THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Power Analysis on Asynchronous S-Box by Measurement and Evaluation

A. Poojaa
Assistant Professor, Department of ECE, Bharathiyar Institute of Engineering for Women, India

Abstract
This project illustrates the hardware implementation of a low-power asynchronous Advanced Encryption Standard substitution box (S-Box). It is capable of resistant to side channel attack (SCA). The asynchronous S-box is based on self-time logic referred to as null conventional logic (NCL). NCL supports for resistant to the side channel attack of SCA's such as clock free, dual – rail encoding and monotonic transitions. To implement both the synchronous and asynchronous S-Box design a specified Field Programmable Gate Array (FPGA) Board is used. The beneficial properties is difficult for an unauthorized person to decipher secret keys which is embed within the cryptographic circuit of FPGA board while comparing the resistant to SCA of proposed with existing DPA (Differential Power Analysis) and Correlation Power Analysis (CPA) are presented in the S-Box. The power measurement results showed that NCL S-Box had 22% - 26% lower total power consumption than the original and was effective against DPA and CPA attacks. The dual-rail encoding with the pre-charge method, spacers (or) return-to-zero protocols is frequently used in both the synchronous and asynchronous designs. SCA's explore the security information by monitoring the emitted outputs from physical cryptosystems. These outputs include execution timing, power consumption, electromagnetic leaks and thermal emanations or acoustic emanations. Accurate measurement and estimation of these outputs are the key points of a successful attack. The SCA's include simple power analysis (SPA), Differential Power Analysis (DPA), Collision attacks and leakage power analysis. Among these, DPA and CPA are the most popular and effective attack.

Key words*: Null Conventional Logic Differential Power Analysis, Correlation Power Analysis, Simple power analysis*

1. Introduction

The crypto hardware devices that have enhanced security measures while being energy efficient are in high demand. In order to reach this demand of low-power devices with high-security features, researchers generally focus around the cryptographic algorithm actually implemented in the hardware itself to encrypt and decrypt information. These works are centered on resisting DPA attacks and introduce methods on how to effectively reduce the impact of DPA attacks. However, they are fundamentally based on synchronized circuits, which either require a precise control of timing or suffer from some timing related issues, such as glitches, hazards, and early propagation, which still could leak some side-channel information to the attackers. Our proposed null-conventional-logic-based (NCL) substitution box (S-Box) design matches the important security properties: asynchronous, dual rail encoding, and an intermediate state.

2. Proposed System

At the present time we design the single integrated chip by combine the embedded system design and algorithm. So it gives minimum size and low power consumption. S-box performed encryption and inverse S-box performed decryption process. In existing System, we have separate designs for S-box and inverse S-box. It's occupied more area and consumes more power. So we want plan an S-box and inverse S-box in same design. So the area will reduce. We using the NCL (Null Conversion Logic) for the speed will increase and area will reduced. This is mainly used in digital information security, crypto hardware devices, mobile phones, portable devices, computer/network security, and industrial control system.

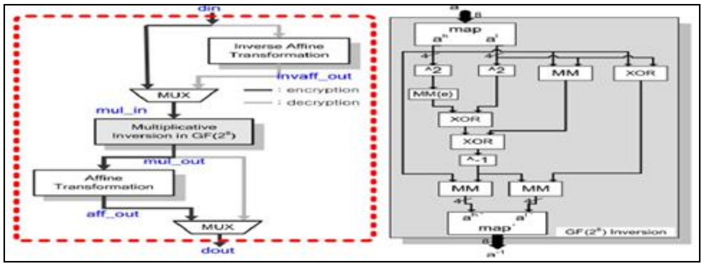


Figure.1 Block Diagram of Proposed System

2.1. Proposed System Technique (Algorithm)

The process of DPA consists of the following steps.

1) The average current corresponding to each output data are calculated in Matlab using the following root-mean square algorithm:

$$\mathbf{Ap}=\sqrt{\frac{1}{Nsample}\sum_{k=0}^{Nsample} xi^2}$$

where *Ap* is the average of *N* sample sampled current for output data *i.*

Two groups are defined according to the select function that is presented in when the secret key is used as follows:

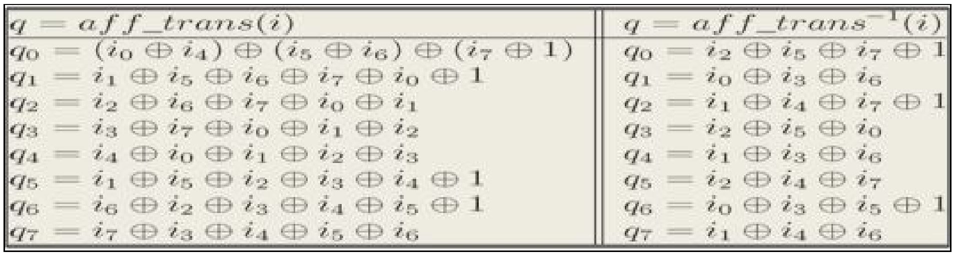
$$\mathrm{A}_{\mathrm{p,x}}=1/\mathrm{N0}\sum_{\square}^{Gx,0,i} Ap,\, i$$

$$\mathrm{A}_{1,\mathrm{x}}= \sum_{\square}^{Gx,1,j} Ap,\, j$$

where *Gx*,0,*i* and *Gx*,1,*j* are two sets of average current, respectively, and they are grouped according to an arbitrary bit in the output.

