Low-Power Side-Channel Attack-Resistant Asynchronous S-Box Design for AES Cryptosystem

H. Shree Kumar
M.Tech VLSI Design,
SRM University.

K. Suganthi
Asst. Professor(Sr.G),
SRM University

ABSTRACT

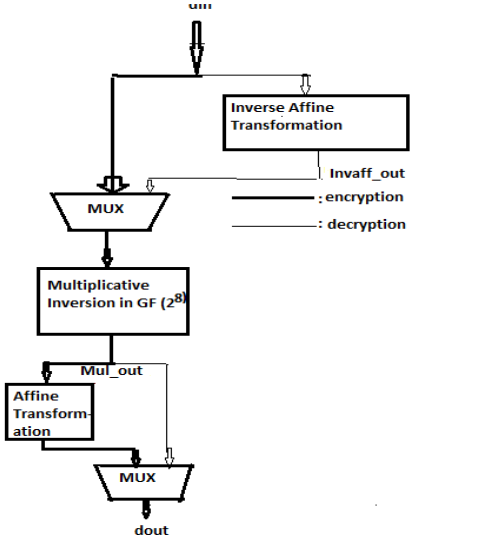
A novel asynchronous combinational S-Box (substitution box) design for AES (Advanced Encryption Standard) cryptosystems is proposed and validated. The S Box is considered as the most critical component in AES crypto-circuits since it consumes the most power and leaks the most information against side-channel attacks. The proposed design is based on a delay-insensitive logic paradigm known as Null Convention Logic (NCL). The proposed NCL

S-Box provides considerable benefits over existing designs since it consumes less power therefore suitable for energy constrained mobile crypto-applications. It also emits less noise and has flatter power peaks therefore leaks less information against side-channel attacks such as differential power/noise analysis. Functional verification, analog simulation and power measurement of NCL S-Box have been done using Mentor Graphics EDA (Electronic Design Automation) tools to assure low-power side-channel attack resistant operation of the proposed clock-free AES S-Box design.

1. INTRODUCTION

Advanced Encryption Standard (AES) [1] is a symmetric encryption algorithm based on a design principle known as a substitution-permutation network. The AES cipher is a series of transformations that convert the plaintext to cipher text by using secret keys. Each round consists of Add Round Key, Shift Rows, Mix Columns steps which are linear operations and Sub Bytes step to be non-linear. The AES algorithm's operations are performed on a two-dimensional array of bytes called the State, which consists of four columns and four rows of bytes. Sub Bytes step is the first step of AES round. Each byte in the array is updated by a 8-bit substitution box (S-Box), derived from the multiplicative inverse over GF (2^8). AES S-Box is constructed by combining the inverse function with an invertible affine transformation in order to avoid attacks based on mathematics. A block diagram of AES S-Box is shown in Fig.1 (a). In the consequent Mix Columns step, an linear transformation operates on each column of the state. The last step, Add Round key, it add a round key to the state by doing the bitwise XOR operation in an AES round .Since AES has become a FIPS standard in November 2001, various attempts of attack against the AE Shave been made. By exhaustive search, with 256-bit keys, 2256 possibilities must be checked, which lead apparent impossibility of attacks under such method. However, side-channel attacks have been proved to successfully attack the AES. Published side-channel attacks include simple power analysis (SPA) attack and differential power analysis (DPA) attack [2], which attack the cryptosystem that inadvertently leak information about the operations they process. DPA attacks are proven to be substantially effective to either directly reveal the hidden private key or significantly reduce key search space for faster and feasible exhaustive search. During these years, various countermeasures of resisting Side-channel analysis attacks have been proposed, including Software-based and hardware-based methods. The hardware Implementation of the AES essentially has higher reliability than software since it is difficult to be read or modified by the attackers and less prone to reverse engineering. The goal of countermeasures against DPA attacks is to reduce or balance the power consumption. For example, one can insert addition noise to interference the power [4], insert the random delays [6], static complementary CMOS logic [3], or the masked logic. However, these methods cannot prevent DPA attacks completely because of the power leakage of CMOS circuit [7]. Dual-rail method is the most promising logic style among many countermeasures. Sense Amplifier Based Logic (SABL) [3], Wave dynamic differential logic (WDDL) [4] and Masked Dual-rail pre-charged Logic (MDPL) [5] are all based on dual-rail logic. The benefit of dual-rail logic is that the constant power consumption can be achieved since the signals are implemented by two complementary wires. The downside is dual-rail method generally increase the area and time delay [9]. Another good countermeasure is using asynchronous logic, [8] presents that the power dissipated is independent of the input data in asynchronous logic. In this article, we propose an asynchronous AES S-Box based on a Null Convention Logic (NCL) [9], which matches the two important properties mentioned above; dual-rail encoding and clock-free operation. It is intended to achieve low power consumption for mobile applications and considerable resistance against side-channel attacks such as DPA

