Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2014, Article ID 837572, 13 pages
http://dx.doi.org/10.1155/2014/837572

Research Article

Asynchronous Advanced Encryption Standard Hardware with Random Noise Injection for Improved Side-Channel Attack Resistance

Siva Kotipalli,[1] Yong-Bin Kim,[2] and Minsu Choi[3]

[1] *Samsung Electronics, Austin, TX 78754, USA*
[2] *Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115, USA*
[3] *Department of Electrical and Computer Engineering, Missouri University of Science & Technology, Rolla, MO 65409, USA*

Correspondence should be addressed to Minsu Choi; choim@mst.edu

Received 18 February 2014; Revised 22 May 2014; Accepted 22 May 2014; Published 20 July 2014

Academic Editor: Sos Agaian

This work presents the design, hardware implementation, and performance analysis of novel asynchronous AES (advanced encryption standard) Key Expander and Round Function, which offer increased side-channel attack (SCA) resistance. These designs are based on a delay-insensitive (DI) logic paradigm known as null convention logic (NCL), which supports useful properties for resisting SCAs including dual-rail encoding, clock-free operation, and monotonic transitions. Potential benefits include reduced and more uniform switching activities and reduced signal-to-noise (SNR) ratio. A novel method to further augment NCL AES hardware with random voltage scaling technique is also presented for additional security. Thereby, the proposed components leak significantly less side-channel information than conventional clocked approaches. To quantitatively verify such improvements, functional verification and WASSO (weighted average simultaneous switching output) analysis have been carried out on both conventional synchronous approach and the proposed NCL based approach using Mentor Graphics ModelSim and Xilinx simulation tools. Hardware implementation has been carried out on both designs exploiting a specified side-channel attack standard evaluation FPGA board, called SASEBO-GII, and the corresponding power waveforms for both designs have been collected. Along with the results of software simulations, we have analyzed the collected waveforms to validate the claims related to benefits of the proposed cryptohardware design approach.

1. Introduction

Advanced encryption standard (AES) is the most widely used symmetric-key algorithm standard in different security protocols [1]. Originally, the algorithm was called Rijndael; but after its selection as the candidate for AES due to its merits, it gained popularity. It is used by hundreds of millions of users worldwide to protect security in various applications. AES was conceived as reliable in providing security for data, until researchers proved that side-channel attacks (SCA) were successful in compromising its security. Since the discovery of various efficient SCAs such as power analysis and EM (electromagnetic) analysis, researchers have started exploring different approaches to design countermeasures.

Wave dynamic differential logic (WDDL) [2] and sense amplifier based logic (SABL) [3] are some of the previously proposed countermeasures of synchronous category. But both of these approaches suffer from timing related issues that could leak side-channel information. Wu et al. [4] proposed an asynchronous S-box design that proved to be power efficient and side-channel attack resistant. Sui et al. [5] proposed a design approach that combines S-box design with random dynamic voltage scaling (RDVS) to boost SCA resistance to a greater extent.

This paper proposes a scalable asynchronous AES Key Expander and Round Function designs that incorporate the merits of null convention logic (NCL) and random voltage scaling. In this work, these two modules are then utilized to

design a NCL based subset of the AES cryptosystem. The reason for calling it a subset is that, in an actual AES, the two modules are utilized iteratively. But for the cryptosystem subset discussed in this work, we utilize the two modules only for a single iteration for verification purposes.

This work has multiple contributions in improving SCA resistance of cryptohardware as follows:

(1) the proposed approach contributes to a uniform and reduced switching activity in cryptosystem and thereby curtail the leaked power and improve resistance against power analysis SCA;

(2) the anticipated improved switching profile also translates to uniform and reduced EM radiation side-channel information emanating from cryptosystem and boosts the resistance of cryptosystem against EM SCA [6];

(3) the proposed Key Expander and Round Function designs allow easy scaling for implementing entire AES algorithm of any of the following variants—128, 192, or 256 bits;

(4) they can also be easily scaled and implemented for different modes of AES like electronic codebook (ECB), cipher feedback (CFB), and cipher block chaining (CBC) modes;

(5) both proposed designs incorporate a power efficient NCL combinational substitution box design, which provides power benefits when compared to the conventional approach;

(6) the proposed design can also be effectively coupled with STRVDS (spatial temporal random dynamic voltage scaling) technique to intentionally inject random noise for even higher SCA resistance.

The rest of the paper is arranged as follows. Section 2 gives a background of AES, NCL, and vulnerabilities of synchronous AES which are essential in understanding the proposed design techniques. Section 3 details the influence of switching activity on SCA. Section 4 describes the proposed NCL AES Key Expander. Section 5 describes the proposed NCL AES Round Function. The proposed STRDVS noise injection technique for NCL cryptohardware is discussed in Section 6. Section 7 discusses the results, which include the functional verification, WASSO analysis, hardware implementation, and power trace analysis for both conventional and proposed designs. This is finally followed by conclusion and future work.

2. Preliminaries and Review

2.1. Advanced Encryption Standard. The AES algorithm is a symmetric block cipher that processes data blocks of 128 bits using cipher keys of three different lengths: 128, 192, or 256 bits. Its operations are performed on the State. The State is a two-dimensional array of bytes which contains the Plaintext, consisting of four rows and N_b columns, where N_b is the block length divided by 32. Similarly, the Key Schedule is a two-dimensional array of bytes which contains the Key.

At the start of the cipher operation, input Plaintext is copied to the State and input Key is copied to the Key Schedule. After an initial Round Key addition, the State is transformed by a Round Function implemented N_r times. This number depends on the key length: $N_r = 10$ for 128 bits, $N_r = 12$ for 192 bits, and $N_r = 14$ for a key length of 256 bits.

Figure 1 shows the two main components of AES. Key Expander and Round Function have four basic byte-oriented transformations each, which are applied to the Key Schedule and the State, respectively.

2.2. Vulnerability of Synchronous AES Hardware Design. Cryptographic algorithms including AES have been used in many applications which require high security. To satisfy these security requirements, various public/private-key algorithms have been proposed and hardware models are designed for encryption and decryption processes. However, without proper hardware implementation, these algorithms and models are still vulnerable to side-channel attacks [7–9]. Differential power analysis (DPA) is one good example of side-channel attack where a series of power traces is intentionally collected for a set of input Plaintexts (or ciphertexts) and statistically analyzed to reveal the private key or significantly narrow down the key search space [7, 8, 10, 11]. The statistical nature of DPA makes it harder to counteract, since extremely small deviations in power can be accumulated and amplified to locate power peaks and the secret key can still be attacked. Even more powerful CPA (correlation power analysis) attack has been also recently gaining attentions [12].

Just as the power consumption of CMOS devices is data-dependent, the electromagnetic radiation emanating from a cryptosystem is also data-dependent. This data-dependent radiation is again the origin of side-channel information leakages. The leaked side-channel information is analyzed by means of electromagnetic analysis (EMA), which measures electromagnetic fields near cryptographic device [6] and uses this data to compromise the security. But if we can curtail the leakage of side-channel information, we can thereby make it difficult for the attacker to have sufficient information to identify the segments in the power waveform and EM radiation. We can secure the cryptosystem more effectively against these power analysis and EMA SCA.

2.3. Null Convention Logic (NCL). NCL is a delay-insensitive (DI) logic design paradigm. The delay insensitivity of NCL circuits is achieved by dual-rail and quad-rail logic [13]. A dual-rail signal can effectively represent four states. Out of them, the three valid states are DATA0, DATA1, and NULL. The fourth state in which both rails are asserted is considered as an illegal state. The valid data states DATA0 and DATA1 correspond to Boolean logic 0, Boolean logic 1, respectively. The control signal NULL is used for asynchronous handshaking. The clock-free operation is implemented via the two delay-insensitive registers located on either side of the combinational circuit and the local handshaking signals.

