ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

Secrecy Enhancement of an Asynchronous S-Box with Reduced SCA

M.Ramya, M.Keerthika, C.Gayathri

Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India

Abstract* — *This paper demonstrates the hardware implementation to enhance the secrecy of confidential data communication. Advanced Encryption Standard S-box is capable of resisting the side channel attack. A specified SCA standard evaluation field-programmable gate array (FPGA) board (SASEBO-GII) is used to implement both synchronous and asynchronous S-Box designs. This asynchronous S-Box is based on self-time logic referred to as null convention logic (NCL). Supports a few beneficial properties for resisting SCAs: clock free, dual-rail encoding, 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. By using this NCL the differential power analysis (DPA) and correlation power analysis (CPA) attacks are avoided. This paper enhances the secrecy with reduction of side channel attack.

***Keywords*— Correlation power analysis (CPA), differential power analysis (DPA), energy consumption, field-programmable gate array (FPGA) implementation, instrumentation and measurement, null convention logic (NCL), power/noise measurement, security, side channel attack (SCA), substitution box (S-Box).**

I. 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. 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 substitution box design matches the important security properties: asynchronous, dual rail encoding, and an intermediate state.

Cryptography is the practice and study of hiding information. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., cipher text).Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms which create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

The National Institute of Standards and Technology (NIST) selected the Rijndael algorithm as the new Advanced Encryption Standard (AES) in 2001. Numerous FPGA and ASIC implementations of the AES were previously proposed and evaluated. To date, most implementations feature high speeds and high costs suitable for high-end applications only. The need for secure electronic data exchange will become increasingly more important. Therefore, the AES must be extended to low-end customer products, such as PDAs, wireless devices, and many other embedded applications. In order to achieve this goal, the AES implementations must become very inexpensive. Most of the low-end applications do not require high encryption speeds.

Current wireless networks achieve speeds up to 60 Mbps. Implementing security protocols, even for those low network speeds, significantly increases the requirements for computational power. For example, the processing power requirements for AES encryption at the speed of 10 Mbps are at the level of 206.3 MIPS. In contrast, a

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

state-of-the-art handset processor is capable of delivering approximately 150 MIPS at 133 MHz, and 235 MIPS at 206 MHz. This project attempts to create a bridge between performance and cost requirements of the embedded applications. As a result, a low-cost AES implementation for FPGA devices, capable of supporting most of the embedded applications, was developed and evaluated. Accurate measurement and estimation of these outputs are the key points of a successful attack. The measurement should be based on the hardware gate-level approach rather than the software instruction-level estimation. In addition, for the power consumption measurement, the focus would be the dynamic power consumption that is dissipated during the transistors switching rather than static leakage power consumption.

Advanced Encryption Standard (AES) was announced with the intention of being a faster and more secure encryption algorithm over others since its algorithm is comprised of multiple processes used to encrypt information with supports of up to 256-bit key and lock sizes, making an exhaustive search impossible to check all 2 power 256 possibilities. Usually, the hardware AES implementation has higher reliability than software since it is difficult to be read or modified by attackers and less prone to reverse engineering.

The hardware implementation of 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. Asynchronous circuits, on the other hand, have natural advantages in terms of SCA resistance. The clock-related information leakage can be either eliminated or significantly reduced, which extensively increases the difficulties of attack due to the lack of timing references.

II. SYNCHRONOUS LOGIC

Synchronous logic with clocked structures has dominated the digital design over the past decades. As the decrease of feature sizes and the increase of the operating frequency of integrated circuits (IC), clock-related issues become more serious, such as clock skews, increased power at the clock edges, extra area, and layout complexity for clock distribution networks, and glitches. These motivate the research of asynchronous (i.e., clock less) logic design which has benefits of eliminating all the clock-related issues. 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. Thus, securing cryptographic devices against various side channel attacks (SCAs) has become a very attractive research topic in recent years along with the developments of information technologies. SCAs explore the security information (i.e., secret keys) by monitoring the emitted outputs from physical cryptosystems. Advanced Encryption Standard (AES) was announced with the intention of being a faster and more secure encryption algorithm over others since its algorithm is comprised of multiple processes used to encrypt information with supports of up to 256-bit key and block sizes, making an exhaustive search impossible to check all 2^{256} possibilities. Usually, the hardware AES implementation has higher reliability than software since it is difficult to be read or modified by attackers. Most of the countermeasures designed for hardware implementation of AES are based on securing the logic cells to balance the power consumption of the system and to make it independent of the processing data. This process of adjusting the basic units of the system makes the overall design less vulnerable to attacks. The hardware implementation of 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.