(a)



(b)

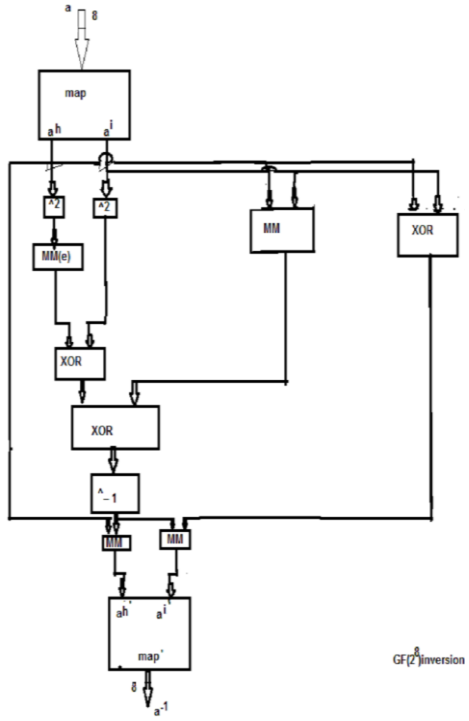


Fig 1: (a) Combinational S-Box architecture with encryption and decryption data paths. (b) Block diagram of multiplicative inversion over the *GF*(28) component, where *MM* is modular multiplication and XOR is EXCLUSIVEOR operation

The downside is dual-rail method generally increase the area and time delay [5]. Another good countermeasure is using asynchronous logic, [3] presents that the power dissipated is independent of the input data in asynchronous logic. In this article, we propose an asynchronous AES S-Box based on a Null Convention Logic (NCL) [4], which matches the two important properties mentioned above; dual-rail encoding and clock-free operation. It is intended to achieve low power consumption for mobile applications and considerable resistance against side-channel attacks such as DPA.

2. SCA VULNERABILITY OF AES S-BOX AND EXISTING COUNTER MEASURES

Differential power analysis (DPA) is a type of side-channel attacks. DPA attack can extract secret keys through statistically analyzing power consumption measurements from a cryptosystem [2]. To do the DPA attack, normally attackers would do the following steps: (1) collect the power consumption measurements from the encrypted device with random inputs; (2) classify the collected results by using decision function; (3) redo (1) with a hypothetical key; (4) sort the results to the existing sets; (5) do the average power calculation in each sets; (6) compare different results until find the correct key. If the hypothetical key is the real key, it can be identified by a obviously spikes in the differential traces. Otherwise, the key is incorrect. In the Sub Bytes operation, S-Box is the most critical component, as it determines the power consumption and throughput of not only the Sub Bytes operation but also the AES hardware implementation. Therefore, in this work, our research is focus on the S-Box design.