The main benefit of NCL is that more uniform power consumption signature can be achieved since the signals are

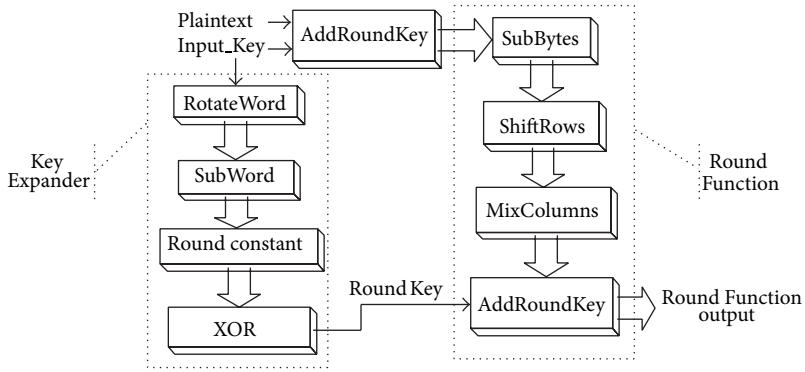

Figure 1: Block diagram of AES Round Function with Key Expander.

implemented by two complementary wires. Furthermore, due to delay-insensitive nature, these DI circuits adhere to monotonic transitions between DATA and NULL; so, there is no glitching, unlike clocked Boolean circuits that produce substantial glitch power and information leakage resulting from glitching. DI systems better distribute switching over time and area, reducing the switching activity, peak power demand, and system noise, unlike clocked Boolean circuits where much of the circuitry switches simultaneously at the clock edge. Another important potential of NCL is it inherently allows intentional noise injection by randomizing timing of switching activities to further reduce the side-channel information leakage. The downside is it generally incurs area and wire overhead.

3. Influence of Switching Activity on SCA

3.1. Role of Switching Activity on Power Analysis SCA. The dynamic power consumption of CMOS gates is particularly relevant from a side-channel point of view since it determines a simple relationship between a device's internal data and its externally observable power consumption. It can be written as

$$P_{\text{dyn}} = A \cdot C_L \cdot V_{\text{dd}}^2 \cdot f. \tag{1}$$

In (1), P_{dyn} is the power consumed, A is the switching activity factor, C_L is the switched capacitance, V_{dd} is the supply voltage, and f is the clock frequency. This data-dependent power consumption is the origin of side-channel information leakages. If we are able to reduce the switching activity factor A in (1), that would directly translate to decreased dynamic power consumption. Messerges et al. discussed the role of SNR ratio in determining the success probability of a DPA attack in [14]. Consider

$$\text{SNR} = \frac{\text{var}\left(P_{\text{expl}}\right)}{\text{var}\left(P_{\text{noise}}\right)}. \tag{2}$$

Equation (2) can be used to estimate SNR [15]. In this equation, var(P_{expl}) is the variance of exploitable component of power consumption and var(P_{noise}) is the variance of noise component. By reducing this exploitable power information P_{expl}, we can lower the SNR ratio. The lower the SNR ratio, the lower the leakage; so, performing the power analysis attack becomes harder.

3.2. Role of Switching Activity on EM SCA. The switching activity also influences the EM radiation leaked from the cryptosystem. The voltage fluctuation caused by ground bounce can be expressed as [6]

$$\Delta V = L_{\text{eff}} \cdot M \cdot \frac{dI}{dt}. \tag{3}$$

In this equation, L_{eff} is the effective parasitic inductance, M is the number of simultaneous switching outputs, and dI/dt is the rate of change of the current. So, it is clear that if we are able to reduce the switching activity M, we can reduce the information leakage due to ΔV, as $\Delta V \propto M$.

4. NCL AES Key Expander Design

The AES algorithm uses a Key Expander to calculate the Round Keys used in AddRoundKey stage of the Round Function. The AES specification refers to this process as the KeyExpansion. The motive behind the purpose of this unit is that generating multiple keys from an initial key and using a unique key for each round, instead of using the same key for all the rounds, greatly increase the diffusion of bits. For this research, we chose AES with a key size of 128 bits.

The control unit for these NCL AES Key Expander and Round Function is shown in Figure 2. In this control unit, the input data which is in ordinary binary format is read and is converted into dual-rail inputs by single-rail to dual-rail converter. K_o is the output acknowledgement signal coming out of the NCL Round function and Key Expander. It acts like clock signal for the other units in the controller. The converter and multiplexer (MUX) are controlled by K_o. When K_o is 1, it means NCL Round function and Key expander are ready for NULL wavefront; then, MUX will send all 0's to Plaintext and Input_Key to nullify the NCL Key Expander and Round function. Otherwise, MUX will select the dual-rail data that is output from the converter. The dual-rail "Input_Key" is fed as input to the NCL Key Expander and it generates the Round Keys necessary for each encryption round of AES.

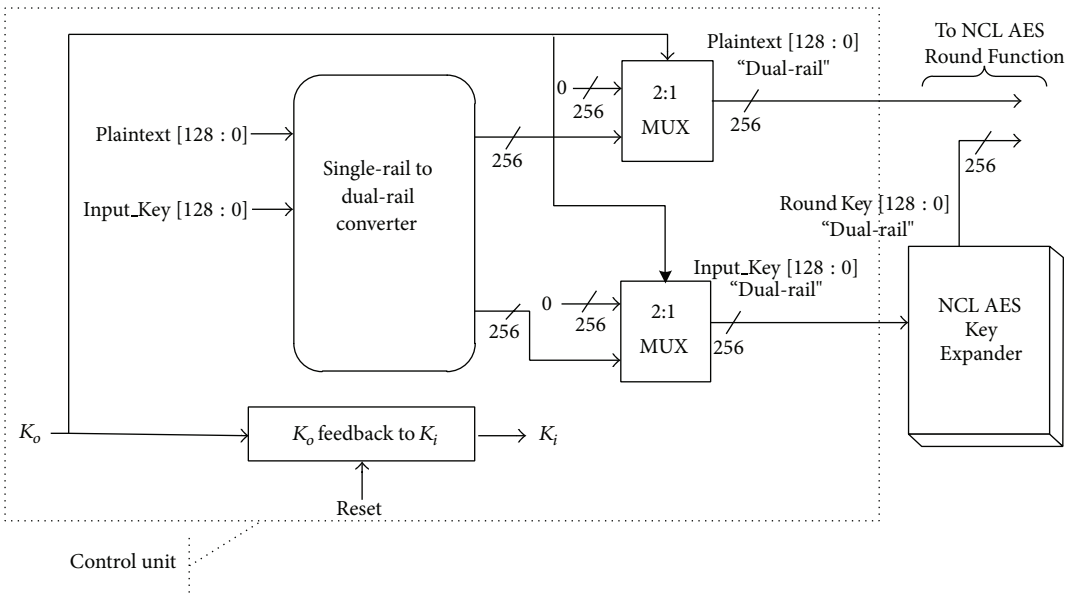

Figure 2: Block diagram of NCL AES control unit.

The block diagram of the Key Expander architecture [16] is presented in Figure 3. The w_0, w_1, w_2, and w_3 are the four columns of the Key Schedule. The columns of the Key Schedule which have their index as a multiple of four undergo the "RSX step" along with the XOR operation; all the remaining columns undergo XOR operations to generate the Round Key. As depicted in the figure, Key Expander consists of the following modules.

RotateWord. This operation accepts an array of 4 bytes and rotates them 1 position to the left. The RotWord function used by KeyExpansion is very similar to the ShiftRows routine used by the encryption algorithm except that it works on a single column of the Key Schedule, instead of the rows of the State array.

SubWord. The SubWord routine performs a byte-by-byte substitution on a given row of the Key Schedule table using the NCL S-box. The substitutions in KeyExpansion operate exactly like those in the SubBytes step of Round Function. The input byte to be substituted is fed as input to the NCL combinational S-box, and this input then undergoes multiplicative inversion in GF(2^8) and affine transformation during encryption. We employed the dual-rail combinational NCL S-box proposed in [4] for this step as this design already proved to be very power efficient and resistant to SCA. The architecture of the S-box and the block diagram of its internal multiplicative inversion module are presented in Figures 4 and 5.

Round Constant Module. This module uses an array Rcon, called the round constant table. In the synchronous implementation, these round constants are 4 bytes each to match with a column of the Key Schedule table. The AES KeyExpansion routine [1] requires 10 round constants, one for each round of the AES algorithm. In our implementation, we implement this as an array of round constants represented in dual-rail notation.

