ISSN: 2277-9655
Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Low Power Counter Measure for Cryptographic Applications using Asynchronous S-Box

Shri Suvega.M.R[*1], Muralidharan.J[2]
[*1] PG Scholar,Dept of ECE,Akshaya College of Engineering and Technology,Coimbatore, India
[2] Assistant professor,Dept of ECE,Karpagam University,Coimbatore, India
shrisuvega1991@gmail.com

Abstract

In this work, a novel asynchronous combinational S-Box (substitution box) design for AES (Advanced Encryption Standard) cryptosystems is projected and validated. The S-Box is examined because the final vital component in AES crypto-circuits since it employs the foremost power and leaks the most information contrary to side-channel attacks. The proposed technique is based on a delay-insensitive logic paradigm referred to as Null Conventional Logic (NCL).The projected NCL S-Box provides vast benefits over existing designs since it consumes less power therefore suited for energy control mobile crypto-applications. It also emits less noise and has blandish power peaks therefore leaks less information against side-channel attacks such as differential power/noise analysis. Functional verification and power measurement of NCL S-Box have been done using Mentor Graphics EDA (Electronic Design Automation) tool to assure low-power side-channel attack-resistant operation of the proposed AES asynchronous S-Box design.

Keyword : Advanced Encryption Standard (AES); Null Convention Logic (NCL); Power measurement; Substitution Box(S-Box).

Introduction

Most modern cryptographic devices are engaged using semiconductor logic gates, which are made out of transistors. The impending of the crypto hardware devices and its algorithms are a framework of modern digital information systems which handles the crisis for data security,verification and vulnerable information.The crypto hardware is exposed to plenty of attacks which precise the physical properties of their aiding.Security is materialized as a development of chief importance.This is the particular truth for the embedded system due to several clear cut security challenges. Cryptography is the best and sufficient solution for these challenges which counterclaims to encode digital information while being energy efficient are in high demand. The novelty for such devices is accessible in today's mobile phones, portable devices and network security. The aim to reach this demand of low-power devices with development security features, researchers examine the cryptographic algorithm. The cryptographic algorithm transforms plain text information into cipher text with additional secret cipher key.The algorithm is an expansion way to inspect the plain text from cipher text without the explicit knowledge of the cipher key. The security is equipped by the algorithm which is equal to its capacity to safe the cipher key. The cryptosystems output consolidate execution timing, power consumption, electromagnetic leaks and also thermal or acoustic emancipation [1]. All these information sources are known as side channels. Such side channel attack exploits power consumption of the device during prediction to derive the secret key. These side channel attacks are known as Differential Power Analysis (DPA) attacks. Among side channels attacks DPA is maximum dominant.DPA attack can mention secret keys through numerically analyzing power consumption measurements from a cryptosystems [15].

Since AES have become a FIPS standard in November 2001, various attempts of attack against the AES have been made. By extensive search, with 256-bit keys, 2^{256} possibilities must be monitored, which lead likely impossibility of attacks under such method.Advanced Encryption Standard (AES) is a symmetric encryption algorithm with the motive of being a faster and more secure encryption algorithm for past years. The AES cipher converts the plain text 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.

Sub Bytes step is the first step of AES round. Each byte in the array is renewed by a 8-bit substitution box (S-Box), which is derived from the multiplicative inverse over GF (2^8). In the sub bytes operation, S-box is the utmost critical component, as it regulates the power consumption and throughput of not only the sub bytes operation further the AES hardware implementation[20]. The distinct peaks of the DPA trace occur to be closely related to first add round key operation and sub bytes operation.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 Figure.1 (a).In the Mix Columns step, a linear transformation operates on each column of the state.The last step, Add Round Key, it adds a round key to the state by doing the bitwise XOR operation in an AES round.