These countermeasures can be separated into two categories based on the framework of the circuit that they are implemented on synchronous and asynchronous. The countermeasures for synchronous circuits include sense amplifier basic logic, which is an improved two-spacer alternating dual-rail circuit; wave dynamic differential logic, which is a dynamic voltage and frequency switching approach; masked logic styles using Fourier transform; random switching logic with its simplified version called dual-rail random-switching logic and the recently proposed masked dual-rail precharged logic and its improved version. These works are centered around 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. Asynchronous circuits, on the other hand, have natural advantages in terms of SCA resistance. The clock-related information leakage can be either eliminated or significantly reduced, which extensively increases the difficulties of attack due to the lack of timing references. The

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

countermeasures based on asynchronous circuits are the balanced delay-insensitive method, the Globally-Asynchronous Locally-Synchronous System module, and the 1-of-*n* data-encoded speed independent circuit.

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 the memory elements in a circuit is called the state of the circuit. The state of a 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. This is called propagation delay. The period of the clock signal is made long enough so the output of all the logic gates have time to settle to stable values before the next clock pulse. As long as this condition is met, synchronous circuits will operate stably, so they are easy to design.

However a disadvantage of synchronous circuits is that they can be slow. The maximum possible clock rate is determined by the logic path with the longest propagation delay, called the *critical path*. So logic paths that complete their operations quickly are idle much of the time. Another problem is that the widely distributed clock signal takes a lot of power, and must run whether the circuit is receiving inputs or not.

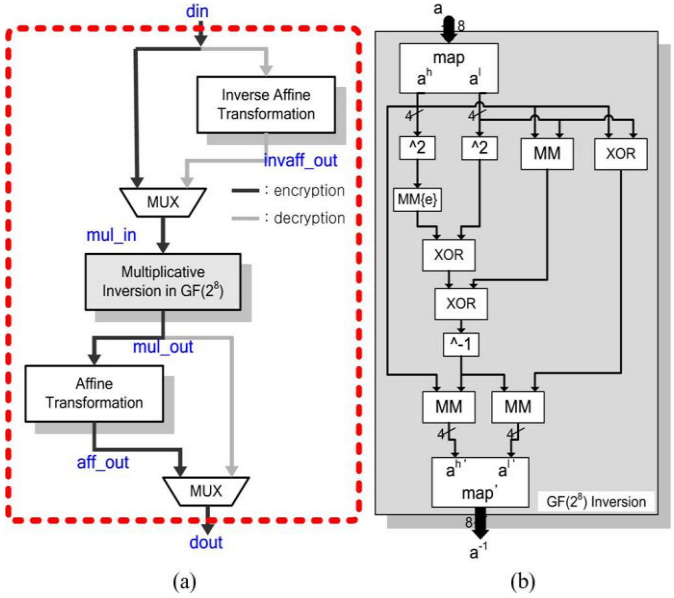

Fig. 1. (a) Combinational S-Box architecture with encryption and decryption data paths. (b) Block diagram of multiplicative inversion, where MM is modular multiplication and XOR is EXCLUSIVEOR operation.