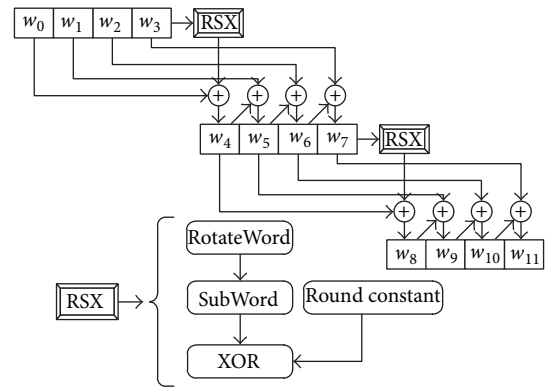

Figure 3: Block diagram of AES Key Expander [16].

XOR Module. In this module, we perform the XOR operation between the columns of the Key Schedule with or without the round constant selected in previous step depending on the column which is being calculated. In order to realize this XOR function in NCL, we have to make use of NCL XOR function designed using the NCL threshold gates.

Unlike Boolean logic, NCL has 27 fundamental threshold gates to realize arbitrary logic [13]. In order to achieve the input-completeness and observability, it is important to choose appropriate threshold gates. For the design of NCL XOR function, the sum-of-product (SOP) expressions are $Z^1 = A^1B^0 + A^0B^1$ and $Z^0 = A^0B^0 + A^1B^1$. They can be realized by mapping them to THxor0 gates as shown in Figure 6. However, two transistors can be eliminated for each rail of Z

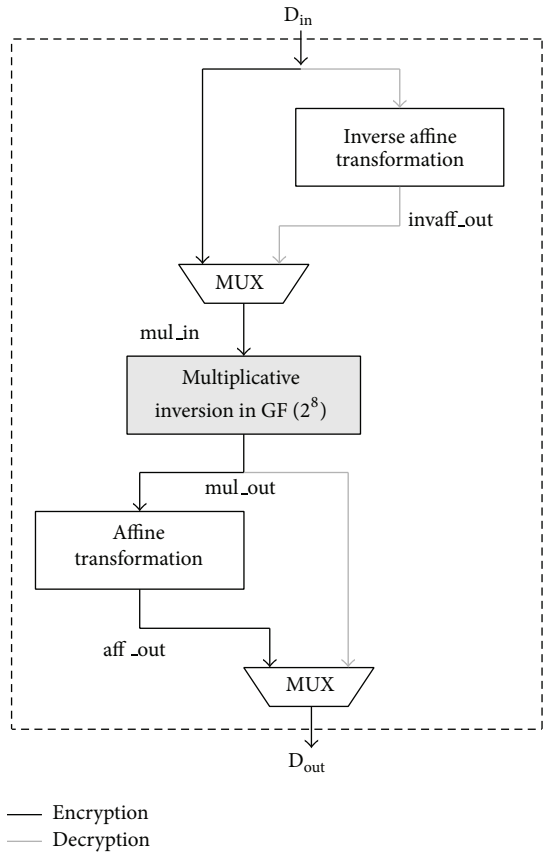

Figure 4: Combinational S-box architecture.

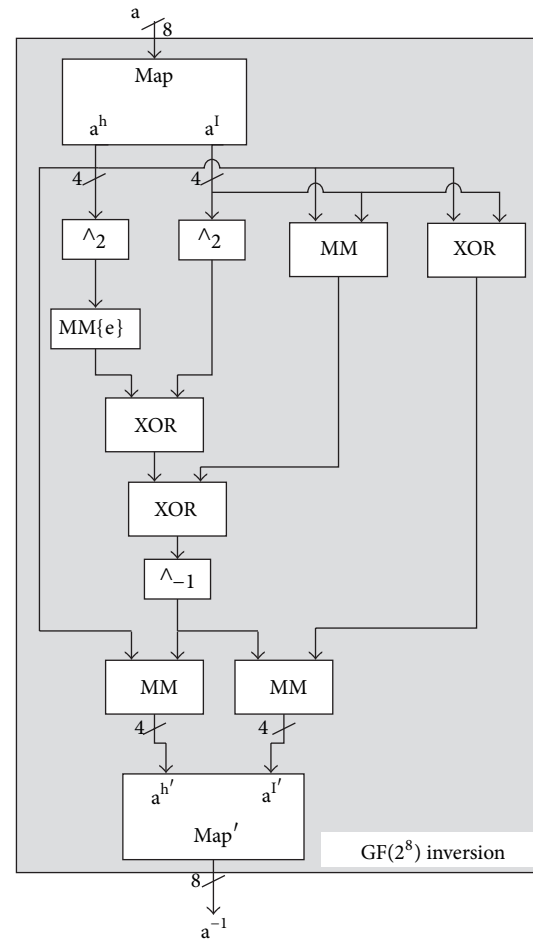

Figure 5: Block diagram of multiplicative inversion over GF(2^8) where MM is modular multiplication unit.

(when using static gates) by realizing this same functionality using TH24comp gates. This is done by adding the two *do not care* terms, representing the cases when both rails of either A or B are simultaneously asserted.

The new equations are $Z^1 = A^1B^0 + A^0B^1 + A^0A^1 + B^0B^1$ and $Z^0 = A^0B^0 + A^1B^1 + A^0A^1 + B^0B^1$. The NCL XOR function realized using these equations and TH24comp gates is presented in Figure 7 and is used in our proposed design. This TH24comp based XOR offers a 10% reduction in the number of transistors required compared to the approach using THxor0 gates.

5. NCL AES Round Function

The top-level architecture of the proposed NCL AES Round Function design is presented in Figure 8. Controller for this module is presented previously in Figure 2. This control unit takes care of converting the ordinary Plaintext and Input_Key into dual-rail notations. The dual-rail "Input_Key" is fed as input to the NCL Key Expander and it generates the Round Key, which along with the dual-rail Plaintext from the controller is fed to the AES Round Function.

The NCL AES Round Function consists of the following four steps which are performed sequentially.

(1) NCL SubBytes. In this transformation, each dual-rail byte of the State matrix is substituted independently by another

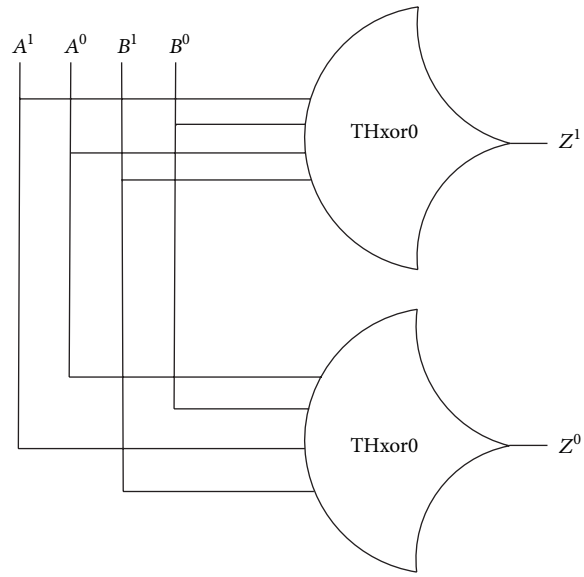

Figure 6: NCL XOR function using THxor gates.

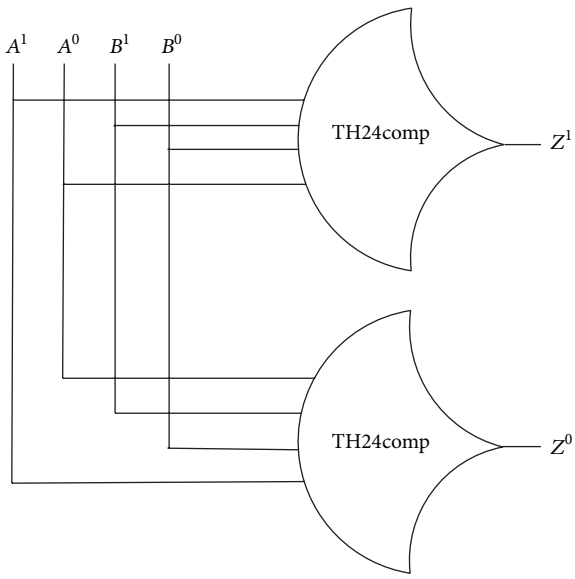

Figure 7: NCL XOR function using TH24comp gates.

one which is computed by the NCL S-box. The S-box is a key element in the AES architecture as it significantly influences the security, power consumption, and throughput of the AES hardware. We are using the dual-rail combinational NCL S-box proposed in [4] for this step as this design already proved to be very power efficient and resistant to SCA.