During these years, various counter measures of resisting side-channel analysis attacks have been proposed, including software and hardware-based methods. The intension of remedy against DPA attacks is to reduce or equity the power consumption. For example, one can inject the random delays or the masked logic. These methods cannot block DPA attacks completely because of the power leakage of CMOS circuit. Dual-rail method is the most promising logic style among many countermeasures[5]. Sense Amplified Based Logic (SABL) [3], Wave dynamic differential logic (MDPL) are all based on Dual-rail logic [6]. The aid 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 normally increase the area and time fall off [5]. Another good countermeasure is using asynchronous logic, presents that the power dissipated is independent of the input data in asynchronous logic. The proposed work is an asynchronous AES S-Box based on a Null Conventional Logic 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.

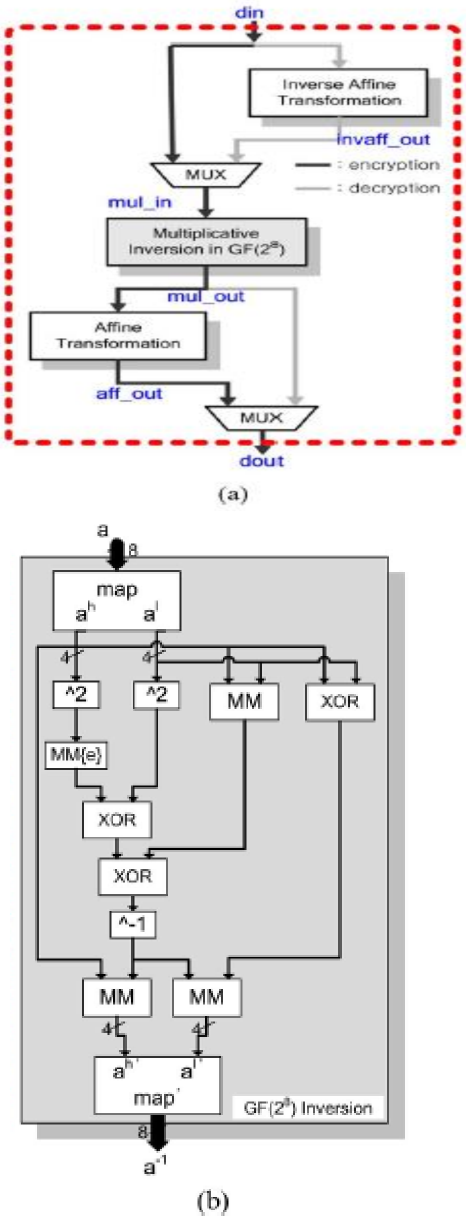


Fig.1.(a) Combinational s-box architecture with encryption and decryption datapaths; (b) Block diagram of multiplicative inversion over GF(2^8) component where MM is modular multiplication and XOR is Exclusive-OR operation [3].

NCL Overview

NCL is a self-timed logic paradigm in which control is in-herent in each datum.NCL follows the so-called conditions of Seitz's delay-insensitive signaling scheme. Like related delay-insensitive logic methods the NCL paradigm assumes that forks in wires are isochronic. Various conditions of the paradigm, including the NULL logic state from which NCL extract its name, have origins in Muller's work on speed-independent circuits in the 1950's and 1969's.

A. Delay Insensitivity

NCL utilizes symbolic completeness of expression to achieve delay- insensitive behavior. A symbolically complete expression depends only on the relationships of the symbols present in the expression without reference to their time of estimation. In particular, dual-rail and quad-rail signals, or other mutually exclusive affirmation groups can incorporate data and control information into one mixed-signal path to eliminate time reference.

For NCL and other circuits to be delay insensitive, assuming isochoric wire forks, they must meet the input completeness and observability criteria. Completeness of input requiresthst all the outputs of a combinational circuit may not transition from NULL to DATA until all inputs have transitioned from NULL to DATA, and thet all the outputs of a combinational circuit may not transition from DATA to NULL until all inputs have transitioned from DATA to NULL.In circuits with various outputs,it is tolerable, according to Seitz's weak conditions, for some of the outputs to transition without having a complete input set present,since all outputs cannot transition before all inputs arrive.Observability requires that no orphans may propagate through a gate. An orphan is defined as a wire that change over during the current DATA wavefront,but is not used in the decision of the output. Orphans are caused by wire forks and can be ignored through the isochronic fork guess,since they are not allowed to access to cross gate boundary. This observability condition is indicated as stability,assure that every gate transitions is necessary to transition at least one of the outputs. The observability condition can be flexible through orphan analysis and still achieve self-timed behavior; however, this requires some delay analysis. Furthermore, when circuits use the bit-wise completion strategy with selective input incomplete components, they must also adhere to the completion completeness criterion, which requires that completion signals only be generated such that no two adjacent DATA wave fronts can interact within any combinational component.