3. ASYNCHRONOUS AES S-BOX DESIGN

Asynchronous clock less circuits require less power, generate less noise and produce less electro-magnetic interference compared to their synchronous counterparts. Null Convention Logic (NCL) is a delay-insensitive logic which belongs to the asynchronous circuit's categories. NCL circuit utilizes dual-rail and quad-rail logic to achieve this delay insensitivity [9]. A dual-rail signal can represent one of available three states, DATA0, DATA1 and NULL, which corresponds to Boolean logic 0 (i.e., DATA0), Boolean logic 1(i.e., DATA1) and control signal NULL for asynchronous handshaking, respectively. In order to achieve clock-free operation, two delay-insensitive registers on both sides of the combinational NCL circuit with local handshaking signals are needed. In this research, dual-rail signals substitutes for corresponding conventional Binary signals in the NCL AES S-Box The AES S-Box algorithm adapted in this research follows the combinational logic circuit architecture.The affine transformation and inverse affine transformation Components follow a series of Boolean equations given in Table 1. As shown in the table, the affine transformation and inverse affine transformation components require 16 and 12 XOR gates, respectively. The multiplicative inversion in GF(28) follows the procedure shown in Figure 1(b). Map, square, multiplication operations also require significant amount of XOR gates of which the sum is 95. To convert the conventional S-Box into NCL, replacing the Boolean XOR and AND operation into a dual-rail NCL gate is required. Besides a series of XOR gates with AND gates, two NCL multiplexers are needed for switching between encryption and decryption process. Unlike Boolean logic, NCL has 27 Fundamental threshold gates [9] to realize arbitrary logic. In order to achieve the input-completeness and observability, it is important to choose

TABLE 1: Boolean Equation for Affine Transformation and Inverse Affine Transformation components.

Q = aff_trans(i)	**Q = aff_trans^{-1}(i)**

$Q_0=(i_0 \circledR i_4) \circledR (i5+i6) \circledR (i7 \circledR 1)$	$Q_0 = i_2 \circledR i5 \circledR i7 \circledR 1$
$Q_1 = i_1 \circledR i_5 \circledR i6 \circledR i7 \circledR i0 \circledR 1$	$Q_1 = i_0 \circledR i_3 \circledR i6$
$Q_2= i_2 \circledR i_6 \circledR i7 \circledR i0 \circledR i1$	$Q_2= i_1 \circledR i_4 \circledR i7 \circledR 1$
$Q_3= i_3 \circledR i_7 \circledR i0 \circledR i1 \circledR i2$	$Q_3= i_2 \circledR i_5 \circledR i0$
$Q_4= i_3 \circledR i_7 \circledR i0 \circledR i1 \circledR i2$	$Q_4= i_1 \circledR i_3 \circledR i6$
$Q_5= i_1 \circledR i_5 \circledR i2 \circledR i3 \circledR i4 \circledR 1$	$Q_5= i_2 \circledR i_4 \circledR i7$
$Q_6= i_6 \circledR i_2 \circledR i3 \circledR i4 \circledR i5 \circledR 1$	$Q_6= i_0 \circledR i_3 \circledR i5 \circledR 1$
$Q_7= i_7 \circledR i_3 \circledR i4 \circledR i5 \circledR i6$	$Q_7= i_1 \circledR i_4 \circledR i6$

appropriate threshold gates. For example, in the design of a 2:1 multiplexer, according to the Karnaugh map in Figure. 3(a), the sum-of-product (SOP) functions can be simplified as follows:

Z0 = A0S0 + S1B0; (1)

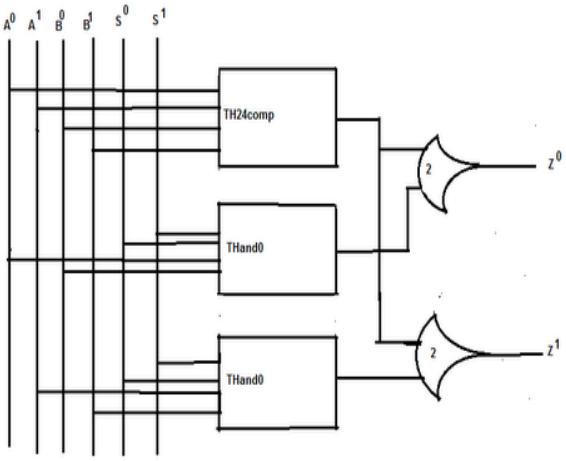
Z1 = A1S0 + S1B1; (2)