(2) NCL ShiftRows. The NCL ShiftRow transformation function performs byte transposition of all dual-rail NCL signals by using circular shifting, where each row of dual-rail State is rotated cyclically to left using 0-, 1-, 2-, and 3-byte offsets for encryption.

(3) NCL MixColumns. In this transformation, each column of the dual-rail State matrix is multiplied by a circulant maximum distance separable matrix. This MixColumns function takes four dual-rail bytes as inputs and four dual-rail bytes as outputs, where each input byte affects all four output bytes. The multiplication of the State array element with 2 in the dual-rail domain is realized by 1-bit left shift of dual-rail signals followed by a conditional NCL XOR operation. The multiplication with 3 is implemented in a similar fashion but it involves an additional NCL XOR operation.

(4) *NCL AddRoundKey*. AddRoundKey transformation performs a byte level dual-rail XOR operation on the dual-rail output of MixColumn and corresponding dual-rail Round Key.

6. Spatial Temporal Random Dynamic Voltage Scaling (STRDVS) Augmentation of NCL AES for Higher SCA Resistance

Recently, Yang et al. [17] applied random dynamic voltage and frequency scaling (RDVFS) to synchronous cryptoprocessors to enhance resistance against side-channel attacks. By randomly changing the supply voltage, "noise" can be injected into the power trace, making the attack more difficult. The clock frequency changes with different supply voltages to avoid timing violation. However, since the circuits are synchronous, the change in clock frequency can be easily observed in the power trace and, using certain hypothesis, the voltage corresponding to the frequency can also be obtained. As such, the attack can still be successful. To alleviate the problem, [18] proposes to use random DVS (RDVS) only, without changing the clock frequency. However, the tight timing constraint gives little room to do the voltage scaling.

It is obvious that the security enhancement highly depends on how much "noise" can be injected; this in turn depends on how much room is available for the voltage scaling. We argue that RDVS is more suitable for QDI designs for two reasons. First, there will be no timing constraint as in the synchronous or bounded-delay counterparts, leaving more room for voltage scaling. Second, since there is no clock signal, fewer gates will switch simultaneously and thus the power supply noise is reduced. Accordingly, the noise margin is increased, providing even more room for voltage scaling.

Different from [17, 18], in addition to changing the supply voltage randomly over time (temporal randomness), we propose to supply different random voltages over different regions in the chip (spatial randomness). Since NCL is self-timed and event-driven, difference in latencies among the regions caused by STRDVS is *inherently tolerated* unlike the clocked counterpart. Such spatial and temporal RDVS (STRDVS) in NCL will maximize the noise injected and thus the resistance to side-channel attacks.

Spatial and temporal random dynamic voltage scaling (STRDVS) is especially suitable for delay-insensitive designs to provide additional resistance to side-channel attack and to further reduce the power consumption as a byproduct [19]. The reason for QDI circuits to still have vulnerabilities is the imbalanced load capacitances between the two rails of a signal. Although the total number of switching is independent of data pattern, the switching activities between the two rails are different. For example, passing consecutive DATA1s makes Rail1 switch all the time, while passing consecutive DATA0s makes Rail0 switch all the time. Since most likely the two rails drive different loads, power is still imbalanced across data patterns and is still coupled with data being processed. A number of literature proposed various techniques to mitigate this problem.

6.1. Leveraging TRNG for the Proposed STRDVS NCL Cryptohardware. TRNG (true random number generator) is widely used for designing hardware systems for secure applications such as secure wireless communications, electronic financial transactions, smart cards, mobile computing, and secure RFID. Unlike PRNG (pseudorandom number generator) which always gives the same number sequence for a particular seed state (i.e., thereby less secure), TRNG are based on microscopic phenomena that generate a low-level, statistically random "noise" signal with high information entropy [20], such as thermal noise, oscillator drift, the photoelectric

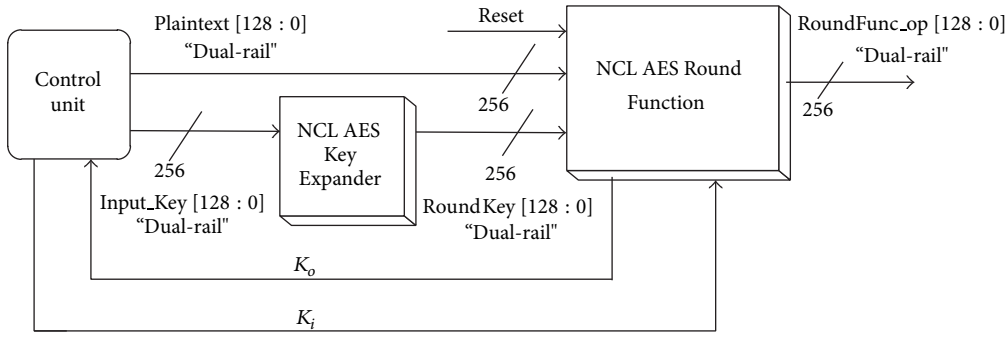

Figure 8: Block diagram of NCL AES Round Function top-level architecture.

effect, or other quantum phenomena [21]. There exist various TRNG designs for hardware implementation purposes including ones that are reported in [22–30]. One good example is TRNG1 IP (intellectual property) core by IP Cores, Inc [31]. TRNG1 features a high entropy source (i.e., either 128 or 256 bits) and satisfies Federal Information Processing Standard (FIPS) Publication 140-2 Annex C (i.e., "approved" random number generator) from the US National Institute of Standards and Technology (NIST) [32] and passes the requirements of the NIST SP 800-22 test suite [33].

The proposed NCL AES components leverage a TRNG for the proposed STRDVS technique for even higher resistance over SCA by intentionally injecting noise. Since TRNG already exists in most secure HW systems, it is not an overhead to the proposed design.

6.2. Spatial/Temporal Randomness & Granularity of STRDVS. The entire circuit is divided into several regions, and different randomly generated voltage control signals from TRNG are supplied to dynamically scale the voltage level in each region. Since NCL is asynchronous and event-driven, difference in latencies among the regions caused by STRDVS is *inherently tolerated* unlike the clocked counterpart. For example, suppose the entire circuit is divided into 56 voltage regions with eight dynamically scaling voltage levels. Then, each region will need a 3-bit randomly-generated voltage control signal. Accordingly, the 8-bit random number generator can yield $C_3^8 = 56$ different random control signals for 56 regions. As such, the temporal randomness can be achieved.

Figure 9 shows a gated signal from TRNG controlling the supply voltage of a STRDVS region as an example. In order for STRDVS to enhance side-channel attack resistance, the power difference due to the change in supply voltage (i.e., for the same input bit) must be comparable with the power difference due to the change in input bit (i.e., for the same supply voltage). As such, the correlation between the input data and the power consumption is substantially reduced. Thereby, the difference in power traces can hardly be used to identify input switching. However, scaling down the voltage has a direct impact on the latency of the processor. Accordingly, the lowest possible voltage that can keep the latency of our NCL processor within the tolerable bound should be determined at design time.

With that determined, we still need to determine two critical parameters: the number of voltage levels K (i.e., *temporal granularity*) and the number of voltage domains L (i.e., regions with different supply voltages, *spatial granularity*). Larger K and L can result in increased security as more noise is injected into the power trace; on the other hand, they may also increase the area and design complexity. As a future work, we will investigate the tradeoffs between area, power, latency, and security and find out the optimal setting of the parameters. In addition, a natural property of our STRDVS method is that the level of security is related to the encryption/decryption data rate: a high data rate gives little room to perform voltage scaling and thus little room to improve the security. It will also be interesting to see a tradeoff curve between the encryption/decryption data rate and the level of security.