III. NCL AES S-BOX DESIGN

The Advanced Encryption Standard is the most widely used symmetric-key algorithm standard in different security protocols. The AES algorithm consists of a number of rounds that are dependent on the key size. For both cipher and inverse cipher of the AES algorithm, each round consists of linear operation (i.e., ADD ROUNDKEY, SHIFTROWS, and MIXCOLUMNS steps) and nonlinear operation (i.e., SUBBYTES step). SUBBYTES step is the first step of AES round. Each byte in the array is updated by an 8-bit S-Box, which is derived from the multiplicative inverse. The AES S-Box is constructed by combining the inverse function with an invertible affine transformation in order to avoid attacks based on mathematics. The S-Box is one the of most critical components in the implementation of AES hardware. NCL is a delay-insensitive (DI) asynchronous (i.e. clock less) paradigm, which means that NCL circuits will operate correctly regardless of when circuit inputs become available; therefore NCL circuits are said to be correct-by-construction (i.e. no timing analysis is necessary for correct operation).NCL circuits utilize dual-rail or quad-rail logic to achieve delay-insensitivity. The two rails are mutually exclusive, such that both rails can never be asserted simultaneously. The existing

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

countermeasures, we can find that the dual-rail encoding with the precharge method, spacers, or return-to-zero (RTZ) protocols, is frequently used in both synchronous and asynchronous designs.

The dual-rail encoding provides better data independence with the power consumption since the Hamming weights (HWs) of each data set are the same. An RTZ protocol, a spacer, or the precharge method was used to achieve the monotonic transition to enhance the security. Our proposed null-conventional-logic-based (NCL) substitution box (S-Box) design essentially matches all these important security properties: asynchronous, dual rail encoding, and an intermediate state (i.e., NULL). Unlike other asynchronous designs, NCL adheres to the monotonic transitions between DATA (i.e., data representation) and NULL (i.e., control representation), which utilizes dual-rail and quad rail signaling methods to achieve the delay insensitivity. This would significantly reduces the design complexity. With the absence of a clock, the NCL system is proved to reduce the power consumption, noise, and electromagnetic interference. Furthermore, we have demonstrated that NCL can also resist SCAs without worrying about the glitches and power supply variations. In addition to the DPA attack, a CPA attack has also been applied to both synchronous and NCL S-Box design to demonstrated that the proposed NCL S-Box is capable of resisting CPA attack as well.

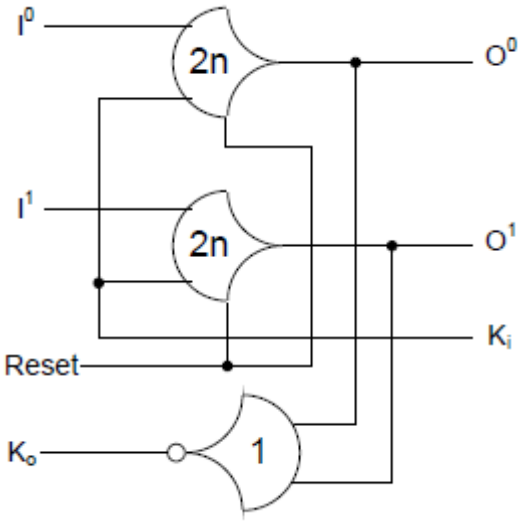

Fig. 2 Single bit dual rail register

IV. FUNCTIONAL VERIFICATION OF THE PROPOSED NCL S-BOX DESIGN

The initial value of the input and that of the output are NULL and DATA0, respectively. Previous input registers are reset to NULL and output registers are reset to DATA0. As soon as the reset falls down to 0, Ko from the output register becomes 1,and Ki for the input register connected to Ko becomes 1. As Ki rises, the input is changed to the waiting input signal 01 01 01 01 01 01 01 01 in dual-rail signaling, which means 00000000 in binary and 0x00 in hexadecimal. The initial value of the input and that of the output are NULL and DATA0, respectively. Previous input registers are reset to NULL and output registers are reset to DATA0. As soon as the reset falls down to 0, Ko from the output register becomes 1,and Ki for the input register connected to Ko becomes 1. As Ki rises, the input is changed to the waiting input signal 01 01 01 01 01 01 01 01 in dual-rail signaling, which means 00000000 in binary and 0x00 in hexadecimal. As every bit of the output signal changes from NULL to DATA, *Ko* falls to 0, which means that the output register has received the proper output DATA wave. Every single component (i.e., affine and inverse affine transformation, and multiplicative inversion)has been separately verified.

