Secured Low Power Overhead Compensator Look-Up-Table (LUT) Substitution Box (S-Box) Architecture

Pammu, Ali Akbar; Chong, Kwen-Siong; Gwee, Bah Hwee

2016

Pammu, A. A., Chong, K.-S., & Gwee, B. H. (2016). Secured Low Power Overhead Compensator Look-Up-Table (LUT) Substitution Box (S-Box) Architecture. 2016 IEEE International Conference on Networking, Architecture and Storage (NAS), 16252998-.

<https://hdl.handle.net/10356/80480>

<https://doi.org/10.1109/NAS.2016.7549420>

© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/NAS.2016.7549420>].

Downloaded on 26 Apr 2023 21:00:22 SGT

Secured Low Power Overhead Compensator Look-Up-Table (LUT) Substitution Box (S-Box) Architecture

Ali Akbar Pammu*, Kwen-Siong Chong and Bah-Hwee Gwee
School of Electrical and Electronic Engineering
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
Email: *ali1@e.ntu.edu.sg

Abstract — Substitution-Box (S-Box) is an important security building block for the Advanced Encryption Standard (AES) algorithm. However, its (high) power dissipation always compromises its security feature under Correlation Power Attack (CPA). In this paper, we propose a secured and low power overhead LUT based S-Box architecture embodying a novel multiplexing circuit and/or a compensator. We achieve these attributes as follows. First, we employ AND and OR gates to realize the multiplexing circuit therein in a regular structure to minimize the delay and power variations for every input pattern, hence mitigating the security risk against CPA. Second, we augment a compensator to complement the multiplexing circuit to further minimize the power variations within the LUT based S-Box. Based on the Sakura-X FPGA board, we realize six AES designs, three embodying reported S-Box architectures and the other three leveraging on our multiplexing circuit and compensator. We show that our AES design, embodying our LUT based S-Box architecture with the AND/OR-gate multiplexing circuit and compensator, has the highest security feature (against CPA) compared with the reported designs, featuring $10\times$ to $300\times$ better security.

Keywords — Compensator, Multiplexer, Look-Up-Table, Substitution-Box, Correlation Power Analysis

I. INTRODUCTION

The proliferation of Internet of Things (IoT) [1] is inevitable, in which the communication data are shared/transferred through internet. The availability of online shared information, in system IoTs, is vulnerable due to unauthorized party (i.e. adversary) who can intercept and abuse the information. Therefore, cybersecurity [2], which concerns about data protection of confidential information, has to be considered when designing system IoTs. Although the communication data are often encrypted, e.g. by Advanced Encryption Standard (AES) [2], the IoT hardware could still be losing security due to various forms of attack, including Side-Channel-Attack (SCA) [6]. The SCA is defined as a method used to reveal the secret information by utilizing its leakage physical parameters, such as power dissipation [6], electromagnetic signals [7] and timing information [8]. Particularly, Correlation Power Analysis (CPA) [6] is one form of SCAs, and is surprisingly effective and amazingly simple to get the encrypted data deciphered by analyzing the correlation of the power dissipation and processed data.

There are many reported counter-methods to mitigate CPA. The general preventive ideas are based on the “masking” and “hiding” approaches [6]. The masking approach aims to mask the relationship/correlation between the encryption/decryption operations and their ensuing power dissipation, and conversely, the hiding approach aims to hide the same through breaking the link between data and power

dissipation. These counter-methods were exemplified in some reported AES designs [9], showing various degrees of security robustness, and trade-offs among overall power dissipation, speed/data rate and area overheads. In an AES implementation, the critical building block is the substitute-box (S-Box) that obscures the relationship between the key and the encrypted data, and it is one of the most power dissipative building blocks, accounting 50%-60% overall power [7]. Hence, power-efficient and yet high security robustness S-Box remains highly desirable.