Maximum multirail delay insensitive systems including NCL have at least two register stages, one at both the input and the output. Two neighbouring register stages interact through request and acknowledge lines k_o and k_i respectively, to prevent the current DATA wave front from overwriting the previous DATA wave front by ensuring that the two are separated by a NULL wave front.

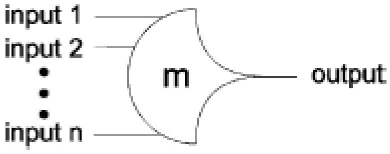


Fig. 2 THmn threshold gate.

B.Logic Gates

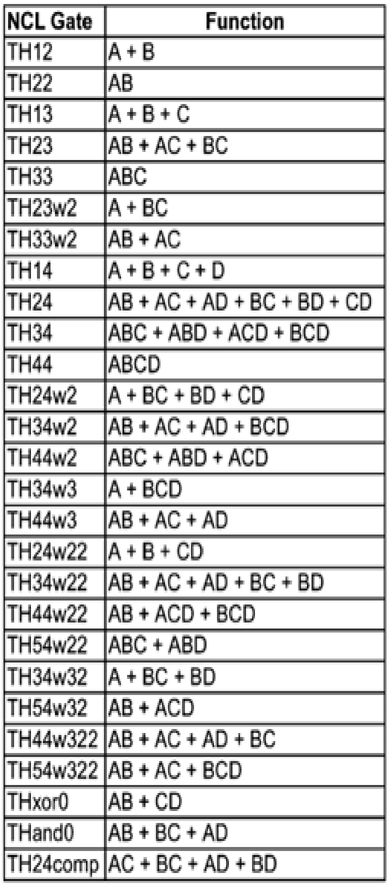
NCL differs from other delay insensitive paradigms, which use only individual type of state holding gate, the c-element. A c-element behaves as follows: when all inputs assume the same value, the output assumes this value;if not the output is not changed. On the supplementary hand,all NCL gates are state holding.NCL utilizes threshold gates as its basic logic elements. The elementary type of threshold gate shown in Figure 2 is the THmn gate, where .THmn gates have n single-wire inputs, where partially m of the n inputs must be asserted before the single-wire output will be declared. NCL threshold gates are described with hysteresis state holding capability, such that all asserted inputs must be de-asserted before the output will be deasserted.Hysteresis ensures a complete transition of inputs back to NULL before asserting the output associated with the next wave front of input data.NCL threshold gates may also include a reset input to initialize their output. Circuit diagrams label the resettable gates by either a D or an N appearing inside the gate, along with gate's threshold denotes the gate as being reset to 1, and N to logic 0.

.

Asynchronous AES S-Box Design

Asynchronous clockless circuits require limited power, generate less noise and produce fewer 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 in-sensitivity. A dual-rail signal can represent one of available three states, DATA0, DATA1 and NULL, which corresponds to Boolean value 0 (i.e., DATA0), Boolean value 1 (i.e., DATA1) and control signal NULL for asynchronous handshaking,correspondingly. In order to bring out clock free operation, two delay in-sensitive 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.