On the NCL S-Box output column, the results are shown as 16 bits, which are the extended dual-rail signals. For example, for input 158, the NCL S-Box output is 01 01 01 01 10 01 10 10, and this dual-rail encoded data word is equivalent to 00001011 in binary, which is equal to the output of the conventional synchronous S-Box. Since the key is 11010100, after the bitwise XOR function, the actual input that goes to the S-Box would be 00101011. According to the standard S-Box table, the corresponding output is 11110001, which is 1010101001010110 in NCL and 0*xF*1 in hexadecimal. Following that, the input signal is incremented to

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

00000000, and the S-Box input becomes 00000000 XOR 1010100 = 11010100, which generates the corresponding output 01001000 (i.e., 0*x*48). Similarly, hexadecimal numbers 0*x*03 and 0*xF*6 shown in the Fig. 5 can be derived as well. All 256 inputs with different keys have been verified during the power analysis programming using MATLAB. The correct behavior of the function is the prerequisite for a successful power attack.

II. DPA

DPA is a much more powerful attack than SPA, and is much more difficult to prevent. While SPA attacks use primarily visual inspection to identify relevant power fluctuations, DPA attacks use statistical analysis and error correction techniques to extract information correlated to secrete keys. Implementation of a DPA attack involves two phases. They are data collection and data analysis. Data collection for DPA may be performed as described by a device's power consumption during cryptographic operations as a function of time. For DPA, a number of cryptographic operations using the target key are observed. This DPA process has been implemented on both synchronous S-Box and NCL S-Box with 256 keys. The DPA attack results show that the selected keys cannot be identified from other assumption keys. Therefore, the proposed NCL S-Box design is secured from DPA attacks. The key that is assumed from the power analysis is avoided by implementing this method. Thus the information that is transmitted from the transmitter to receiver will be secured that has different keys which makes the attacker to hack the data.

TABLE I. SIMULATION RESULTS FOR TEN ARBITRARY SAMPLES FROM THE CONVENTIONAL SYNCHRONOUS S-BOX AND THE PROPOSED NCL S-BOX.THE S-BOX OUTPUTS ARE DUAL RAIL ENCODED

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

VI. COUNTER MEASURE CIRCUIT

The countermeasures for synchronous circuits include sense amplifier basic logic, which is an improved two-spacer alternating dual-rail circuit wave dynamic differential logic, which is a dynamic voltage and frequency switching approach masked logic styles using Fourier transform random switching logic with its simplified version called dual-rail random-switching logic and the recently proposed masked dual-rail precharged logic and its improved version. These works are centered around 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.

Asynchronous circuits, on the other hand, have natural advantages in terms of SCA resistance. The clock-related information leakage can be either eliminated or significantly reduced, which extensively increases the difficulties of attack due to the lack of timing references. The countermeasures based on asynchronous circuits are the balanced delay-insensitive method, the Globally-Asynchronous Locally-Synchronous System module, and the 1-of-n data-encoded speed independent circuit. However, the increased security does not come for free. The area required to implement them is potentially larger than their synchronized counterpart The benefits in terms of total power consumption and speed are still questionable. In addition, some of the countermeasures are based on the electronic design automation tool simulation results or theoretical analysis, which may not effectively prove that these methods can experimentally resist real SCAs. From these existing countermeasures, we can find that the dual-rail encoding, with the precharge method, spacers, or return-to-zero (RTZ) protocols, is frequently used in both synchronous and asynchronous designs. **T**he dual-rail encoding provides better data

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

independence with the power consumption since the Hamming weights (HWs) of each data set are the same. An RTZ protocol, a spacer, or the precharge method was used to achieve the monotonic transition to enhance the security.