7. Experimental Verification of the Proposed Design

7.1. Functional Verification of the Proposed Design. The conventional synchronous implementation and the proposed NCL AES Key Expander and NCL AES Round Function have been implemented in VHDL for a comparative study. The functional verification simulations of these designs have been performed with Mentor Graphics ModelSim. The proposed designs have been functionally verified completely using a large set of test vectors from [1]. A sample set of test vectors is presented in Figure 10 and the corresponding functional verification results are presented in Figures 11, 12, and 13.

7.2. Weighted Average Simultaneous Switching Output (WASSO) Analysis. WASSO tool is an utility of Xilinx PlanAhead suite that validates signal integrity of the device based on the I/O pin and bank assignments made in the design.

This analysis gives a measure of the amount of simultaneous switching occurring in the design. So, we used this analysis to determine the variation in switching activity across both AES Round Function designs. The results obtained were plotted and presented in Figure 14. The implementation platform chosen for carrying out WASSO analysis is Xilinx Virtex-5 FPGA. As switching activity directly depends on

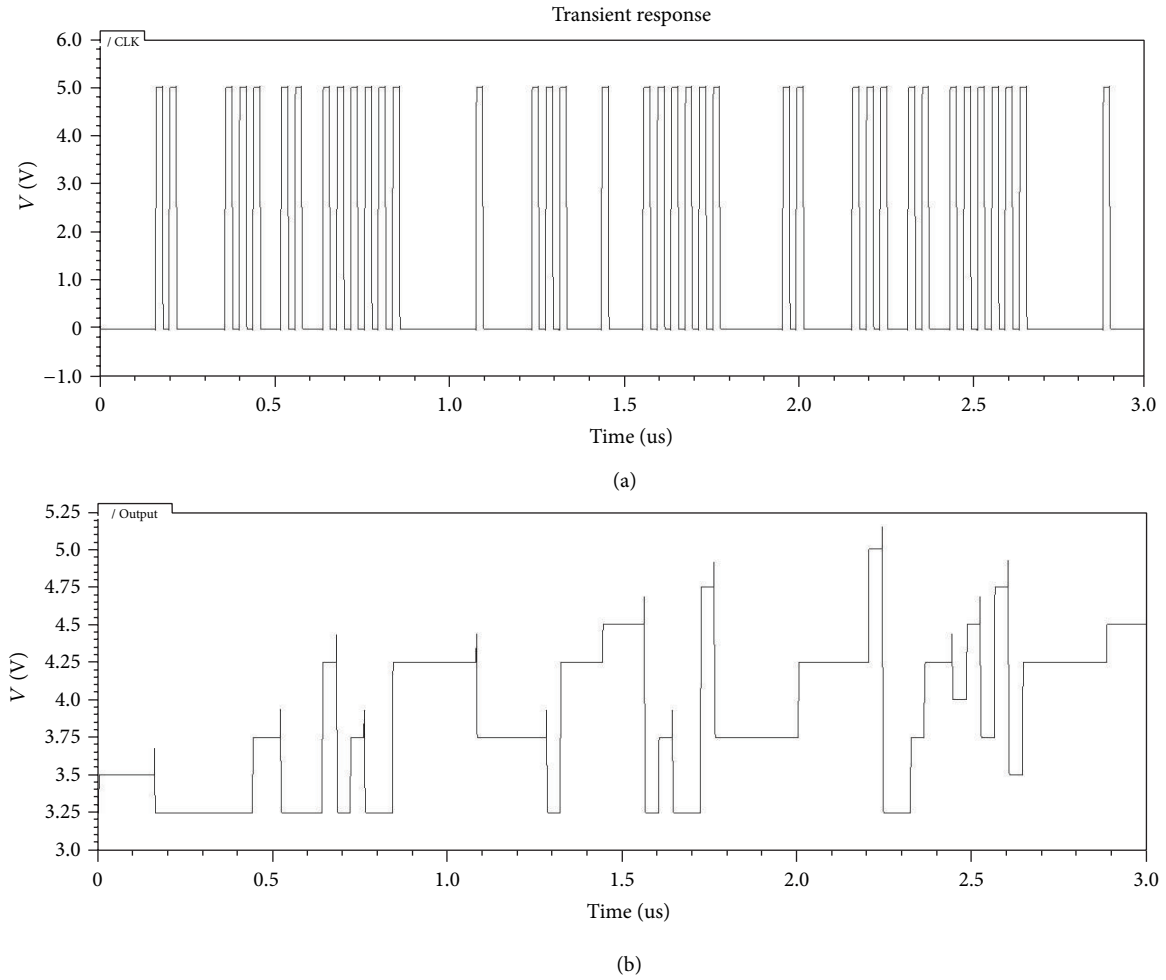

Figure 9: Waveforms of the gated signal from TRNG (a) to generate temporal randomness in the final supply voltage ranging from 3.25 V to 5.0 V at 0.25 V resolution (b).

Plaintext	3243F6A8885A308d313198A2E0370734
Key	2B7E151628AED2A6ABF7158809CF4F3C
Ciphertext	A49C7FF2689F352B6B5BEA43026A5049

Figure 10: A set of sample AES test vectors used for Figures 11~13.

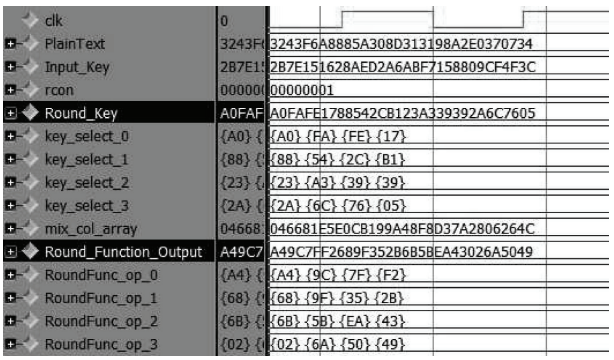

Figure 11: Functional verification result for synchronous design.

the number of simultaneously switching outputs, switching activity can be reduced if SNR gets reduced.

From Figures 14(a) and 14(b), it can be observed that the switching activity in the proposed design is lessened to a considerable extent and is also more uniform as compared to its synchronous counterpart. This reduction decreases the amount of unintentionally leaked information and the uniformity makes it more difficult to exploit the remaining leaked information to carry out SCAs.

7.3. Effects of Switching Activity on Signal-to-Noise Ratio. According to (2), it is clear that SNR is directly proportional to var(P_{expl}). The P_{expl} is a combination of two quantities: P_{oprn} and P_{data}. But var(P_{oprn}) is zero as we are considering a DPA attack, in which we perform the same operation again and again but with different input data. So, var(P_{expl}) becomes equal to var(P_{data}). The P_{data} is data-dependent and is a function of switching activity. So, the reduction of switching activity observed from WASSO simulations will translate into reduction of P_{data} of all the points on the power trace. This overall reduction of P_{data} will translate into reduction of var(P_{expl}) and consequently reduction of SNR.

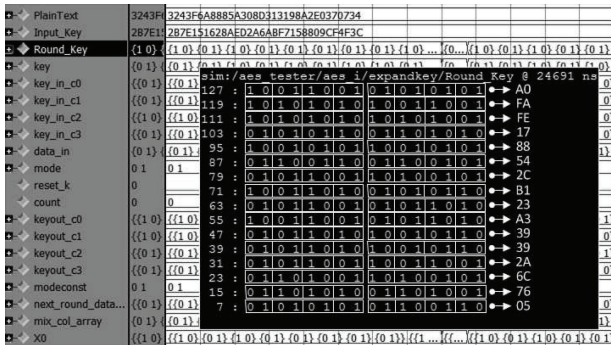

Figure 12: Functional verification result for the proposed NCL based Key Expander design.