2.2. Affine Transform

The affine transformation and inverse affine transformation components follow a series of Boolean equations given in Table.1, where i and q represents the 8-bit input and output, respectively. Both transformations require many XOR gates.



$q = aff\_trans(i)$	$q = aff\_trans^{-1}(i)$
$q_0 = (i_0 \oplus i_4) \oplus (i_5 \oplus i_6) \oplus (i_7 \oplus 1)$	$q_0 = i_2 \oplus i_5 \oplus i_7 \oplus 1$
$q_1 = i_1 \oplus i_5 \oplus i_6 \oplus i_7 \oplus i_0 \oplus 1$	$q_1 = i_0 \oplus i_3 \oplus i_6$
$q_2 = i_2 \oplus i_6 \oplus i_7 \oplus i_0 \oplus i_1$	$q_2 = i_1 \oplus i_4 \oplus i_7 \oplus 1$
$q_3 = i_3 \oplus i_7 \oplus i_0 \oplus i_1 \oplus i_2$	$q_3 = i_2 \oplus i_5 \oplus i_0$
$q_4 = i_4 \oplus i_0 \oplus i_1 \oplus i_2 \oplus i_3$	$q_4 = i_1 \oplus i_3 \oplus i_6$
$q_5 = i_1 \oplus i_5 \oplus i_2 \oplus i_3 \oplus i_4 \oplus 1$	$q_5 = i_2 \oplus i_4 \oplus i_7$
$q_6 = i_6 \oplus i_2 \oplus i_3 \oplus i_4 \oplus i_5 \oplus 1$	$q_6 = i_0 \oplus i_3 \oplus i_5 \oplus 1$
$q_7 = i_7 \oplus i_3 \oplus i_4 \oplus i_5 \oplus i_6$	$q_7 = i_1 \oplus i_4 \oplus i_6$

Table.1 Boolean Equations for Affine Transform and Inverse Affine Transformation

2.3. Multiplicative Inverse Block

The multiplicative inversion in GF (2^8) follows the procedure shown in Figure.2.

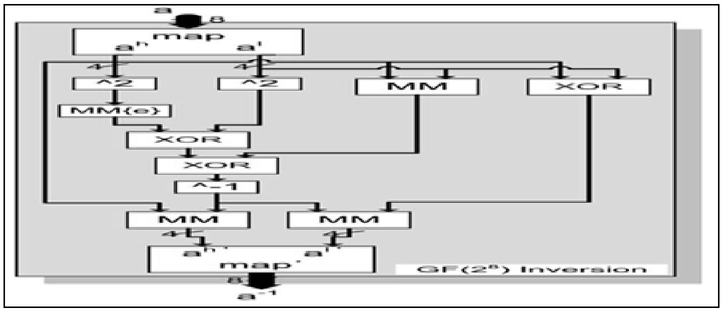


Figure. 2 Multiplicative inverse

- *Addition In GF(2^4)*
  Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation.
- *GF(2^4) Multiplier*
  Sub Bytes are a nonlinear transformation that uses 16 byte substitution tables (S-Boxes). An S-Box is the multiplicative inverse of a Galois field GF(2^4) followed by an affine transformation**.** Although two Galois Fields of the same order are isomorphic, the complexity of the field operations may heavily depend on the representations of the field elements. Composite field arithmetic can be employed to reduce the hardware complexity. Three multipliers in GF (2^4) are required as a part of finding the multiplicative inverse in GF (2^8). Figure shows the GF (2^4) multiplier circuit.