The proposed null-conventional-logic-based (NCL) substitution box (S-Box) design essentially matches all these important security properties: asynchronous, dual rail encoding, and an intermediate state (i.e., NULL). Unlike other asynchronous designs, NCL adheres to the monotonic transitions between DATA (i.e., data representation) and NULL (i.e., control representation), which utilizes dual-rail and quadrail signalling methods to achieve the delay insensitivity. This would significantly reduces the design complexity. With the absence of a clock, the NCL system is proved to reduce the power consumption, noise, and electromagnetic interference.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Fig. 3 The Effect of the Sub Bytes() transformation of the state

Furthermore, we have demonstrated that NCL can also resist SCAs without worrying about the glitches and power supply variations. This project provides an extension to what has been presented in. In addition to the DPA attack, a CPA attack has also been applied to both synchronous and NCL S-Box design to demonstrated that the proposed NCL S-Box is capable of resisting CPA attack as well. By transforming this input to the polynomial the input is converted and the respective code is replaced by the use of matrix array. The counter measure logic will shift the secret key with user defined counts and it continues till the count completes. By this logic the attacker will find difficult to hack the key. The counter measure circuit is inserted as the initial stage which introduces shift register and shifts the key. By this method the security key is shifted in a considerable count till the information reaches the receiver. So, the attacker cannot hack the secrete key.

Thus the simulation result shown below will get the 128 input and segments into 8 bit and shifting will takes place 6 times. After this shifting the 8bit input will be converted into dual rail code. Then the corresponding output is obtained from the affine transformation. Till the shifting the key will not be known to the attackers and at the receiver the inverse affine transformation is done and the original output information is retrieved.

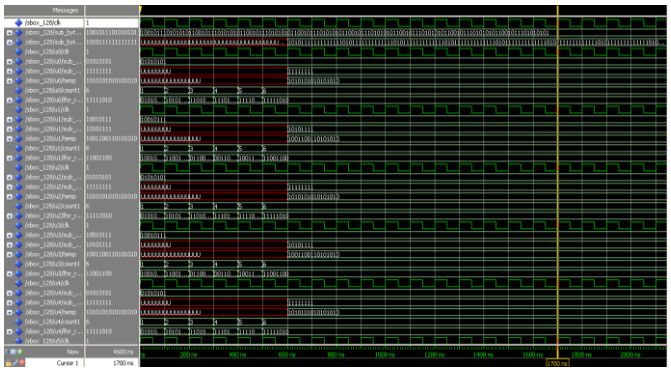

Fig 4 Simulation result of counter measure circuit

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

VII. POWER CONSUMPTION

Power minimization is of paramount importance for designers today, especially in the portable electronic-device market, where devices have become increasingly feature rich and power hungry. Low supply voltages play a significant role in determining the power consumption in portable electronic-device circuits.Many side-channel attacks on implementations of cryptographic algorithms have been developed in recent years demonstrating the ease of extracting the secret key. In response, various schemes to protect cryptographic devices against such attacks have been devised and some implemented in practice. Almost all of these protection schemes target an individual side-channel attack and consequently, it is not obvious whether a scheme for protecting the device against one type of side channel attacks may make the device more vulnerable to another type of attacks.

Examination of the concept is the possibility of such a negative impact for the case where fault detection circuitry is added to a device (to protect it against fault injection attacks) and analyze the resistance of the modified device to power attacks. To simplify the analysis we focus on only one component in the cryptographic device (namely, the S-box in the AES and Kasumi ciphers), and perform power attacks on the original implementation and on a modified implementation with an added parity check circuit. Our results show that the presence of the parity check circuitry has a negative impact on the resistance of the device to power analysis attacks. After the functional verification, the VHDL code has been synthesized and its power measurements are executed using XILINX ISE simulator. Power simulation results from XILINX ISE simulator for the proposed NCL S-Box and conventional synchronous S-Box are shown in Fig 5.As Fig s5 shows the proposed NCL S-Box has 165 mW and conventional synchronous S-Box has 174 mW for temperature about 27 degree Celsius.

