International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-4 Issue-13 December-2013

FPGA - Based Evaluation of Power Analysis Attacks and Its Countermeasures on Asynchronous S-Box

G. Gokulashree[1], R. Ramya[2]

Abstract

A novel asynchronous S-Box design for AES 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 completely based on a delay insensitive logic paradigm known as Null Conversion Logic (NCL). Asynchronous S-Box is based on self-time logic referred to as NCL which supports few beneficial properties for resisting SCAs such as clock free, duail rail encoding and monotonic transitions so that it consumes less power therefore suitable for energy constrained mobile crypto-applications. These beneficial properties make it difficult for an attacker to decipher secret key embedded within the cryptographic circuits of the FPGA board. Resistant to SCAs of both existing and proposed S-Box design are presented using differential power analysis (DPA) and correlation power analysis (CPA) attacks. The power measurement result showed that the NCL S-Box had lower total power consumption than original and effective against DPA and CPA attacks.

Keywords

Substitution Box, Null Conversion Logic, Side Channel Attack, Simple Power Analysis, Advanced Encryption Standard.

1. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. Application of cryptography includes ATM cards, specification for the encryption of electronic data based on the Rijndael cipher. computer passwords and electronic commerce. Cryptography prior to the modern age was effectively synonymous with encryption the conversion of information from a readable state to apparent nonsense. The advanced encryption standard is the Rijndael is a family of ciphers with different key and block sizes. AES [2] uses three members of the Rijndael family each with a block size of 128 bits but three different key lengths: 128, 192 and 256 bits. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers along with an auxiliary value as their public key. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications [6] in cryptography. Public-key cryptography is based on the intractability of certain mathematical problems. In cryptography a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem. For example timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Some side-channel attacks require technical knowledge of the internal operation of the system on which the cryptography is implemented although others such as differential power analysis are effective as black-box attacks.

2. Existing Method

A) Synchronous Method

Digital logic circuits can be divided into combinational logic in which the output signals depend only on the current input signals and sequential logic in which the output depends both on current input and the past history of inputs. Sequential logic is divided into two types

G. Gokulashree, Department of Electronics and communication Engineering, K.S. Rangasamy College of Technology, KSR Kalvi Nagar, Tiruchengode, Namakkal, Tamilnadu, India.

R. Ramya, Department of Electronics and communication Engineering, K.S. Rangasamy College of Technology, KSR Kalvi Nagar, Tiruchengode, Namakkal, Tamilnadu, India.

synchronous logic and asynchronous logic. The synchronous S-Box result has obtained as shown in Table 1. In synchronous logic circuits an electronic oscillator generates a repetitive series of equally-spaced pulses called the clock signal. The clock signal is applied to all the memory elements in the circuit called flip-flops. The output of the flip-flops only change when triggered by the edge of the clock pulse so changes to the logic signals throughout the circuit all begin at the same time at regular intervals synchronized by the clock. The outputs of all

Table 1: Simulation Results For Three Samples from the Existing S-Box for 128-Bit.

Input	Output
55555554399566A656655654D519A954	FCFCFC2012293324B14DB12003D4D320
AB505C5556AA6A83C2954D352B4B2B2D	62534AFCB1AC02EC2529E396F1B3F1D8
869053F0A7826E55DEA51945555554A9	4460ED8C5C139FFC1D06D46EFCFC20D3

the memory elements in a circuit is called the state of the circuit. Synchronous circuit changes only on the clock pulse. The changes in signal require a certain amount of time to propagate through the combinational logic gates of the circuit it is called as propagation delay.

B) Bytes Substitution Transformation

The bytes substitution transformation Bytesub (state) is a non-linear substitution of bytes that operates independently on each byte of the State using a substitution table(S-box).