After modifying both functions for input completeness, new SOP functions are obtained as follows:

Z0 = A0S0 (A0 +A1)(B0 +B1)+S1B0(A0 +A1)(B0 +B1);(3)

Z1 = A1S0 (A0 +A1)(B0 +B1)+S1B1(A0 +A1)(B0 +B1);(4)

(a)



) Optimized NCL multiplexer

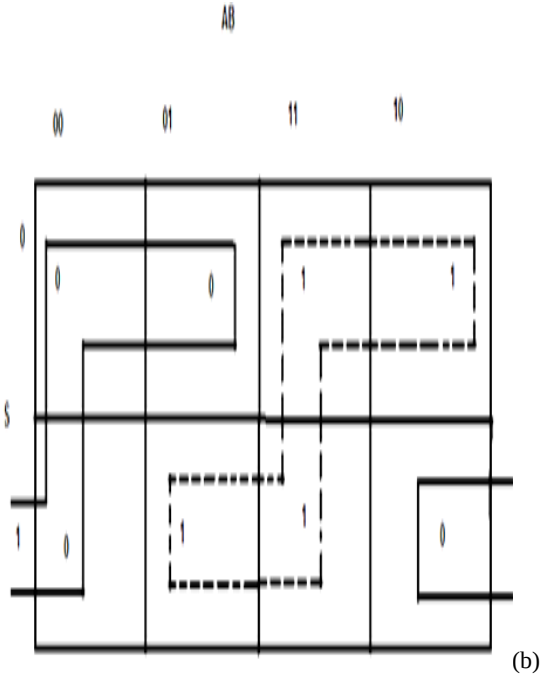
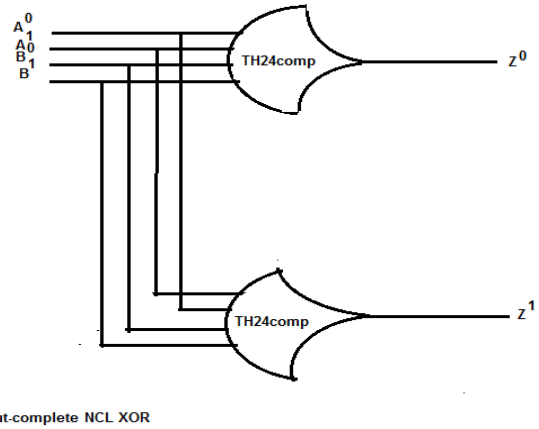


Fig. 2.: (a) Optimized NCL multiplexer.(b) K-map for the NCL multiplexer



---->> Input-complete NCL XOR

In NCL, each NCL combinational logic block should be bracketed by input and output registrations to alternate a NULL wave front and DATA wave front to achieve delay insensitivity. Since two consecutive DATA wave fronts are separated by a NULL wave front, a reference clocking signal is not needed. Each NCL register has a single bit Ko(i.e., output acknowledgement signal) and Ki (i.e., input acknowledgement signal) signals which alternate between 0 and 1, defined as request for null (i.e., rfn) and request for data (i.e., rfd), respectively. Timing is locally handled