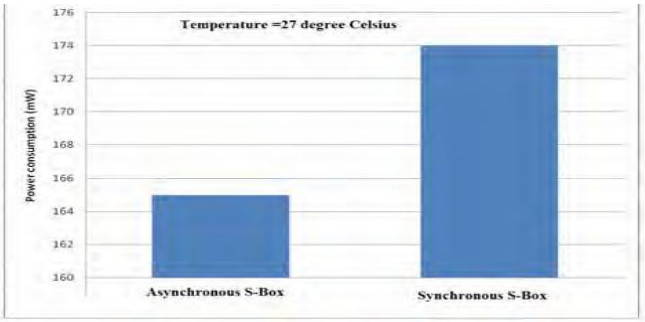

Fig. 5 Total estimated power consumption.

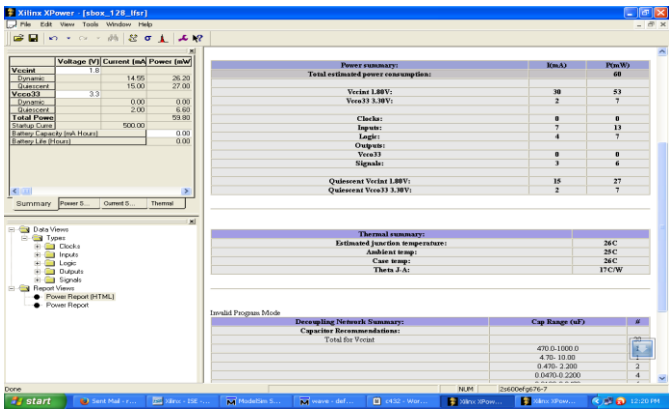

Fig. 6 Power consumption without LFSR

The power consumption without using the counter measure logic is 88mW and the power consumption with counter measure logic is 60mW.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

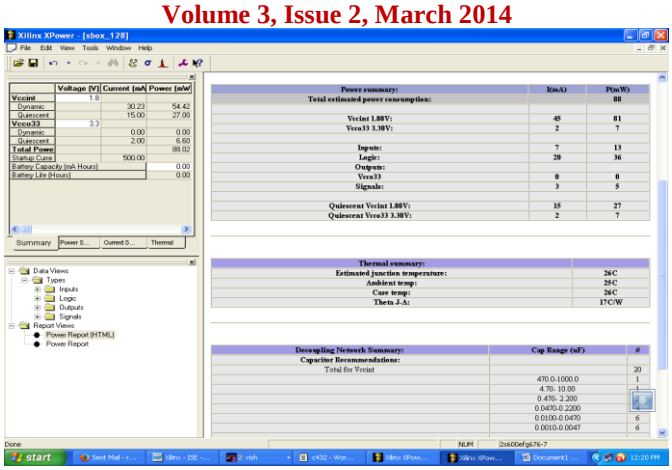

Fig. 7 Power consumption with LFSR

Power consumption is less by using the counter measure logic.

VIII. CONCLUSION

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. 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. Thus by the introduction of counter measure circuit the secrecy enhancement is achieved.

REFERENCES

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

[2] D. Sokolov, J. Murphy, A. Bystrov, 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.

[3] 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.

[4] V. Satagopan, B. Bhaskaran, A. Singh, and S. C. Smith, "Automated energy calculation and estimation for delay-insensitive digital circuits," Micro electron. J., vol. 38, no. 10/11, pp. 1095–1107, Oct. /Nov. 2007.

[5] 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.

[6] 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.

[7] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES sboxes," in Proc. Cryptographer's Track RSA Conf. Topics Cryptol., 2002, pp. 67–78.

[8] L. Medina, R. de Jesus Romero-Troncoso, E. Cabal-Yepez, J. de Jesus Rangel-Magdaleno, and J. Millan-Almaraz, "FPGA based multiple-channel vibration analyzer for industrial applications in induction motor failure detection," IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 63–72, Jan. 2010.

[9] 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.

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

[11] R.C. for Information Security. Side-channel attack standard evaluation board SASEBO-GII specification, Sep. 2009.[Online].Available:http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-GII-en.html

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014
[12] P. Kocher, J. Jaffe, and B. Jun, Differential Power Analysis. London, U.K.: Springer-Verlag, 1999, pp. 388–397.