3. Proposed method

A) Asynchronous Method

In asynchronous circuits there is no clock and the state of the circuit changes as soon as the input changes. Since they don't have to wait for a clock pulse to begin processing inputs asynchronous circuits can be faster than synchronous circuits and their speed is theoretically limited only by the propagation delays of the logic gates. So asynchronous circuits are more difficult to design and subject to problems not found in synchronous circuits. Thus the resulting state of an asynchronous circuit can be sensitive to the relative arrival times of inputs at gates. If transitions on two inputs arrive at almost the same time then circuit leads into the wrong state depending on slight variations in the propagation delays of the gates so it is called a race condition. In synchronous circuits the problem is less severe because race conditions can only occur due to inputs from outside the synchronous system, asynchronous inputs. Although some fully asynchronous digital systems have been built today asynchronous circuits are typically used in a various critical parts of otherwise synchronous systems where speed is at a premium such as signal processing circuits.

B) Null Conversion Logic

NCL gates [8],[7] are a special case of the logical operators or gates available in digital VLSI circuit design. Such an operator consists of a set condition and a reset condition that the environment must ensure are not both satisfied at the same time. If it satisfies both conditions then the operator maintains its current state. A number of NCL-based designs have been commercially developed by Theseus Logic which has formed strategic alliances with Motorola for microcontroller design and Synopsys for NCL-based design tool development.

Delay-Insensitivity: NCL[13],[12] uses symbolic completeness of expression to achieve self-timed behavior. A symbolically complete expression is defined as an expression that only depends on the relationships of symbols that is present in the expression without a reference to the time of evaluation.

Logic Gates and Functional Blocks: NCL uses threshold gates with hysteresis[11] for its composable logic elements. One type of threshold gate is the THmn gate where $1 \leq m \leq n$ as depicted in Fig.1. A THmn gate corresponds to an operator with at least m signals asserted as its set condition and all signals de-asserted as its reset condition. THmn gates has n inputs. At least m of the n inputs must be asserted before the output will become asserted. Because threshold gates are designed with asserting inputs must be de-asserted before the output will be de-asserted.