There are two general types of implementations for S-Box, one is based on the conventional computational means [3], and the other one on the Look-Up-Table (LUT) [9]. The LUT implementation is generally preferred due to its low overheads and high speed attributes. An LUT implementation consists of a pre-stored LUT circuit and multiplexing circuits. In this paper, we investigate and propose power-efficient and yet secured look-up-table (LUT) based S-Box architectures as a solution in IoT applications. We only consider the hiding approach in our study. Our study is based on the Field-Programmable-Gate-Array (FPGA) which provides a more flexible and programmable implementation for IoTs

There are three key significances in our study. First, we propose to use AND and OR gates to realize the multiplexing circuits embedded in the LUT based S-Box. The AND and OR gates are structured to minimize the power and delay variation in the S-Box design for every input pattern, hence increasing the security feature against CPA. Second, we propose to include compensators in the LUT based S-Box to further minimize the power variations due to the data dependency of the input signals. The compensator is only applied to the multiplexing circuits and no compensator is required for the pre-stored LUT circuit. Third, we comprehensively compare six AES designs embodying various S-Box architectures in terms of security feature (against CPA), hardware resources, power dissipation and speed. Of the six AES designs, three are based on the reported designs, and three are our designs, leveraging on our LUT based architecture and compensators. Based on the measurements, we show that our AES design, embodying our LUT based S-Box architecture with AND/OR gates and with a compensator, has the highest security, $10\times$ to $30\times$ better than reported design. We also show that the hardware and power overheads of our designs are modest, and our proposed S-Box architectures are suitable for low-to-medium speed secured ubiquitous electronics, including IoT applications.

This paper is organized as follows. Sec. II reviews the AES algorithm, the various S-Box implementations and CPA attack. Sec. III describes our proposed Power-Efficient LUT

based S-Box architectures. Sec. IV shows the measurement results on AES implementations and finally, conclusions are drawn in Section V.

II. REVIEW: ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM, SUBSTITUTION BOX (S-BOX) AND CORRELATION POWER ANALYSIS (CPA)

In this section, an overview of the AES algorithm is briefly described followed by a description of its pertinent building block S-Box and the attacking technique in CPA.

A. Advanced Encryption Standard (AES)

The AES algorithm has been employed in a variety of security systems including the defense and banking applications since 2001 [6]. It is categorized as a symmetric-key encryption algorithm, in which the transmitter and receiver employ the same *key* for encryption and decryption respectively. The AES algorithm transforms a plaintext into a ciphertext using the key by several iterative processes. The processed data block length is fixed at 128 bits, while the key length can be 128, 192, or 256 bits [3]. For the 128, 192 and 256 key length, 10, 12 and 14 round of iterations are required respectively.

Fig. 1 depicts the flow chart of the encryption process in the AES algorithm. Each round of iteration consists of four operations, namely S-Box, ShiftRow, MixColumn and AddRoundKey, except for the last round which does not have MixColumn operation. The decryption is a reverse operation of the encryption process, i.e. transforming the ciphertext into plaintext (original message) using the same key. The decryption structure can be derived by inverting the encryption structure directly [3]. The equivalent decryption structure has the same sequence of operation as in the encryption structure, thus, the resources sharing is allowed for the encryption and decryption process.

Fig. 1. Flow chart of Advanced Encryption Standard (AES)

B. Substitution-Box (S-Box)

The S-Box is the one of the most critical blocks in AES and dissipates relatively high power. Two main sub modules in the S-Box which are the multiplicative inversion and the Affine transformation [7]. The idea is to enable a non-self-inverse function in S-Box to effectively protect the data against the deciphering attack. There are two general types of implementations for S-Box, one is based on the conventional computational means, and the other one on the LUT matrix. Figs. 2 (a) and (b) depict the block diagrams of the conventional computational S-Box and of the LUT based S-Box respectively. Each input to the S-Box is a 1-byte of intermediate data x , and the S-Box will generate 1-byte of output $S(x)$. In the Fig. 2(a), the output $S(x)$ is obtained through a series of computations (labeled as “A” to “F” and the matrix multiplication). As the 8-bit x processes through all these operations to generate $S(x)$, the S-Box dissipates different power for different x . Thus, the power dissipation could corresponded with the value of the processed data in the S-Box, potentially leaking information under CPA.

- A = isomorphic mapping
- A⁻¹ = inverse isomorphic mappings
- B = square operation in GF(2⁴)
- C = sum operation in GF(2⁴)
- D = multiplication operation in GF(2⁴)
- E = multiplication with constant operation
- F = inverse operation in GF(2⁴)

(a)

(b)

Fig. 2. Block diagram of S-Box: (a) based on computational means, and (b) Based on Look-Up-Table (LUT)

In Fig. 2 (b), for each possible input x , $S(x)$ can be pre-computed and stored in an LUT. The corresponding output can then be retrieved directly from the LUT for a given input x . In this context, multiplexing circuits are used to select a corresponding output data from the 256 Byte LUT which functions as a ROM. The LUT based S-Box is generally

advantageous for small area and low power implementation. However, the study of the LUT based S-Box architectures remains insufficient. From security concern viewpoint, we observe that 256 Byte LUT [9] is constantly voltage-biased without dissipating any dynamic power, only the multiplexing circuits dissipate dynamic power according to the input x . Viewed from a different perspective, should the power variation in the multiplexing circuits be as small as possible, the security features (against CPA) will be significantly enhanced.