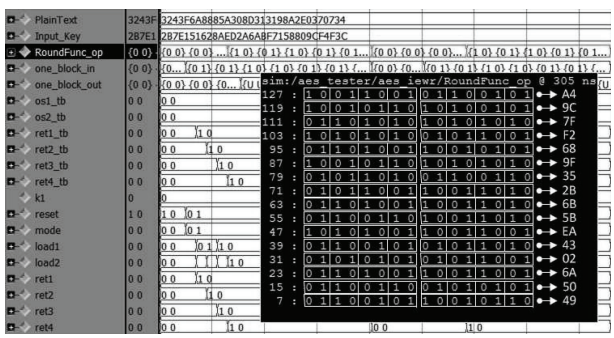

Figure 13: Functional verification result for the proposed NCL based Round Function design.

Additionally, as discussed previously, power consumption of a cryptosystem is heavily dependant on Hamming weight of data it processes. Due to this, equal Hamming weights of all inputs in our proposed design will enable our NCL design to maintain a uniform power consumption and thereby a uniform SNR on power trace. Thus, the proposed design enables the cryptosystem to have a reduced and uniform SNR, which is a key element for enhancing security.

By using the switching activity results, we performed parametric simulations and plotted SNR of NCL design in comparison to the synchronous approach. These approximate results are presented in Figure 15(a). Using this SNR data, Figure 15(b) shows how variation in SNR influences number of traces that an attacker must collect to perform a successful DPA attack. As SNR ratio decreases, performance of this NCL based approach keeps getting better. So, this is the advantage of employing NCL for cryptosystem design.

7.4. Power Benefits. In AES implementations, the SubBytes transformation which entirely depends on the S-box is the most crucial factor deciding the energy performance of the AES itself. More than 50% of entire power is dependent on this step [34–36]. Due to the use of novel NCL S-box design, we achieve a 22% reduction in power consumption [4] at this SubBytes step. So, this reduction will cause significant improvement in the energy efficiency of the proposed NCL based design approach.

7.5. Hardware Implementation and Power Trace Analysis. In the previous section, the performance of our proposed design was evaluated using software simulations. However, to get a more accurate performance analysis, simulations on the hardware implementation are necessary. In this section, we discuss in detail the procedure used for hardware implementation experiment of the proposed design and the synchronous AES. Additionally, we present the power trace data obtained from the power measurements on the hardware implementations and discuss the variations between this obtained data for the two designs. Figure 16 shows the side-channel attack standard evaluation board (SASEBO-GII board) [37] that is used as the basic platform in this experiment.

The reason for choosing this FPGA board as a platform for hardware implementation is that this board has been specifically designed for security evaluation of cryptographic circuits and for the purpose of side-channel attack experiments. There are two FPGA cores in this board that can be utilized. The first FPGA is a cryptographic FPGA which is a Xilinx Virtex-5 series FPGA. The second one is the control FPGA which is a Spartan-3A series FPGA. These FPGAs are connected through a general-purpose input/output common bus. The AES Round Function and Key Expander circuits are implemented in the cryptographic FPGA and the configuration circuit is programmed into the configuration FPGA. The purpose of separating these two circuits is to prevent the power trace of the configuration circuit from interfering with the power trace of the cryptographic circuit so that the measurements of power traces, which decide the resistance of the design to power analysis attacks, can be done fairly.

For the purpose of power trace measurement, shunt resistors are present on FPGA board which utilize core V_{DD} and/or ground lines of cryptographic FPGA to give an accurate measurement of the cryptographic FPGA power consumption. These measurements can be captured by an oscilloscope via a voltage probe.

Figure 17 presents the experimental setup used for power trace analysis. For making a qualitative comparison, in terms of security, between the quality of power traces of the conventional design and the proposed NCL design, we supply a set of three inputs to both designs. As the same inputs are applied to both designs, this enables us to evaluate the performance of different circuits to the same input data.

If we are able to prove that the following two features of the power trace are true for NCL based design, then we can conclude that the proposed approach enhances security. They are as follows. (1) The power trace is more uniform compared to synchronous design for the same input; and (2) the power trace of NCL based approach exhibits a higher degree of similarity between all the three different input cases as compared to the similarity exhibited by synchronous approach.

So, in order to perform a qualitative comparison, we applied a series of three Plaintexts, which are shown in Figure 18, to both cryptosystem designs and encrypted it with the same key. Then, we recorded the power traces for each of these cases for both designs and compared their quality in terms of security. The results are presented in Figures 19 to 24.

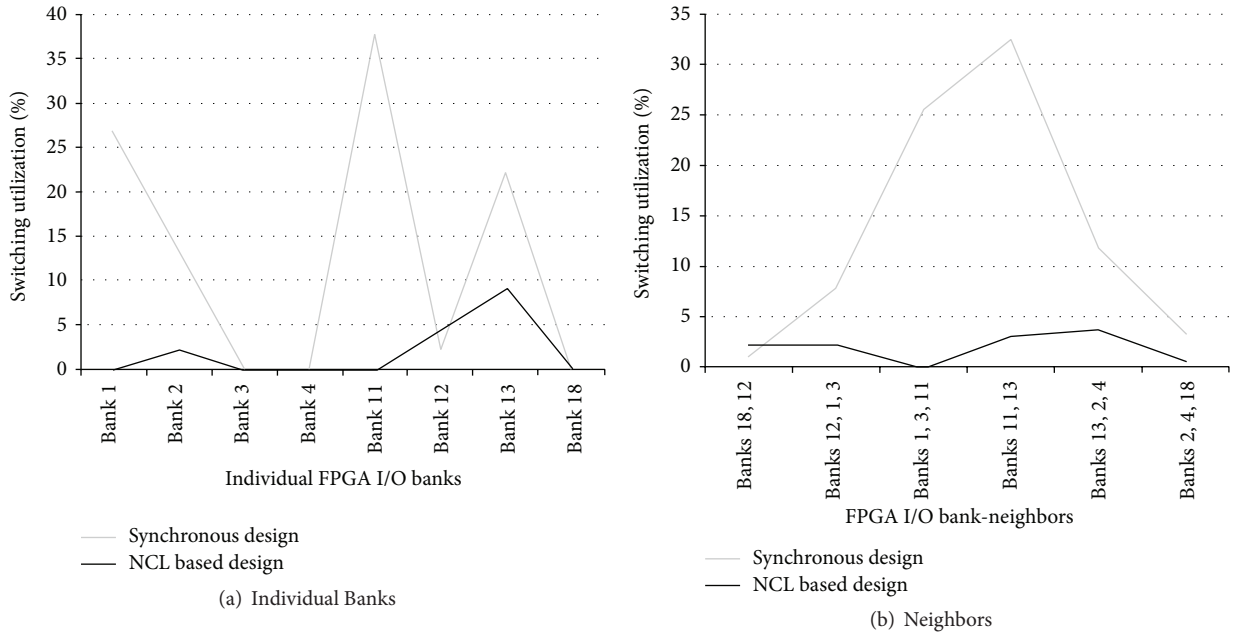

Figure 14: WASSO utilization plots for individual banks and neighbors.