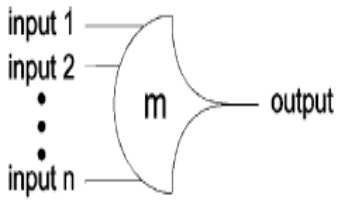

Figure. 1 THmn threshold gate

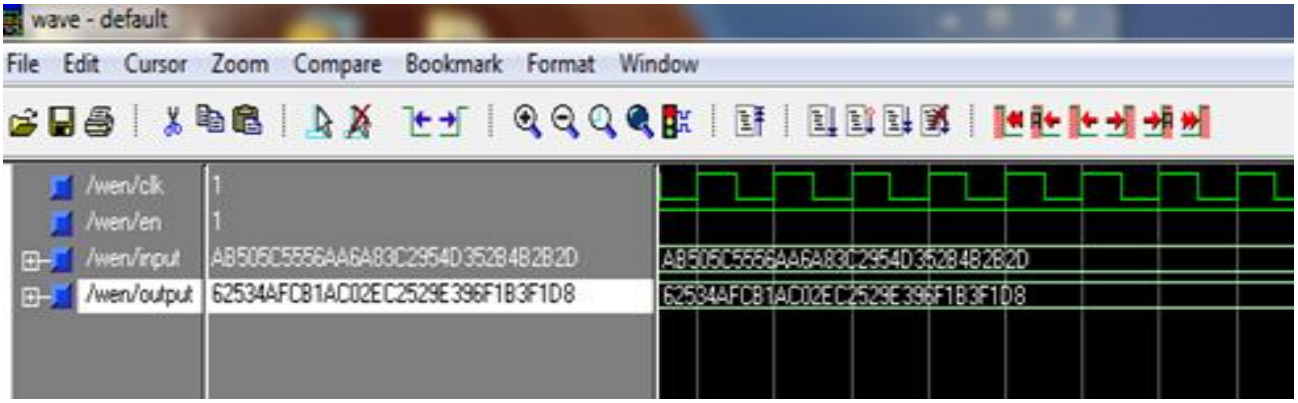

Figure. 2 Synchronous(S-Box) Output Waveform

C) NCL S-Box

The multiplicative inversion in GF(2^8) follows the procedure shown in Fig.3. First operation converts the 8-bit input in to elements of GF(2^4)[1]. Second calculating the square of duail output. GF(2^4) is done by multiplying the polynomial $a_h(x)a_h(x)$ followed by a modular reduction. Third a series of multiplication and XOR operations were implement to extend the field GF(2^4) to the field GF(2^8). In order to implement this conventional S-Box using NCL the XOR, AND and MUX operations in dual-rail NCL gates. NCL has a total of 27 threshold gates to realize various logic functions. In order to achieve the input completeness and delay insensitivity and other important properties it is important to choose appropriate threshold gates.

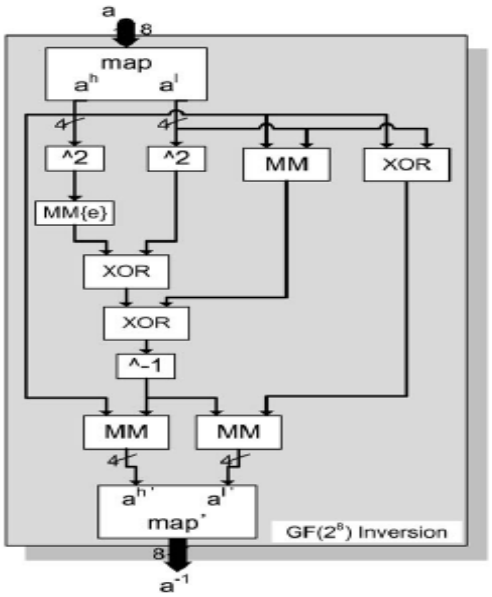

Figure. 3 Block Diagram of Multiplicative Inversion Over the GF (2^8) Component

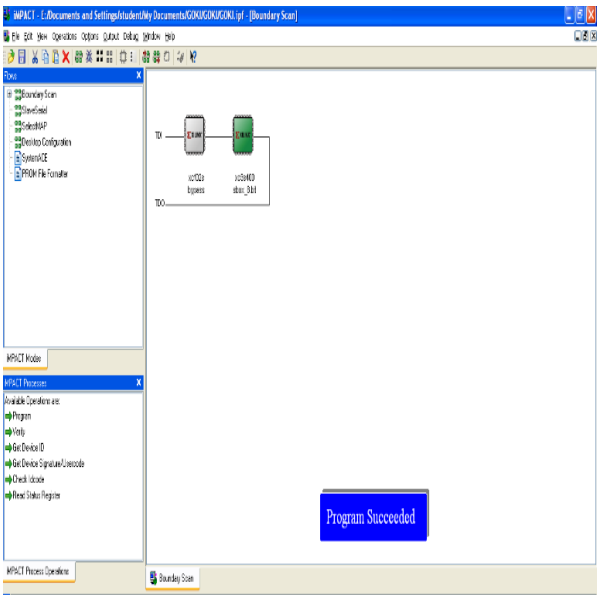

Figure. 4 NCL Output Implemented in FPGA

The asynchronous S-Box result obtained in duail rail[3] in Table 2[4]. A specified SCA standard evaluation field programmable gate array board is used to implement both synchronous and then

Table 2: Simulation Results For Three Samples from the Proposed NCL S-Box for 8-Bit.

Input	NCL Output	NCL Duail Rail Output
00110111	00101100	0101100110100101
10110111	10100011	1001100101011010
01100011	01100110	0110100101101001