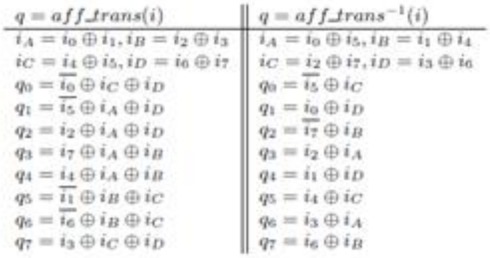
TABLE 1 : 27 FUNDAMENTAL NCL GATES



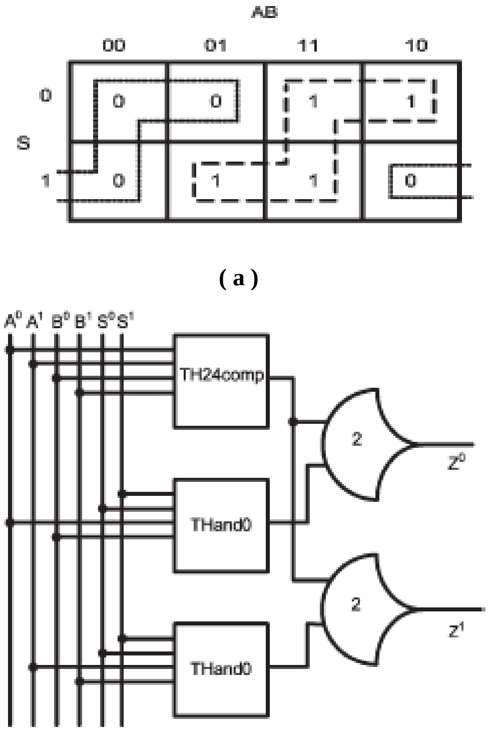
NCL Gate	Function
TH12	A + B
TH22	AB
TH13	A + B + C
TH23	AB + AC + BC
TH33	ABC
TH23w2	A + BC
TH33w2	AB + AC
TH14	A + B + C + D
TH24	AB + AC + AD + BC + BD + CD
TH34	ABC + ABD + ACD + BCD
TH44	ABCD
TH24w2	A + BC + BD + CD
TH34w2	AB + AC + AD + BCD
TH44w2	ABC + ABD + ACD
TH34w3	A + BCD
TH44w3	AB + AC + AD
TH24w22	A + B + CD
TH34w22	AB + AC + AD + BC + BD
TH44w22	AB + ACD + BCD
TH54w22	ABC + ABD
TH34w32	A + BC + BD
TH54w32	AB + ACD
TH44w322	AB + AC + AD + BC
TH54w322	AB + AC + BCD
THxor0	AB + CD
THand0	AB + BC + AD
TH24comp	AC + BC + AD + BD

The AES S-Box algorithm adapted in this research follows the combinational logic circuit architecture presented in [3].The affine transformation and inverse affine transformation components follow a series of Boolean equations given in table 2. As demonstrated in the Table 2, the affine transformation and inverse transformation components require 16 and 12 XOR gates, subsequently.

Table 2: boolean equations for affine transformation and inverse affine transformation components [19].



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



(a)

(b)

Fig.3. (a) K-map for NCL Multiplexer; (b) Optimized NCL Multiplexer [19].

The multiplicative inversion in GF (2^8) follows the procedure shown in Fig 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.Likewise a series of XOR gates with AND gates,two NCL multiplexers are desided for switching between encryption and decryption process. Unlike Boolean logic, NCL has 27 elementary threshold gates and it is important to choose convenient threshold gates. For example, in the case of designing a 2:1 multiplexer, according to the Karmaugh map in figure, 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 revising both functions for input-completeness, new Sum Of Product functions are obtained as follows,

$$Z^0 = A^0S^0(A^0 + A^1)(B^0 + B^1) + S^1B^0(A^0 + A^1)(B^0 + B^1);$$

$$Z^1 = A^1S^0(A^0 + A^1)(B^0 + B^1) + S^1B^1(A^0 + A^1)(B^0 + B^1);$$

Both of them can be mapped to a NCL circuit with a TH24comp gate, a THand0 gate and a TH22 gate. The finalized NCL MUX logic diagram is shown in Fig 3(b).

Additionally, OR function and AND function can also be realized by threshold gates. An input-complete XOR logic is profiled to two TH24comp gates. An input-entire AND logic is concluded to a THand0 and a TH22 gate. The completed NCL XOR and AND logic diagrams are as shown in Fig 4 and Fig 5.