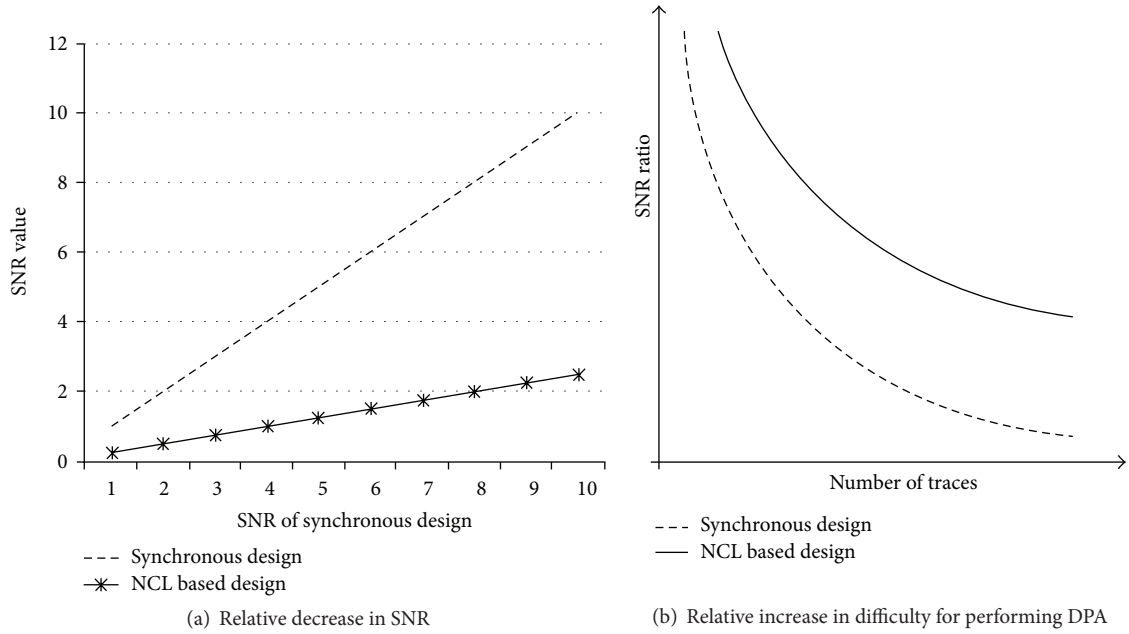

Figure 15: Comparison of SNR and difficulty of performing successful DPA for both designs.

From Figures 20, 22, and 24, we can clearly see that the power waveforms look considerably similar for the proposed design in all the three cases even when the input Plaintext is different. But on the contrary for synchronous design, from Figures 19, 21, and 23, we can see that the power trace has clear variations between the three cases, as represented by ovals. These variations as discussed previously can be effectively exploited to compromise security. But, in case of proposed design, we do not see any clear variations between the three traces. In addition to the lack of these variations in the proposed design, we can also see that the waveforms are far more uniform as compared to their synchronous counterparts.

So, with this increased uniformity and with high degree of similarity between power traces for different Plaintexts, we can conclude that security is improved to a considerable extent due to inherent benefits of NCL.

Figure 25 shows the power trace corresponding to NULL-DATA wavefronts in the hardware implemented design. Figure 26 presents the propagation delay in the hardware

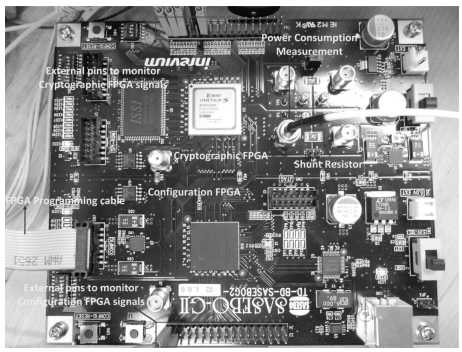

Figure 16: Side-channel attack standard evaluation FPGA board (SASEBO-GII).

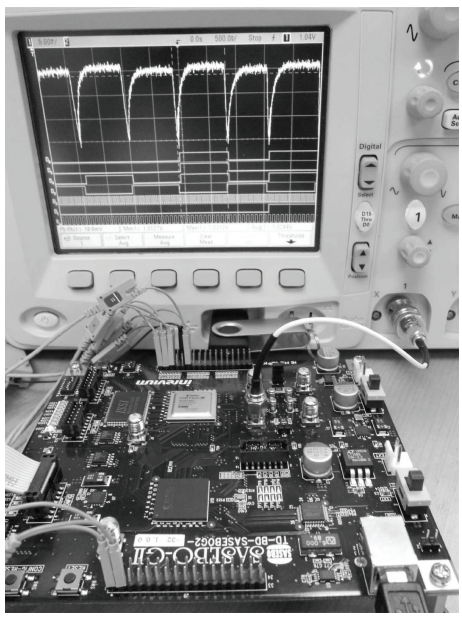

Figure 17: Experimental setup for power trace measurement.

Plaintext 1	3243F6A8885A308d313198A2E0370734
Plaintext 2	3243F6A8885A308d313198A2E0370735
Plaintext 3	3243F6A8885A308d313198A2E0370736
Key	2B7E151628AED2A6ABF7158809CF4F3C

Figure 18: Plaintexts and Key used for power trace analysis.

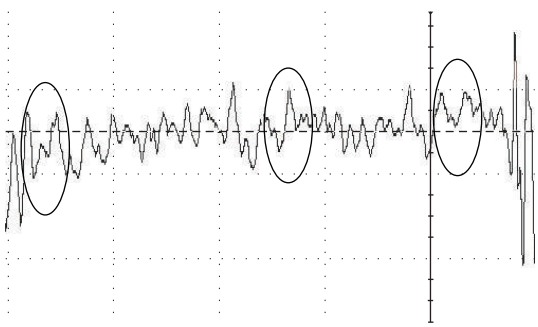

Figure 19: Power trace of synchronous cryptosystem for Plaintext 1.

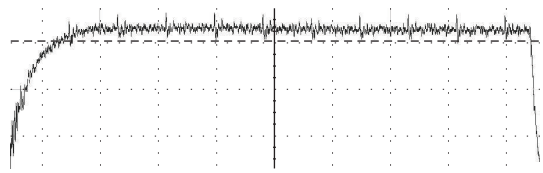

Figure 20: Power trace of asynchronous cryptosystem for Plaintext 1 (DATA).

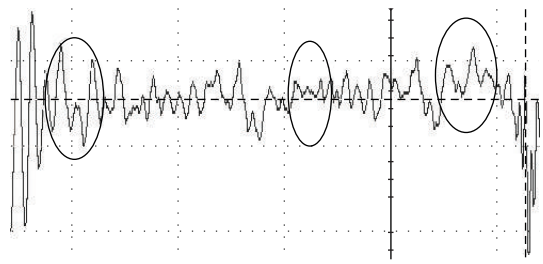

Figure 21: Power trace of synchronous cryptosystem for Plaintext 2.

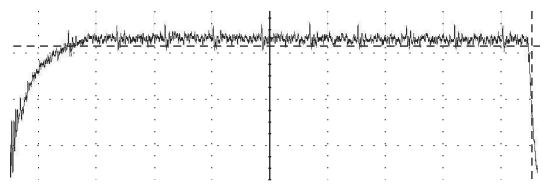

Figure 22: Power race of asynchronous cryptosystem for Plaintext 2 (DATA).

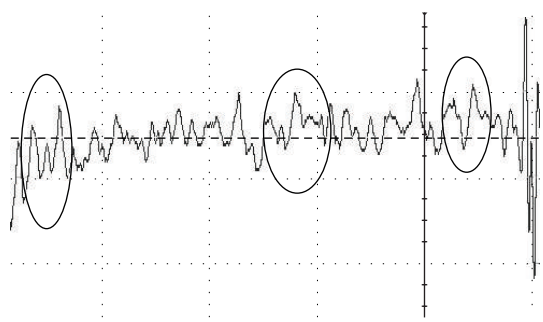

Figure 23: Power trace of synchronous cryptosystem for Plaintext 3.

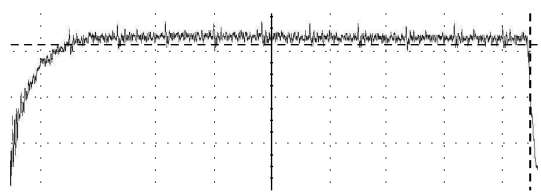

Figure 24: Power trace of asynchronous cryptosystem for Plaintext 3 (DATA).

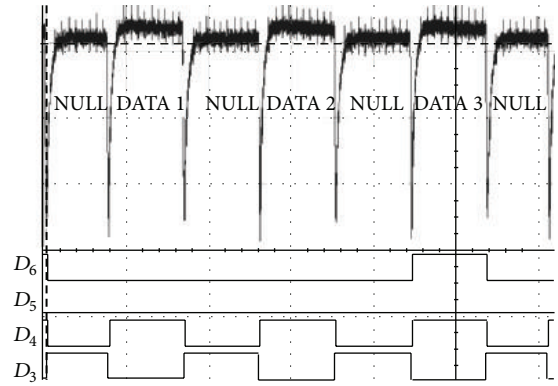

Figure 25: Power traces of NULL-DATA wavefronts in hardware implementation of proposed design.