3. Screen Shots

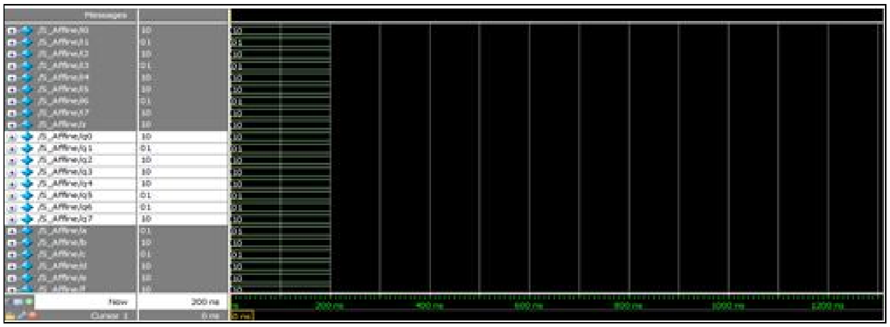


Figure.3 Affine Transformation NCL

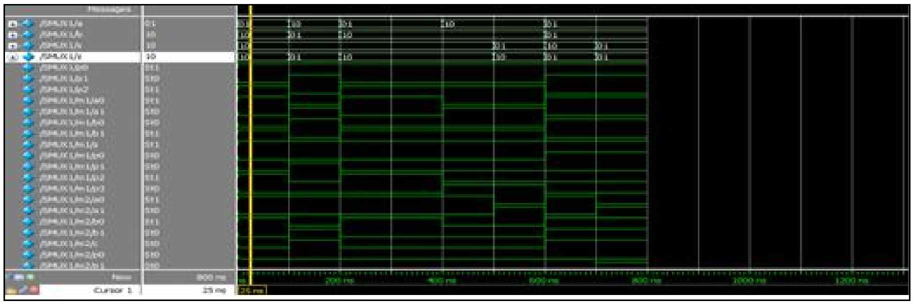


Figure.4 NCL Multiplexer

Figure.5 AES Encryption NCL

4. Conclusion

In this project, a hardware implementation of the proposed low-power SCA resistant asynchronous S-Box design for the AES cryptosystem has been revealed to be successfully resisting DPA and CPA attacks. The asynchronous S-Box design is based on self-time logic referred to as NCL, which supports beneficial properties for resisting DPA: clock free, dual-rail signal, and monotonic transitions. These beneficial properties make it difficult for an attacker to decipher secret keys embedded within the cryptographic circuit of the FPGA board. Utilizing the two FPGAs included in the SASEBO-GII board, the configuration and cryptographic functions are able to be separately performed to ensure that the power trace measurements for the analysis attacks do not interfere with each other. Experimental results of the original design against the proposed S-Box revealed that the asynchronous design decreased the amount of information leaked from both DPA and CPA attacks. Results also revealed that the proposed design showed of flatter power peaks and 22%–26% lower total power consumption during regular operation. The proposed DPA and CPA attacks procedure based on power measurement is comprehensive and general and not limited to the SASEBO-GII board. It can be revised and used for studying SCAs on other devices.

5. References

1. M.Ahn and H.Lee, “Experiments and hardware countermeasures on power analysis attacks,” in Proc. ICCSA, 2006, vol. 3982, pp. 48–53.
2. M.Alioto, L.Giancane, G.Scotti, and A.Trifiletti, “Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits,” IEEE Trans. Circuits Syst. I, Reg. Projects, vol. 57, no. 2, pp. 355–367, Feb. 2010.
3. L.Angrisani, M.D.Apuzzo and M.Vadursi, “Power measurement in digital wireless communication systems through parametric spectral estimation,” IEEE Trans. Instrum. Meas., vol. 55, no. 4, pp. 1051–1058, Aug. 2006.
4. R.Anderson, P.Cunningham, S.Moore, R.Mullins and G.Taylor, “Improving smart card security using self-timed circuits,” in Proc. 8th Int. Symp. Asynch. Circuits Syst., 2002, pp. 211–218.

5. R.Anderson, J.J.A.Fournier, S.Moore, R.Mullins and G.Taylor, “Balanced self-checking asynchronous logic for smart card applications,” J. Microprocess. Microsyst., vol. 27, pp. 421–430, 2003.
6. A.Bailey, J.Di, G.Fu, S.C.Smith and A.A.Zahrani, “Multi-threshold asynchronous circuit design for ultra-low power,” J. Low Power Electron., vol. 4, pp. 337–348, 2008.
7. A.Bogdanov, “Multiple-differential side-channel collision attacks on AES,” in Proc. CHES, 2008, pp. 30–44.
8. B.Bhaskaran, V.Satagopan, A.Singh, and S.C.Smith, “Automated energy calculation and estimation for delay-insensitive digital circuits,” Microelectron. J., vol. 38, no. 10/11, pp. 1095–1107, Oct./Nov. 2007.
9. A.Bystrov, J.P.Murphy, D.Sokolov and A.Yakovlev, “Improving the security of dual-rail circuits,” in Proc. Workshop CHES, 2004, pp. 282–297.
10. A.Bystrov, J.Murphy, D.Sokolov and A.Yakovlev, “Design and analysis of dual-rail circuits for security applications,” IEEE Trans. Comput., vol. 54, no. 4, pp. 449–460, Apr. 2005