless the reader possesses the key that can undo the encryption. In 1997 the National Institute of Standards and TECHNOLOGY (NIST), a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES). It was generally recognized that DES was not secure because of advances in computer processing power. The goal of NIST was to define a replacement for DES that could be used for non-military information security applications by US government agencies. Of course, it was documented that commercial and other non-government users would advantage from the work

of NIST and that the work would be usually adopted as a lucrative standard. The NIST asked cryptography and data security experts from around the world to participate in the discussion and selection process. Five encryption algorithms were adopted for study. Through a process of agreement the encryption algorithm proposed by the Belgium cryptographers Joan Daeman& Vincent Rijmen are selected. Prior to selection Daeman&Rijnmen used the name Pipelined (derived their names) for the algorithm. After adoption the encryption algorithm was given the name Advanced Encryption Standard (AES) which is in common use today. In 2000 the NIST officially adopted the AES encryption algorithm and published it as a federal standard underneath designation FIPS-197. The full FIPS-197 standard is available on the NIST web site (see the Resources section below). As predictable many providers of encryption software & hardware have combined AES encryption into their products.

AES encryption is a block cipher that is usages an encryption key and several circles of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term "rounds" mentions to the way in which the encryption algorithm blends the data re encrypting it ten to fourteen times depending on the extent of the key. This is described in the Wikipedia article on AES encryption. The AES algorithm the situation is not a computer program or source code. It is a mathematical description of a process of obscuring data. Several people have created source code applications of AES encryption, including the original authors.

II. LITERATURE SURVEY-1:

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

Differential Power Analysis (DPA) is a powerful and practical technique used to attack a cryptographic implementation in a resource limited application environment. In this paper, they show that some intermediate values from the inner rounds can be exploited by deploying techniques such as fixing certain plaintext/cipher text bytes. We give five general principles on DPA vulnerability of unprotected AES implementations, and give several general principles on DPA vulnerability of protected AES implementations. These principles specify which processes of AES are susceptible to first and second order DPA. To illustrate the principles, we attack the two AES implementations [1, 2] that use two kinds of countermeasures to achieve a high resistance against power analysis, and demonstrate that they are even vulnerable to DPA. Finally, we conclude that at least the first two and a half rounds and the last three rounds of AES should be secured for an AES software implementation to be unaffected against first and second order DPA in practice.

III. LITERATURE SURVEY-2:

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

This article examines vulnerabilities to power analysis attacks between software and hardware implementations of cryptographic algorithms. A simulation-based experimental environment is built to acquire power data, and single-bit differential power analysis (DPA), and multi-bit DPA and correlation power analysis (CPA) attacks are conducted on two implementations respectively. The experimental results show that the hardware implementation has less data-dependent power leakages to resist power attacks. Furthermore, an improved DPA approach is proposed. It accepts hamming distance of intermediate outcomes as power model and arranges plaintext inputs to

separate power traces to the best probability. Related with the unique power attacks, our better DPA performs a positive attack on AES hardware executions with acceptable power measurements and fewer calculations.

IV. EXISTING SYSTEM:

We exploit the SDRRin a conventional advanced encryption standard (AES)-128architecture, improving the immunity of the cryptographic hardwareto the state-of-the-art PAAs. In the AES-128 exploitingSDRR, the combinational path evaluates random data throughoutthe entire clock cycle, and the interleaved processing of randomand real data ensures the protection of both combinational andsequential logics.

V. EXISTING SYSTEM DRABACKS:

- A conventional masked AES engine requires a large lookup table
- The performance is significantly reduced Due to the SDRR Architecture

VI. PROPOSED SYSTEM:

The AES implementation consists of the masked AES core and Clock gating to generate the encryption masks. The maskedAES core performs 128 bit encryption. The process is done in 10cycles, computing 1 round per cycle, with the hardware of eachround being reused to save area verses a fully unrolledimplementation. Where the original data (plaintext) is first masked by a randommask. The masked plaintext and the mask are, then, fed through the "Nano AES core" which encrypts the masked data with thesecret key. Result masked cipher-text is input into the module to arrive at the intended cipher-text.

In the different parts of the design, we apply the clock gating technique to reduce the dynamic power consumption. The clock gating is separately applied on State-Register, the internal registers of Mix-Columns, Key-Register, and RCON. For instance, the most power consumption is saved during the key expansion phase; the clock of State-Register and Mix- Columns is disabled to save power because these two blocks are not used in the key expansion phase.

Clock gating is a best technique to reduce chip active power. Clock gating techniques based on Adaptive Clock Gating and instruction level clock gating. clock gating technique decreases not only switching activity of practical blocks in IDLE state but also dynamic power in running state. Our modified Adaptive Clock Gating can automatically enable or disable the clock of the functional block. Clock gating is a popular method used in many synchronous circuits for dipping dynamic power dissipation. Clock gating saves power by adding more logic to a circuit to prune the clock tree.

VII. PROPOSED SYSTEM ADVANTAGES:

- Low-power Design
- Low-energy high-throughput hardware AES encryption module providing multiple levels
- High security with Best Attacks Prevention scheme

VIII. SYSTEM ARCHITECTURE:

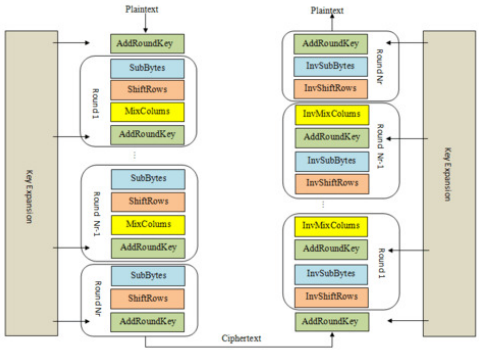

Fig. 1System Architecture

IX. COMPARISON TABLE:

S.No	Method Name	Area			Delay		
		Slice	Flip Flops	LUT	Max Delay	Gate Delay	Path Delay
1	Normal AES Design	7734	21207	21207	160.860ns	25.302ns	135.558ns
2	Proposed Nano AES with Clock Gating	1670	1066	3900	3.405ns	2.923ns	0.482ns

Fig. 2 Comparison Table

X. CONCLUSIONS

Nano AES is safe symmetric cryptography algorithm with a high level of security, which is broadly used in several applications and networks. Thus, AES is a suitable algorithm for tiny IoT devices. In this article, we designed a lightweight AES architecture for resource-constrained IoT devices. The design had 8-bit datapath and included two specified register banks for storing plain text, keys, and intermediate results. To reduce the required logic, Shift-Rows was run inside of the State- Register. Also, the design had an optimized Sub-Bytes that was shared with encryption and the key expansion phase, Furthermore, we designed mix-Columns with 8-bit input and output, which is a proper block for low-area design. To reduce the Area & power consumption, we applied the clock gating technique in different blocks of the design, which led to reduce the area by 30% on Virtex 5 xcVLX330T FF1738 -2 board.

REFERENCES

[1] 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] 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] 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] 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] 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] 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] 7. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011.
[8] 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] 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, pp. 608–622, May 2010.
[10] 10. M. Mozaffari-Kermani and R. Azarderakhsh, "Efficient fault diagnosis schemes for reliable lightweight cryptographic ISO/IEC standard CLEFIA benchmarked on ASIC and FPGA," IEEE Trans. Ind. Electron., vol. 60, no. 12, pp. 5925–5932, Dec. 2013.

