Design and Evaluation of Side Channel Attack Resistant Asynchronous AES Round Function

Siva Pavan Kumar Kotipalli1, KyungKi Kim2, Yong-Bin Kim3 and Minsu Choi1
1Department of Electrical and Computer Engineering, {sk7fc,choim}@mst.edu
Missouri University of Science & Technology, Rolla, MO 65409, USA
2School of Electronic Engineering, kkkim@daegu.ac.kr
Daegu University, Daegu, Korea
3Department of Electrical and Computer Engineering, ybk@ece.neu.edu
Northeastern University, Boston, MA 02115, USA

Abstract—A novel Asynchronous AES Round Function design is proposed in this paper, which offers increased Side-Channel Attack (SCA) resistance by combining the advantages of dual rail encoding and clock free operation. The design is based on a Delay Insensitive (DI) logic paradigm known as Null Convention Logic. By reducing switching activity and thereby Signal-to-Noise (SNR) ratio, the proposed design leaks far less side channel information than traditional approaches and this feature boosts SCA resistance of this approach. Functional verification and WASSO analysis simulations were carried out on both synchronous approach and the proposed NCL based approach using Xilinx simulation tools to validate the claims related to benefits of employing this novel dual rail design approach.

I. INTRODUCTION

The Advanced Encryption Standard (AES) [1] was very reliable in providing security for data until a few years ago, when researchers proved that side channel attacks were successful in compromising this security. Since the detection of power analysis and EM analysis SCA effectiveness, researchers have started exploring different approaches to design countermeasures.

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

This paper proposes a scalable dual rail AES Round Function design that incorporates the merits of Null Convention Logic (NCL). This paper has multiple contributions in the field of improving SCA resistance of cryptosystems through NCL:
1) This design approach reduces the amount of switching activity occurring in cryptosystem and thereby curtails the leaked power and improves resistance against Power Analysis SCA; 2) The switching activity reduction also reduces EM radiation side channel information emanating from cryptosystem and boosts the resistance of cryptosystem against EMA SCA [6]; 3) This round function design allows easy scaling for implementing it to entire AES algorithm of any of the following variants 128,192 or 256 bit; 4) It can also be easily scaled and implemented for different modes of AES like ECB, CFB, CBC etc; 5) The proposed design incorporates a power efficient NCL S-box design, which provides power benefits when compared to the conventional approach; 6) This design can also be effectively coupled with RVDS to enhance security to even greater extent as demonstrated previously for the AES S-box in [5].

II. VULNERABILITY OF SYNCHRONOUS AES ROUND FUNCTION DESIGN

The main flaws of synchronous AES implementation is its vulnerability to side-channel attacks. SCA utilize any of the following information: power consumption, switching activity, timing information, electromagnetic leaks or acoustic information emanating from cryptosystem to identify the secret key of the algorithm. The Power analysis SCA has proved to be an effective approach to compromise security. The attack is based on the fact that the leaked power consumption information actually contains information about the module’s behavior. Out of the different types of Power analysis attacks, the Differential Power Analysis (DPA) [7] are the most effective at revealing the hidden private key. These DPA attacks make use of statistical analysis and multiple waveforms to identify secret keys [8].

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 and 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 SCAs.
III. INFLUENCE OF SWITCHING ACTIVITY ON SCA

A. 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:

\[ P_{\text{dyn}} = A C L V_{DD}^2 f \]  

\( P_{\text{dyn}} \) is the power consumed, \( A \) is the switching activity factor, i.e., the fraction of the circuit that is switching, \( C \) is the switched capacitance, \( V \) 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. Thomas S. Messerges et al. [9] discussed the role of SNR ratio in determining the success probability of a DPA attack.

\[ SNR = \frac{\sigma_\text{expl}}{\sigma_\text{noise}} \]  

In (2), \( \sigma_\text{expl} \) is the variance of exploitable component of power consumption and \( \sigma_\text{noise} \) is the variance of noise component. By reducing this exploitable power information \( P_{\text{expl}} \) we can lower the SNR ratio. The lower the SNR ratio is, the lower is the leakage, so performing the DPA attack becomes harder.

B. Role of Switching Activity on EMA SCA

The switching activity also influences the EM radiation leaked from the cryptosystem. The voltage fluctuation caused by ground bounce can be expressed as:

\[ \Delta V = L_{\text{eff}} M \frac{dI}{dt} \]  

where \( L_{\text{eff}} \) 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 from (3), it is clear that if we are able to reduce the switching activity \( M \), we can reduce the information leakage due to \( \Delta V \), as \( \Delta V \propto M \).

IV. NULL CONVENTION LOGIC

NCL is a delay insensitive asynchronous paradigm. The delay insensitivity of NCL circuits is achieved by dual-rail and quad-rail logic [10]. For the current research we have opted the dual rail approach. A dual rail signal can effectively represent four states. Out of them, the three valid states are: DATA0, DATA1, NULL. The fourth state in which both the rails are asserted is considered illegal state. The valid states DATA0, 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.

Advantages of using Null Convention Logic : The main benefit of using dual-rail logic is that, constant power consumption can be achieved since the signals are 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. 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. The downside is dual-rail method generally incurs area overhead.

The independence of power consumption from input data and the overall reduction in power consumption, which are attributed to dual rail logic and monotonic transitions respectively, boost the SCA resistance of AES cryptosystem. Additionally, the above mentioned merits also reduce the electromagnetic interference making the AES more robust.