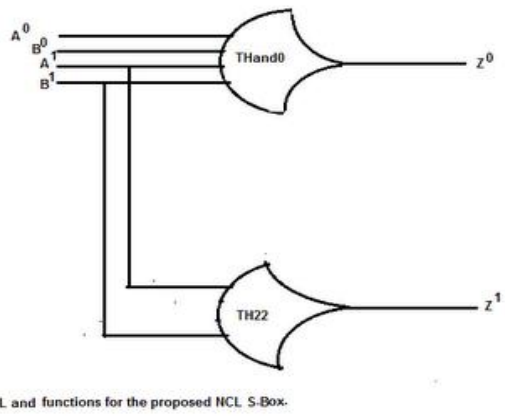


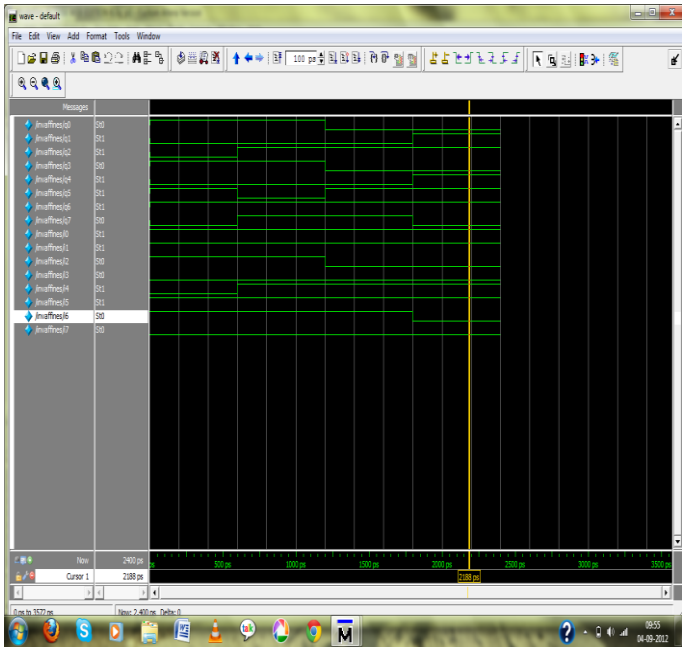
Fig. 3: Input-complete NCL XOR and NCL AND functions for the proposed NCL S-Box.

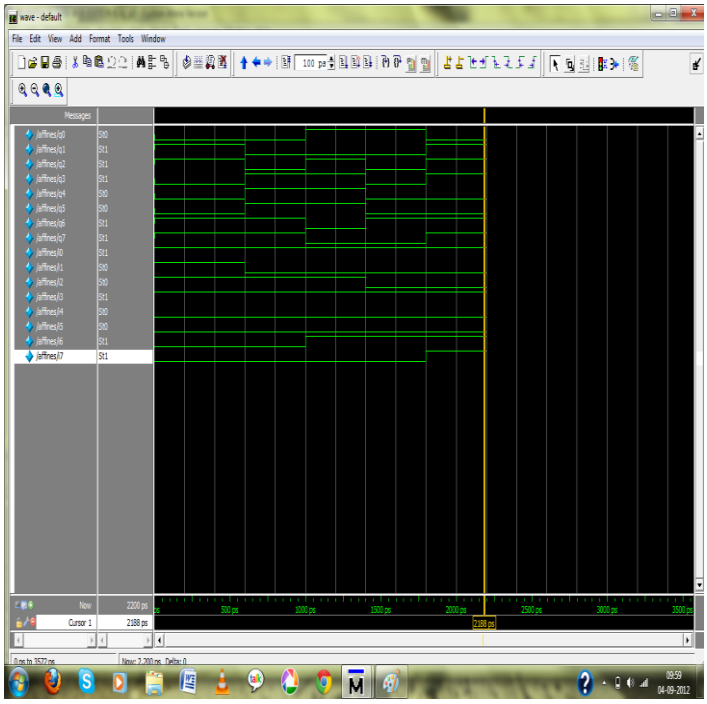
by this delay-insensitive hand-shaking protocol. In the completion detection component, the Ko signals are gathered and they are operated through an cascade of AND gates where output is set to Ki of the previous register, determining the state of current operation. Notably, the proposed NCL S-Box design shown in Figure 2 is free from glitches. Two possible transitions, NULL-to-DATA and DATA-to-NULL are monotonic and glitch-free since only 0 " 1 wire transitions are possible for NULL-to-DATA cycle and 1 " 0 wire transitions for DATA-to-NULL cycle, respectively. Therefore, the proposed NCL S-Box is completely immune to side-channel attacks based on glitch power/noise measurements.

4. FUNCTIONAL VERIFICATION OF THE S-BOX DESIGN

The simulation result of each part of the S-Box is shown below using Modelsim..