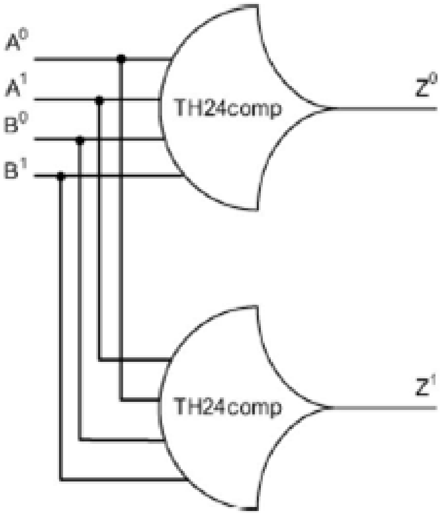


Fig. 4. Input-complete NCL, XOR function for the proposed NCL S-Box.

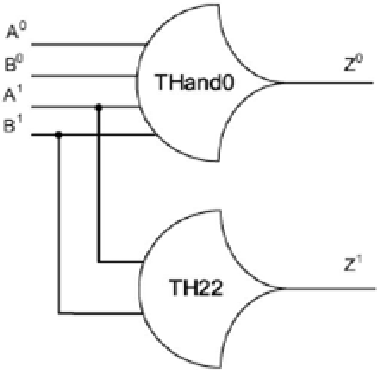


Fig.5. Input-complete NCL, AND function for the proposed NCL S-Box

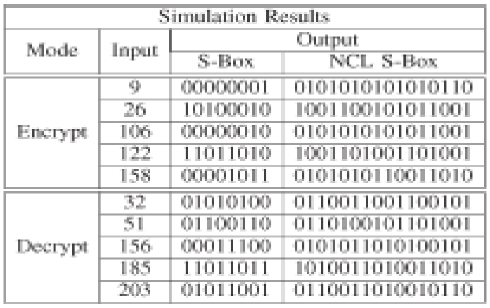
Functional Verification Of The Proposed Ncl S-Box Design

VHDL is used as a Hardware Description Language because of its flexibility to exchange among surroundings. The proposed NCL S-Box has been implemented using VHDL and simulated with ModelSim by Mentor Graphics. In order to realize more complex operation,Fibonacci LFSR (Linear Feedback Shift Register) is used as a counter measure circuit and it is a shift register, when clocked moves the signal through the register from one bit to the next most significant bit.The bit position that affects the next state is called taps and from right most bit output is taken.The plain text is given as input to the Fibonacci LFSR. The output of the Fibonacci LFSR convey its output to the asynchronous S-Box as its input, to make it not easy to estimate the count series. The outcome product of asynchronous S-Box is analyzed and is shown as waveform in Figure 6.

By referring the waveform displayed on Figure 6, the fundamental value of the input is NULL and output is DATA 0,correspondingly,as previously input register is reset to NULL and output register is reset to DATA.Instantly reset falls down to 0, k_o in distinction to the output register becomes 1 and k_o for the input register connected to k_o becomes 1.As k_i increases, the input is replaced to the waiting input signal, 0101010101011001 in dual-rail signaling which means 00000010 in Binary As every bit of the output signal changes to DATA0 or DATA1 from NULL, k_o falls to 0 which means the output register has received the proper output DATA wave.

Table 3 shows the encryption and decryption simulation results for 10 arbitrary sample inputs, 5 for encryption and 5 for decryption,respectively.On the NCL S-Box output list, the results are shown as 16 bits, which are the dual-rail signals.For example, for input 185, the NCL S-Box output is 1010011010011010 in Binary which matches to the output of the synchronous S-Box.

Table 3. Simulation results for 20 arbitrary samples from conventional synchronous s-box and the proposed ncl s-box.



Simulation Results			
Mode	Input	Output	
		S-Box	NCL S-Box
Encrypt	9	00000001	0101010101010110
	26	10100010	1001100101011001
	106	00000010	0101010101011001
	122	11011010	1001101001101001
	158	00001011	0101010110011010
Decrypt	32	01010100	0110011001100101
	51	01100110	0110100101101001
	156	00011100	0101011010100101
	185	11011011	1010011010011010
	203	01011001	0110011010010110