V. NCL AES ROUND FUNCTION

The top-level architecture of the proposed design is presented in Figure 1. In this control unit, the input data which is in ordinary binary format is read from a file and is converted into dual rail inputs by Single rail to Dual-rail converter. Ko is the output acknowledgement signal coming out of the NCL Round function. It acts like clock signal for the other units in the controller. The converter and multiplexer (MUX) are controlled by Ko. When Ko is ‘1’, it means NCL Round function is ready for NULL wavefront, then MUX will send all 0’s to “PlainText”, “Input Key” and “Round Key” to nullify the NCL Round function. Otherwise, MUX will select the dual rail data that is output from the converter.

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

1) NCL SubBytes: This transformation is presented in Figure 2, where each dual-rail byte of the State matrix is substituted independently by another 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 presented in Fig. 3, 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 offset 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 shown in Fig. 4, takes four dual-rail bytes as input and outputs four dual-rail bytes, 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 shown in Fig. 5, performs a byte level dual-rail XOR operation on the dual-rail output of MixColumn and corresponding dual-rail round-key.

### VI. RESULTS

#### A. Functional Verification of Proposed Design

The traditional synchronous implementation and the proposed NCL AES Round function have been implemented in VHDL. The functional verification simulations were performed with Mentor Graphics ModelSim. The proposed design has been functionally verified completely using a large set of test vectors which were chosen from [1]. A sample test vector is presented in Table I and the corresponding functional verification results are presented in Fig. 6 and Fig. 7.

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>3243F6A8885A308d313198A2E0370734</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>2B7E151628AED2A6A6HF7158809CF4F3C</td>
</tr>
<tr>
<td>Ciphertext</td>
<td>A49C7FF2689F352B6B5BEAEAA3026A3039</td>
</tr>
</tbody>
</table>

**TABLE I: Test Vectors**

---

#### B. WASSO Analysis

Weighted Average Simultaneous Switching Output (WASSO) tool is an utility of Xilinx PlanAhead suite that validates signal integrity of the device. 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 designs. The results are presented in the tables II, III. As switching activity directly depends on the number of simultaneously switching outputs, if we are able to decrease switching activity we can reduce the SNR. The implementation platform chosen for carrying out WASSO analysis is Xilinx Virtex-5 FPGA.

**TABLE II: WASSO Results - Individual Banks**

<table>
<thead>
<tr>
<th>Package Banks</th>
<th>WASSO Allowance</th>
<th>WASSO Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Banks</td>
<td>Synchronous Design</td>
<td>NCL Design</td>
</tr>
<tr>
<td>Bank 1</td>
<td>100%</td>
<td>26.70%</td>
</tr>
<tr>
<td>Bank 2</td>
<td>100%</td>
<td>15.30%</td>
</tr>
<tr>
<td>Bank 3</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>Bank 4</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>Bank 11</td>
<td>100%</td>
<td>37.80%</td>
</tr>
<tr>
<td>Bank 12</td>
<td>100%</td>
<td>2.20%</td>
</tr>
<tr>
<td>Bank 13</td>
<td>100%</td>
<td>22.20%</td>
</tr>
<tr>
<td>Bank 18</td>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**TABLE III: WASSO Results - Neighbors**

<table>
<thead>
<tr>
<th>Package Banks</th>
<th>WASSO Allowance</th>
<th>WASSO Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbors</td>
<td>Synchronous Design</td>
<td>NCL Design</td>
</tr>
<tr>
<td>Bank 18, 12</td>
<td>100%</td>
<td>1.1%</td>
</tr>
<tr>
<td>Bank 12, 1, 3</td>
<td>100%</td>
<td>7.8%</td>
</tr>
<tr>
<td>Bank 1, 3, 11</td>
<td>100%</td>
<td>25.6%</td>
</tr>
<tr>
<td>Bank 11, 13</td>
<td>100%</td>
<td>11.9%</td>
</tr>
<tr>
<td>Bank 13, 2, 4</td>
<td>100%</td>
<td>3.3%</td>
</tr>
</tbody>
</table>

**TABLE IV: WASSO Results - Neighbors**

---

**Fig. 6: Functional Verification Result for Synchronous Design**

**Fig. 7: Functional Verification Result for the proposed NCL based Design**

**Fig. 8: WASSO Utilization Plots**
From the Fig. 8 (a), (b) we can observe that the switching activity in NCL based approach is lessened to a considerable extent and is also more uniform as compared to its synchronous counterpart. This reduction and uniformity in switching limits the amount of unintentionally leaked information, that can be used for carrying out SCAs.

### C. Effects of Switching Activity on Signal-to-Noise ratio

According to (2), it is clear that SNR is directly proportional to $\text{Var}(P_{\text{expl}})$. The $P_{\text{expl}}$ is a combination of two quantities $P_{\text{open}}$ and $P_{\text{data}}$. But $\text{Var}(P_{\text{open}})$ 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 $\text{Var}(P_{\text{expl}})$ becomes equal to $\text{Var}(P_{\text{data}})$. The $P_{\text{data}}$ 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 $P_{\text{data}}$ of all the points on the power trace. This overall reduction of $P_{\text{data}}$ will translate into reduction of $\text{Var}(P_{\text{expl}})$ and consequently reduction of SNR.

Additionally, 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 an 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 9(a). Using this SNR data, Figure 9(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.

![Fig. 9: Comparison of SNR and Difficulty of performing successful DPA for both designs](image)

### D. 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 [11]. 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.

### VII. Conclusion

A novel design approach for AES Round function based on NCL is reported and validated in this work. The proposed design, with slight modifications is valid for any mode of AES or any key size of AES. Unlike existing countermeasures which do not eliminate the source of SCA problem and try to find solutions in later stages, the proposed approach combines the merits of dual rail encoding with asynchronous design approach to eliminate 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.

We performed quantitative comparisons between the proposed approach and the traditional synchronous design and proved that our approach is beneficial. Simulation results validate the effectiveness and correctness of our approach.

### REFERENCES