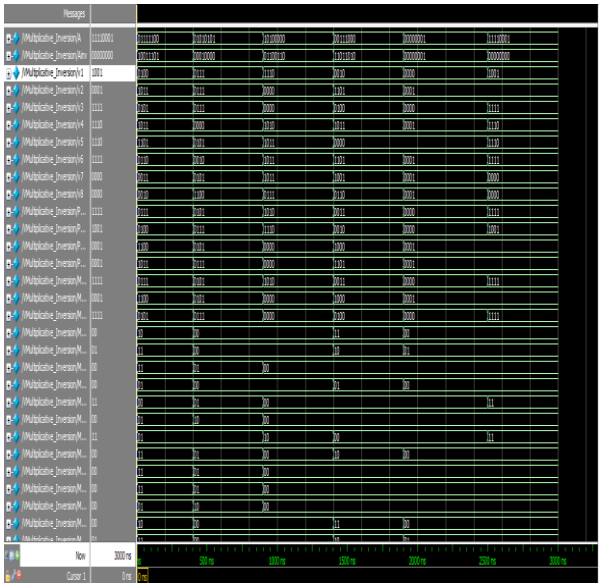
4.1 AFFINE TRANSFORM AND INVERSE AFFINE TRANSFORMATION





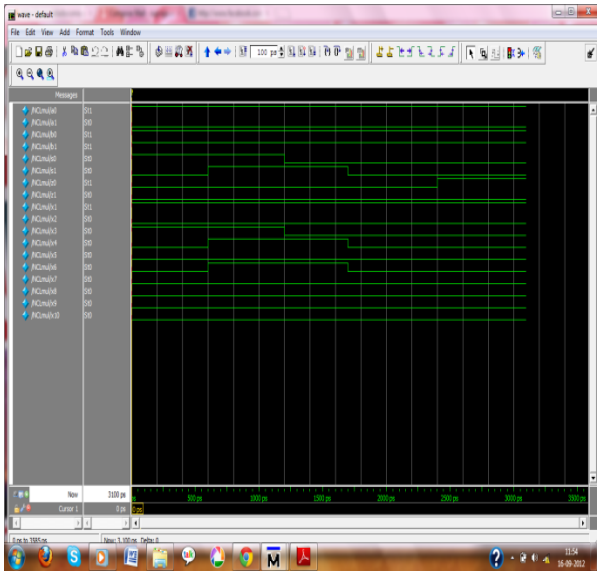
The affine transformation and inverse affine transformation components follow a series of Boolean equations 8-bit input and output, respectively. Both transformations require many XOR gates. We have carried out the Affine and inverse affine transformation using Verilog.

4.2. THE MULTIPLICATIVE INVERSE IN GF (2^8) IS



First, map operation converts the 8-bit input into elements of GF (2^4) (i.e., a^h and a^l).Then, calculate the square of a^h and a^l. It should be noticed that multiplication in GF (2^4) is done by multiplying the polynomial $a^h(x)$ $a^h(x)$ followed by a modular reduction. Lastly, a series of multiplication and XOR operations were implemented to extend the field GF (2^4) to the field GF (2^8).

4.3 NCL MULTIPLEXER



In the design of a 2:1 multiplexer, according to the Karnaugh map, the sum-of-product (SOP) functions can be simplified as follows.