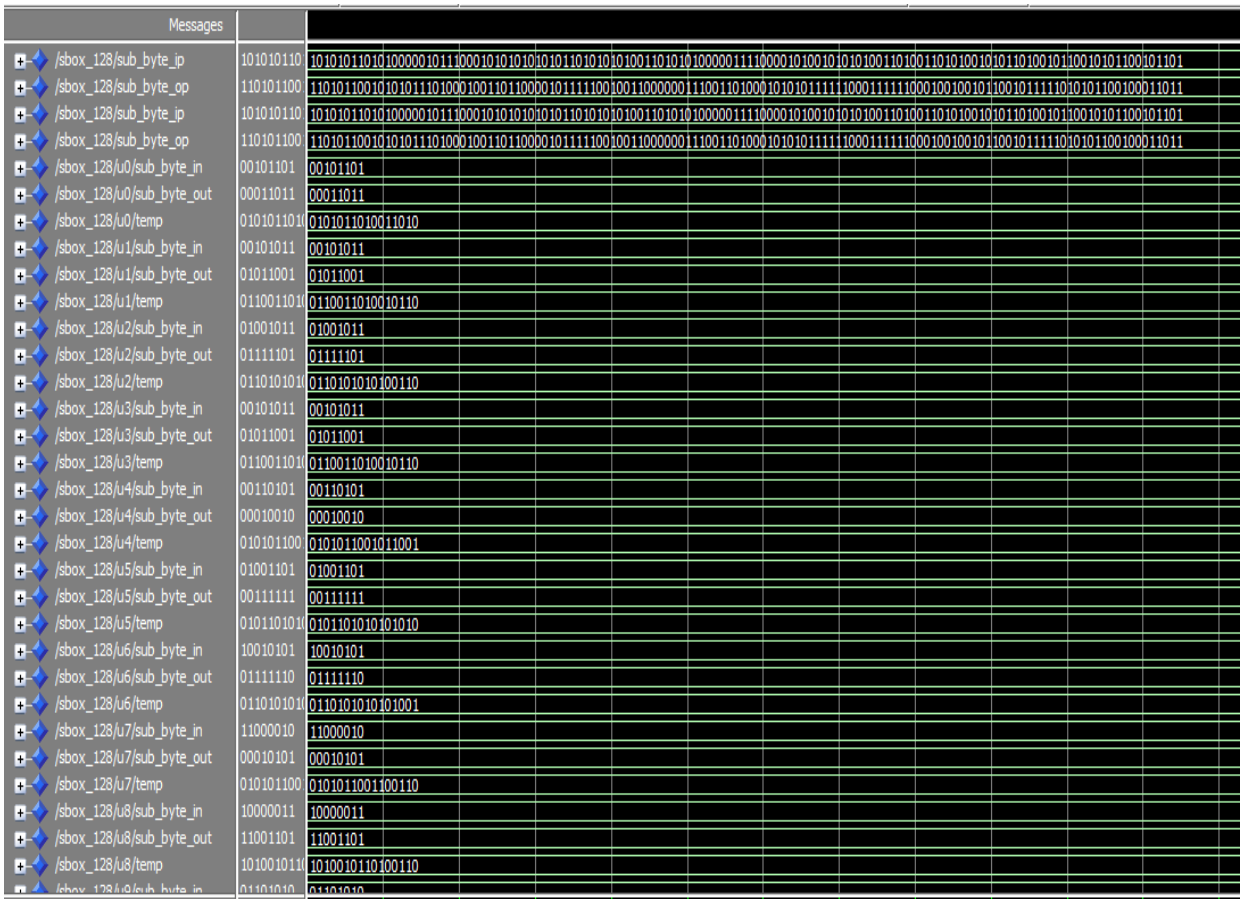

Figure. 5 NCL S-Box for 128 bit Output

Table 3: Power Comparison for Synchronous and Asynchronous S-Box

	Power(mW)
Synchronous S-Box	56
NCL S-Box	34

asynchronous S-Box designs. The beneficial properties make it difficult for an attacker to decipher secret keys embedded within the cryptographic circuit of the FPGA board. A power measurement methodology for the FPGA[9],[10] was also presented to break down the power consumption of different elements inside the logic allowing attackers to get detailed information inside the circuit. Fig.4 shows the successful implementation of an asynchronous method that is used as the basic platform in this paper. As shown in Fig. 5 the input signal is 128 bit and the corresponding output signals also 128 bit respectively.Table 3. Shows the Xilinx power consumption for both synchronous and asynchronous s-box and obtained power in mW.