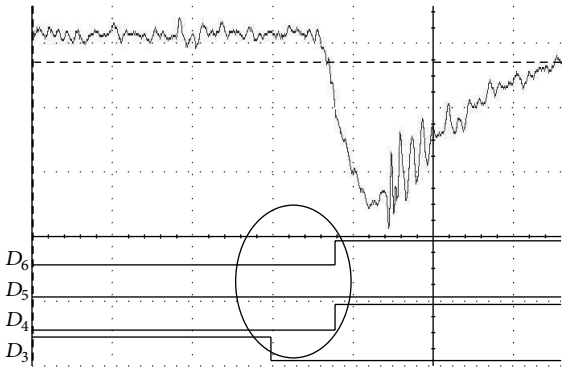

Figure 26: Propagation delay in NCL based design.

implementation of the proposed design. After the input is applied, output arrives after 40 ns.

8. Conclusion and Future Work

A novel asynchronous design approach for the two main components of AES, which are the Key Expander and Round function, is reported and validated in this work. This research is being used as the basis for a research project that aims to tape out a silicon chip of NCL AES design, which can be used to carry out more performance evaluation experiments. Contrary to the existing countermeasures which do not target the source of SCA problem and try to find solutions in later stages, the proposed approach combines the merits of (1) NCL design paradigm for balanced switching profile and event-driven operation and (2) spatial/temporal random dynamic voltage scaling (STRDVS) for injecting random noise to mitigate the source of the SCA problem, which is side-channel information leakage. In addition to providing power analysis SCA resistance, our approach also enhances resistance to EMA SCAs. Qualitative comparisons between the proposed approach and the traditional synchronous design have been conducted to verify merits of the proposed design. Both software simulation and hardware implementation results validate the effectiveness and correctness of our approach. In the future, the efficacy of the proposed design approach and its augmentation with STRDVS technique will be evaluated by performing an actual side-channel attack like the DPA or correlation power analysis (CPA).

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] NIST, *Advanced Encryption Standard (AES), FIPS PUB 197*, National Institute of Standards and Technology, 2001.

[2] K. Tiri and I. Verbauwhede, "A dynamic and differential CMOS logic style to resist power and timing attacks on security ICs," *ACR Eprint Archive, Report*, vol. 66, p. 2004, 2004.

[3] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE '04)*, vol. 1, pp. 246–251, IEEE Computer Society, February 2004.

[4] J. Wu, Y. Kim, and M. Choi, "Low-power side-channel attack-resistant asynchronous S-box design for AES cryptosystems," in *Proceedings of the 20th Symposium on Great Lakes Symposium on VLSI*, pp. 459–464, ACM, Houston, Tex, USA, May 2010.

[5] C. Sui, J. Wu, Y. Shi, Y. Kim, and M. Choi, "Random dynamic voltage scaling design to enhance security of NCL S-box," in *Proceedings of the 54th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '11)*, pp. 1–4, August 2011.

[6] T. Sugawara, Y. Hayashi, N. Homma et al., "Mechanism behind information leakage in electromagnetic analysis of cryptographic modules," in *Information Security Applications*, vol. 5932 of *Lecture Notes in Computer Science*, pp. 66–78, Springer, 2009.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO '99*, pp. 388–397, Springer, 1999.

[8] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[9] P. N. Fahn and P. K. Pearson, "IPA: a new class of power attacks," in *Cryptographic Hardware and Embedded Systems*, pp. 173–186, Springer, New York, NY, USA, 1999.

[10] J. Zhao, J. Han, X. Zeng, A. Li, and Y. Deng, "Differential power analysis and differential fault attack resistant AES algorithm and its VLSI implementation," in *Proceedings of the 9th International Conference on Solid-State and Integrated-Circuit Technology (ICSICT '08)*, pp. 2220–2223, Beijing, China, October 2008.

[11] A. Abrial, J. Bouvier, M. Renaudin, P. Senn, and P. Vivet, "A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 7, pp. 1101–1107, 2001.

[12] P. Kocher, "Design and validation strategies for obtaining assurance in countermeasures to power analysis and related attacks," in *NIST Physical Security Testing Workshop*, Honolulu, Hawaii, USA, 2005.

[13] S. C. Smith and J. Di, "Designing asynchronous circuits using NULL convention logic (NCL)," *Synthesis Lectures on Digital Circuits and Systems*, vol. 4, no. 1, pp. 1–96, 2009.

[14] T. S. Messerges, E. A. Dabbish, and R. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[15] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, vol. 31, Springer, New York, NY, USA, 2007.

[16] A. Kak, "Lecture Notes on Computer and Network Security by Avinash Kak," 2012, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf.

[17] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in *Proceedings of the Design, Automation and Test in Europe (DATE '05)*, pp. 64–69, IEEE, Munich, Germany, March 2005.

[18] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proceeding of the 20th International Conference on VLSI Design held jointly with 6th International Conference on Embedded Systems (VLSID '07) Held jointly with 6th International Conference on Embedded Systems*, pp. 854–862, Bangalore, India, January 2007.

[19] H. Geng, J. Wu, J. Liu, M. Choi, and Y. Shi, "Utilizing random noise in cryptography: where is the Tofu?" in *Proceedings of the 30th IEEE/ACM International Conference on Computer-Aided Design (ICCAD '12)*, pp. 163–167, November 2012.

[20] Wikipedia, "Entropy (information theory)," 2013, http://en.wikipedia.org/wiki/Shannon_entropy.

[21] "Hardware random number generator," 2013, http://en.wikipedia.org/wiki/TRNG.

[22] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109–119, 2007.

[23] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in *Proceedings of the ACM/SIGDA 12th ACM International Symposium on Field-Programmable Gate Arrays (FPGA '04)*, pp. 71–78, ACM, usa, February 2004.

[24] V. Fischer and M. Drutarovský, "True random number generator embedded in reconfigurable hardware," in *Cryptographic Hardware and Embedded Systems—CHES 2002*, vol. 2523 of *Lecture Notes in Computer Science*, pp. 415–430, Springer, Berlin, Germany, 2003.

[25] T. E. Tkacik, "A hardware random number generator," in *Cryptographic Hardware and Embedded Systems—CHES 2002*, pp. 450–453, Springer, 2003.

[26] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 403–409, 2003.

[27] C. S. Pétrie and J. A. Connelly, "A noise-based ic random number generator for applications in Cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615–621, 2000.

[28] B. Jun and P. Kocher, *The Intel Random Number Generator*, Cryptography Research Inc. white paper, 1999.

[29] P. Hellekalek, "Good random number generators are (not so) easy to find," *Mathematics and Computers in Simulation*, vol. 46, no. 5-6, pp. 485–505, 1998.

[30] B. Barak, R. Shaltiel, and E. Tromer, "True random number generators secure in a changing environment," in *Cryptographic Hardware and Embedded Systems—CHES '03*, pp. 166–180, Springer, 2003.

[31] IP Cores Inc, "TRNG1: True Random and Pseudorandom Number Generator Core," 2013, http://www.ipcores.com/True_Random_Generator_TRNG_IP_core.htm.

[32] U. N. I. of Standards and T. (NIST), Approved Random Number Generators for FIPS PUB 1 40-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf.

[33] A. Rukhin, J. Soto, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2013, http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[34] S. Morioka and A. Satoh, "An optimized S-Box circuit architecture for low power AES design," in *Cryptographic Hardware and Embedded Systems-CHES 2002*, vol. 2523 of *Lecture Notes in Computer Science*, pp. 172–186, Springer, 2002.

[35] M. Kim, J. Kim, and Y. Choi, "Low power circuit architecture of AES crypto module for wireless sensor network," in *Proceedings of the World Academy of Science, Engineering and Technology*, vol. 8, pp. 146–150, 2005.

[36] F. Gurkaynak, *GALS System Design: Side Channel Attack Secure Cryptographic Accelerators*, Hartung-Gorre, 2006.

[37] R. C. for Information Security, "Side-channel Attack Standard Evaluation Board SASEBO-GII Specification," September 2009, http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-GII-en.html.