$Z^0 = A^0S^0 + S^1B^0$

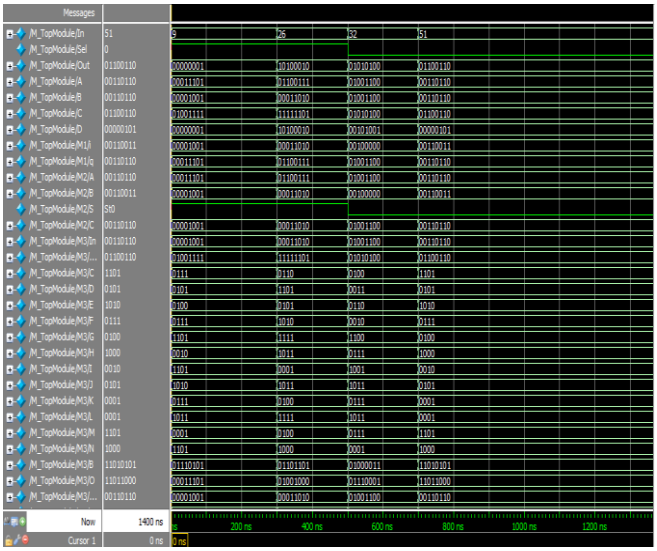
$Z^1 = A^1S^0 + S^1B^1$

After modifying both functions for input completeness, new SOP functions are obtained as follows:

$$\mathbf{Z^0 = A^0 S^0 (A^0 + A^1) (B^0 + B^1) + S^1 B^0 (A^0 + A^1) (B^0 + B^1)}$$

$$\mathbf{Z^1 = A^1 S^0 (A^0 + A^1) (B^0 + B^1) + S^1 B^1 (A^0 + A^1) (B^0 + B^1)}$$

After connecting all the blocks we obtained the S-BOX with its simulation results given below



4.4 SIMULATION RESULT

Mode	Input	S-BOX Output
Encrypt	9 26 106	00000001 10100010 00000010
Decrypt	32 51 156	01010100 01100110 00011100

5.CONCLUSION AND FUTURE ENHANCEMENT

Our future enhancement is to implement the S-box in AES (Advanced Encryption Standard).I will also implement all the blocks in NCL which will make the whole system more secure and power efficient. Here we encrypt the image or data by AES with the help of our S-box. The input of AES is image or data pixels, which consist of 4x4 image or 128 bit applied to the both test and reference circuit. For encryption a specific key is required, in this encrypt key also we use 4x4 key or 128 bit data which makes the better performance of the AES.We will then calculate the relative power analysis of both the existing and then the proposed design using X Power tool in Xilinx 13.1 and then Micro win for more accuracy. The proposed system will have beneficial properties make it difficult for an attacker to decipher secret keys embedded within the cryptographic circuit of the FPGA board. Lower total power consumption during regular operation as well as lesser area is required for the whole implementation.

6. REFERENCES

[1] NIST,"Advanced Encryption Standard (AES), FIPSPUBS 197, National Institute of Standards and Technology", NIST, Nov 2001

[2] P. Kocher, J. Jaffe and B. Jun, "Introduction to differential power analysis and related attacks", Technical Report, Cryptography Research Inc., San Francisco, California, 1998.

[3] S. Moore, R. Anderson, P. Cunningham, R. Mullins and G. Taylor, "Improving smart card security using self-

time circuits", Proceeding of Eighth International Symposium on Asynchronous Circuits and System, pp. 211-218, IEEE Computer Society, 2002.

[4] S. C. Smith and J. Di, "Designing Asynchronous Circuits using NULL Convention Logic", Synthesis Lectures on Digital Circuits and Systems, Vol. 4/1, July 2009

[5] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P.Schaumont, and I. Verbauwhede"Prototype IC with WDDL and Differential Routing - DPA Resistance Assessment", Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), LNCS, vol. 3659, pp. 354-365, Aug 2005

[6] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully Attacking Masked AES Hardware Implementations", Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), LNCS, vol. 3659, pp. 157-171, Aug 2005

[7] W. Johannes, O. Elisabeth and L. Mario, "An ASIC Implementation of the AES SBoxes", Topics in cryptology, CT-RSA 2002, LNCS, Vol. 2271, pp. 29-52, Jan 2002

[8] K. Fant and S. Brandt, "NULL Convention Logic: A Complete and Consistent Logic for Asynchronous Digital Circuit Synthesis", International Conference on Application Specific Systems, Architectures, and Processors, pp. 261-273, 1996

[9] V. Satagopan, B. Bhaskaran, A. Singh, S.C. Smith," Automated energy calculation and estimation for delay-insensitive digital circuits," Elsevier's Microelectronics Journal, Vol 38/10-11, pp. 1095-1107, Oct/Nov 2007