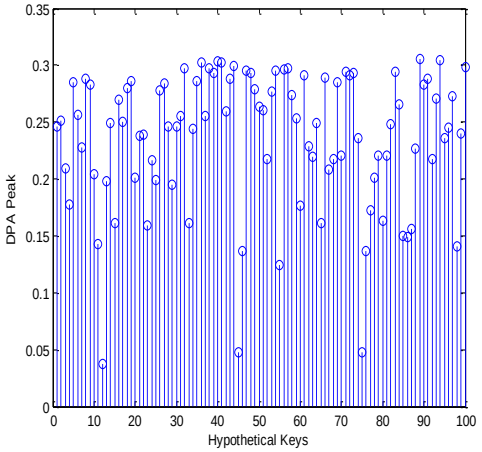

Figure. 6 Power Peaks for Various Key assumptions for a DPA Attack

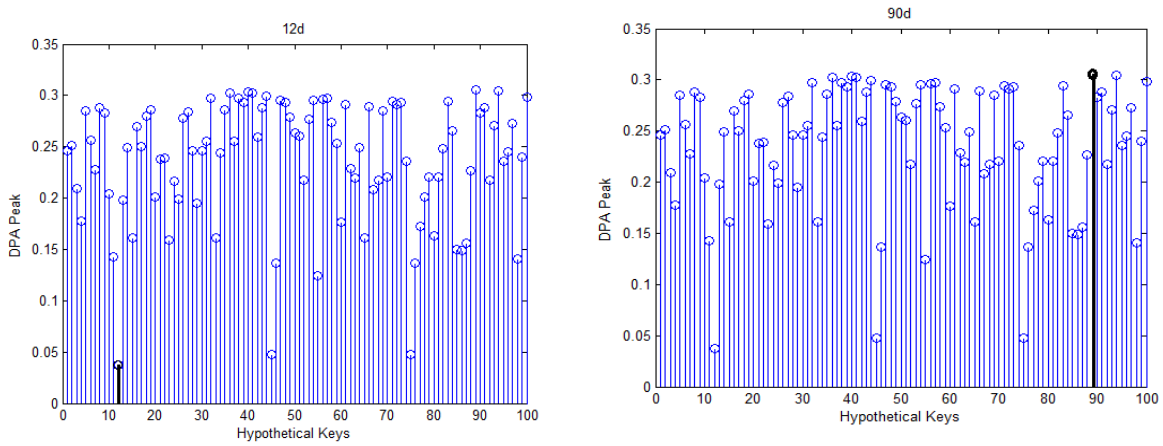

Figure. 7 Power Peaks for Various Key Assumptions for a DPA Attack

D) Differential Power Analysis

In cryptography power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device. The attack can non-invasively extract cryptographic keys and other secret information from the device.

Simple Power Analysis (SPA) involves visually interpreting power traces, or graphs from several electrical activity like power, frequency, time etc all over time. Differential Power Analysis (DPA)[5] is a more advanced form of power analysis which can allows an attacker to identify the intermediate values within cryptographic circuit by continously analyzing data collected from multiple cryptographic operations. The attack exploits several output according to varying power consumption of microprocessors or other hardware while performing operations using secret keys.

DPA process has been implemented on both synchronous S-Box and NCL S-Box with 256 keys. Fig. 6 is the result of the DPA attack on the synchronous S-Box design; the correct key (16d) is clearly identifiable since the power peak is much higher than other hypothesized keys. Fig. 7 shows the result of the DPA attack on the same S-Box design using NCL. The attacker cannot identify the correct key since its power peak is not prominent compared to the others.

E) Correlation Power Analysis

A more effective way to find the secret key of a cryptographic device is to analyze the correlative relationship between the plain text/cipher text and the instantaneous power consumption of the device. The Pearson correlation coefficient is the most familiar measure of dependence between two quantities. CPA is an improvement of DPA. In CPA a power model has been made to predict the power consumption in terms of hypothetical keys and various input/output data the predicted power is then compared with the measured power using a correlation coefficient.