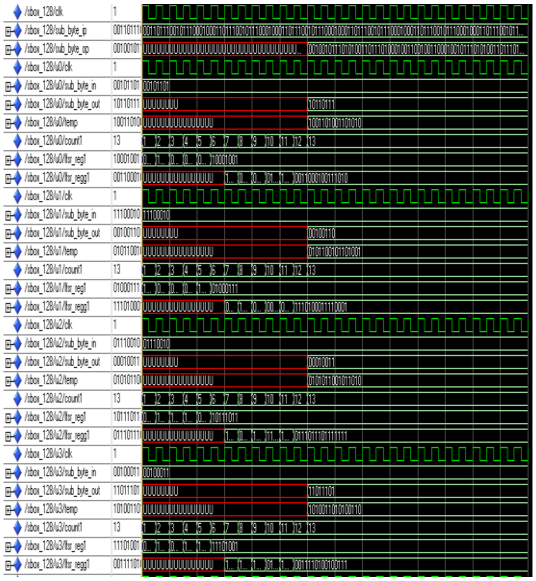

/sbox_128/clk 1
/sbox_128/sub_byte_ip 00110111
/sbox_128/sub_byte_op 00100101
/sbox_128/u0/clk 1
/sbox_128/u0/sub_byte_in 00101101
/sbox_128/u0/sub_byte_out 10110111
/sbox_128/u0/temp 10011010
/sbox_128/u0/count1 13
/sbox_128/u0/lfsr_reg1 10001001
/sbox_128/u0/lfsr_regg1 00110001
/sbox_128/u1/clk 1
/sbox_128/u1/sub_byte_in 11100010
/sbox_128/u1/sub_byte_out 00100110
/sbox_128/u1/temp 01011001
/sbox_128/u1/count1 13
/sbox_128/u1/lfsr_reg1 01000111
/sbox_128/u1/lfsr_regg1 11101000
/sbox_128/u2/clk 1
/sbox_128/u2/sub_byte_in 01110010
/sbox_128/u2/sub_byte_out 00010011
/sbox_128/u2/temp 01010110
/sbox_128/u2/count1 13
/sbox_128/u2/lfsr_reg1 10111011
/sbox_128/u2/lfsr_regg1 01110111
/sbox_128/u3/clk 1
/sbox_128/u3/sub_byte_in 00100011
/sbox_128/u3/sub_byte_out 11011101
/sbox_128/u3/temp 10100110
/sbox_128/u3/count1 13
/sbox_128/u3/lfsr_reg1 11101001
/sbox_128/u3/lfsr_regg1 00111101

Fig. 6. Mentor Graphics ModelSim waveform for the proposed NCL S-Box

Power Consumption Simulation And Comparison

After the functional verification, the VHDL code has been compiled and its power measurements are executed using XILINX ISE simulation tool. The Power measurement results from XILINX ISE simulator for the proposed NCL S-Box and conventional synchronous S-Box are shown in Figure 7.As Figure 7 shows the proposed NCL S-Box has 161 mW and conventional synchronous S-Box has 174 mW for Temperature about 27 degree Celsius.

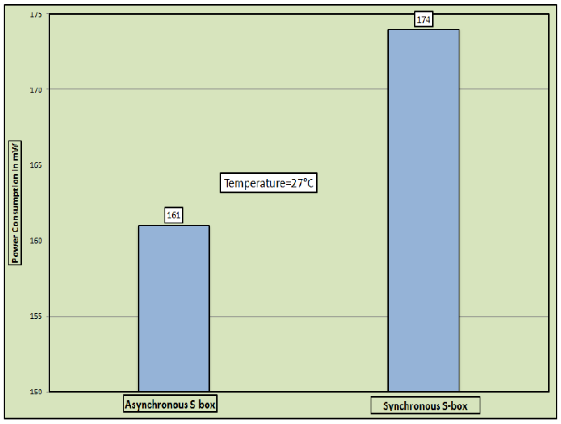


Fig.7. Total estimated power consumption.