If the hypothetical key is the secret key its correlation coefficient with the measured power will be significantly higher than other wrong keys. The core current of the cryptographic FPGA is measured through a series resistor in the core power supply and it represents the instantaneous power consumption. Fig. 8 shows the result of the CPA attack on the synchronous S-Box design and the NCL S-Box design respectively. The *x*-axis represents the length of a data window and the *y*-axis represents the correlation value for each key hypothesis.

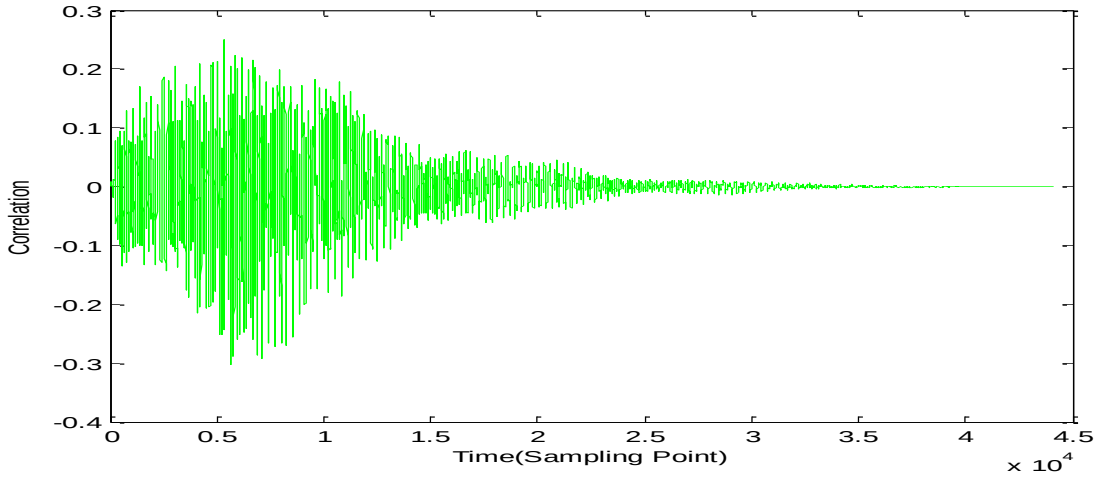

Figure. 8 CPA Result

4. Conclusion

A new asynchronous S-Box design for AES cryptosystems has been proposed and validated. The proposed NCL 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.

A simple attack procedure based on the correlation coefficient evaluation has been done. Experimental result have been discussed including the effect of analysis shows that CPA attacks are successful even in the presence of process variations and this is shown to be valid even in future technologies. The proposed design has been compared with the existing synchronous AES S-Box design reduces power. The proposed NCL AES S-Box has been implemented in VHDL and simulated in ModelSim and obtain low-power operation and DPA resist. . But still power consumption will leak the information so that it can be further reduced by performing a good encryption method to exclude the repetitive terms such that no trace of repetitions can be tracked down and then it is possible to include QCA (Quantum-dot cellular automata) and it has lower total power consumption and it was effective against power analysis attack.

Appendix

Power Report

Power analysis report obtained from FPGA for asynchronous S-Box as one example:

Release 8.1i - XPower SoftwareVersion:I.24
Copyright (c) 1995-2005 Xilinx, Inc. All rights reserved.
Design: sbox_8.ncd
Preferences: sbox_8.pcf
Part: 3s400tq144-5
Data version: ADVANCED,v1.0,11-03-03
XPower and Datasheet may have some Quiescent Current differences.
This is due to the fact that the quiescent numbers in XPower are based on
measurements of real designs with active functional elements reflecting real
world design scenarios.
Power summary: I(mA) P(mW)

Total estimated power consumption: 56

Vccint 1.20V: 15 18
Vccaux 2.50V: 15 38
Vcco25 2.50V: 0 0

Inputs: 0 0
Logic: 0 0
Outputs:
Vcco25 0 0
Signals: 0 0

Quiescent Vccint 1.20V: 15 18
Quiescent Vccaux 2.50V: 15 38
Thermal summary:

Estimated junction temperature: 27C
Ambient temp: 25C
Case temp: 26C
Theta J-A: 33C/W

Decoupling Network Summary: Cap Range (uF) #

Capacitor Recommendations:
Total for Vccint : 4
470.0 - 1000.0 : 1
0.0100 - 0.0470 : 1
0.0010 - 0.0047 : 2

Total for Vccaux : 4
470.0 - 1000.0 : 1
0.0100 - 0.0470 : 1
0.0010 - 0.0047 : 2

Total for Vcco25 : 8
470.0 - 1000.0 : 1
0.0470 - 0.2200 : 1
0.0100 - 0.0470 : 2
0.0010 - 0.0047 : 4
Analysis completed: Sun May 12 23:45:14 2002

References

[1] Jun Wu, Yiyu Shi, and Minsu Choi, "Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box" in instrumentation and measurement, vol. 61, no. 10, october 2012.

[2] 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.

[3] 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.

[4] K. J. Kulikowski, M. Su, A. Smirnov, A. Taubin, M. G. Karpovsky, and D. MacDonald, "Delay insensitive encoding and power analysis: A balancing act", in Proc. 11th IEEE Int. Symp. ASYNC, 2005, pp. 116–125.

[5] F. Gurkaynak, S. Oetiker, H. Kaeslin, N. Felber, andW. Fichtner, "Improving DPA security by using globally-asynchronous locally-synchronous systems", in Proc. 31st Eur. Solid-State Circuits Conf., Sep. 2005, pp. 407–410.

[6] S. Moore, R. Anderson, R. Mullins, G. Taylor, and J. J. A. Fournier, "Balanced self-checking asynchronous logic for smart card applications", J. Microprocess. Microsyst., vol. 27, pp. 421–430, 2003.

[7] S. Smith, "Design of an FPGA logic element for implementing asynchronous null convention logic circuits", IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 15, no. 6, pp. 672–683, Jun. 2007.

[8] A. Bailey, A. A. Zahrani, G. Fu, J. Di, and S. C. Smith, "Multi-threshold asynchronous circuit design for ultra-low power", J. Low Power Electron., vol. 4, pp. 337–348, 2008.

[9] 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.

[10] Indira P. Dugganapally, Waleed K. Al-Assadi, Tejaswini Tammina and Scott Smith, "Design and Implementation of FPGA Configuration Logic Block Using Asynchronous Static NCL",2008.

[11] Mototsune nakahodo, chikatoshi yamada, yasunori nagata, "design and evaluation of hysteresial threshold gate based on neuron mos", international journal of mathematics and computers in simulation, issue 3, volume 1, 2007.

[12] Yancey, Steven, and Scott C. Smith. "A differential design for C-elements and NCL gates." In Circuits and Systems (MWSCAS), 2010 53rd IEEE International Midwest Symposium on, vol., no, vol. 632, pp. 1-4. 2010.

[13] S.C. Smitha,*, R.F. demarab, J.S. Yuanb, D. Fergusonc, D. Lamb, "Optimization of NULL convention self-timed circuits", INTEGRATION, the VLSI journal 37 (2004) 135–165.

G. Gokulashree received the B.E. degree in electronics and communication engineering, SSM College of Engineering certificate from Anna University, Chennai. From 2008 to 2012. She is currently working toward the P.G. degree in the Applied Electronics, K.S. Rangasamy College of Technology, Tiruchengode. From 2012 to 2014.

R. Ramya received the B.E. degree in electronics and communication engineering from K.S.R College of Engineering, Tiruchengode and P.G. degrees in the Applied Electronics, K.S. Rangasamy College of Technology, Tiruchengode. From 2010 to 2012. She is currently an Assistant Professor with the Department of Electronics and communication Engineering, K.S. Rangasamy College of Technology, Tiruchengode.