Conclusion

A new asynchronous combinational S-Box design for AES cryptosystems has been planned and validated in this work. The proposed S-Box design is based on a delay-insensitive logic paradigm known as Null Convention Logic (NCL) and achieves improved low power operation and DPA-resistance over its clocked counterpart. The proposed NCL AES S-Box has been implemented in VHDL and simulated with Mentor Graphics EDA tool set. Various tools including ModelSim, Accusim, DesignArchitect-IC, Eldo and AdvanceMS have been used to perform functional verification, low–power application and DPA-resistance. The proposed design has been compared with the existing synchronous combinational logic AES S-Box design and both reduced power consumption and improved DPA-resistance has been verified.

References

[1] *J. Kocher, P. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," Cryptography Res. Inc., San Francisco, CA, 1998, Tech. Rep.*

[2] *J.-S. Coron, "Resistance against differential power analysis for Elliptic Curve cryptosystems," in Proc. 1st Int. Workshop CHES, 1999,pp. 292–302.*

[3] *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.*

[4] *K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", 28th European Solid-State Circuits Conference, 2002*

[5] *K. Tiri and I. Verbauwhede, "Securing encryption algorithms against DPA at the logic level: Next generation smart card technology," in Proc.Workshop CHES, 2003, pp. 125–136.*

[6] *D. Sokolov, J. P. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," in Proc. Workshop CHES, 2004,pp. 282–297.*

[7] *K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant asic or FPGA implementation," in Proc. Des., Autom. Test Eur. Conf. Exhib., Feb. 2004, vol. 1, pp. 246–251.*

[8] *P. Kocher, "Design and validation strategies for obtaining assurance in Countermeasures to power analysis and related attacks," in Proc. NIST Phys. Security Workshop, 2005, pp. 1–11.*

[9] *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

[10]D. Macii and D. Petri, “Accurate software-related average current drain measurements in embedded systems,” IEEE Trans. Instrum. Meas.,vol. 56, no. 3, pp. 723–730, Jun. 2007.

[11]Y. Han, X. Zou, Z. Liu, and Y. Chen, “Improved differential power Analysis attacks on AES hardware implementations,” in Proc. Int. Conf. Wireless Commun. Netw. Mobile Comput. Sep. 2007, pp. 2230–2233.

[12]J. Hunsinger and B. Serio, “FPGA implementation of a digital sequential phase-shift stroboscope for in-plane vibration measurements with sub pixel accuracy,” IEEE Trans. Instrum. Meas., vol. 57, no. 9, pp. 2005–2011, Sep. 2008.

[13]A. Bogdanov, “Multiple-differential side-channel collision attacks on AES,” in Proc. CHES, 2008, pp. 30–44.

[14]T. Popp, M. Kirschbaum, and S. Mangard, “Practical attacks on masked hardware,” in Proc. Cryptographers’ Track RSA Conf. Topics Cryptol.,2009,pp. 211–225.

[15]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. Papers, vol. 57, no. 2, pp. 355–367, Feb. 2010.

[16]M. Lazzaroni, V. Piuri, and C. Maziero, “Computer security aspects in Industrial instrumentation and measurements,” in Proc. IEEE I2MTC,May 2010, pp. 1216–1221.

[17]J.Wu, Y.-B. Kim, andM. Choi, “Low-power side-channel attack-resistant asynchronous s-box design for AES cryptosystems,” in Proc. 20th Symp.Great Lakes Symp. VLSI, 2010, pp. 459–464.

[18]R. Jevtic and C. Carreras, “Power measurement methodology for FPGA devices,” IEEE Trans. Instrum. Meas., vol. 60, no. 1, pp. 237–247,Jan. 2011.

[19]J. Wu, Y. Shi, and M. Choi, “FPGA-based measurement and evaluation of power analysis attack resistant asynchronous s-box,” in Proc. IEEE I2MTC, May 2011, pp. 1–6.

[20]J. Wu, Y. Shi, and M. Choi, ”Mesurement and evaluation of power analysis attacks on asynchronous s-box” IEEE Trans. In strum. Meas., vol. 61, no.10, pp. 2765–2775, Oct. 2012.

[21]M.R.S. Suvega and P.N. devi, ”Enhanced mesurement and evaluation of power analysis attacks on asynchronous s-box” Int. J. of Comput. Sci. and Eng, vol. 2, no.6, pp.306–312,Nov. 2013.