C. Correlation Power Analysis (CPA) Attack

The CPA attack is a byte-based power analysis attack. Each byte of key (sub-key) is estimated by means of 256 possible values ($2^8 = 256$). The CPA attack is performed by analyzing the correlation coefficient ($r_{i,j,t}$) of two variables, power model ($X_{i,j,m}$), and the power traces ($Y_{t,m}$), for $i = 1, \dots, 16$ sub-keys, $j = 1, \dots, 256$ sub-key candidates, $t = 1, \dots, N$ sampling points, as follows:

$$r_{i,j,t} = \frac{\sum_{m=1}^n (X_{i,j,m} - \bar{X}_{i,j})(Y_{t,m} - \bar{Y}_t)}{\sqrt{\sum_{m=1}^n (X_{i,j,m} - \bar{X}_{i,j})^2} \sqrt{\sum_{m=1}^n (Y_{t,m} - \bar{Y}_t)^2}} \quad (1)$$

The correct sub-key, i , corresponds to the highest $r_{i,j,t}$ at the particular sub-key candidate, j , and sampling point of power traces, t . The common power model used is either Hamming Distance (HD) or Hamming Weight (HW). The higher number of power traces required to reveal the correct sub-key, the higher CPA-resistant to the hardware, hence more secured.

III. SECURED S-BOX ARCHITECTURES

In this section, we describe and propose LUT based S-Box architectures with and without compensator to enhance the security feature in the overall AES implementation. The compensators are used to further mitigate the power variation for each input pattern in order to prevent CPA.

A. LUT based S-Box Architectures without Compensators

Figs. 3 (a) and (b) depict the reported LUT based S-Box architecture based on the multiplexers, and our proposed LUT based S-Box architecture based on the AND and OR gates for the multiplexing circuits. In Fig. 3 (a), the multiplexing circuits are designed by cascading 4-level ($L=1$ to 4) 4-to-1 multiplexers. This architecture is simple, however, the multiplexers collectively dissipate various power depending on the input x ; the power dissipation in the multiplexing circuits is still somewhat data-dependent.

Fig. 3 (b) is a more power-balanced LUT based S-Box architecture where AND gates are first used to allow the specific LUT value to pass through followed by cascading 8-level ($L=1$ to 8) 2-input OR gates. The architecture in Fig. 3 (b) balances the propagation delay paths for each input pattern, and likely dissipates a similar power profile for each input pattern, hence increasing the security feature (against CPA). The reasons are explained as follows. The AND gates first serve as filters, removing the unwanted switching whereas the unwanted switching may happen in Fig. 3 (a). The unwanted switching are often data-dependent, posing security risks under CPA. Only the specific LUT value will be passed over to the AND gates based on the 8-to-256 decoders. The 2-input OR gates (as opposed to other higher-in OR gates) are used because the 2-input OR gate has less power variation among its input pattern combination. For every input pattern, only one OR gate in each level is enabled to pass the specific LUT value.

B. Proposed LUT based S-Box Architectures with Compensators

The vulnerability of normal S-Box (uncompensated) is mainly due to the data dependency of x , dissipating power, which correlates to the processed data. An improved method is to include a compensator to further make an even more relatively similar power profile for each input pattern. This concept has been previously applied by using a Gate-Level approach such as dual-rail logic, e.g. Wave-Dynamic-Dual-Rail-Logic (WDDL) [14], Sense-Amplifier-Based Logic

Fig. 3 LUT based S-Box architectures: (a) Reported design based on MUX gates, and (b) Proposed design based on AND/OR gates

[13], Pre-Charge-Static-Logic [10], etc. We apply the same concept in our LUT based S-Box architectures here.

Since the 256 Byte LUT is voltage-biased at the specific voltage level, we do not need to compensate the power dissipation in the 256 Byte LUT. The 256 Byte LUT only dissipates leakage power but not dynamic power. Assuming that the leakage power is unlikely to be data-dependent, we propose to compensate only the multiplexing circuits (see Fig. 2 (a)), making a similar power profile for every input pattern. In this respect, we are proposing a semi-block level compensator in the LUT based S-Box.

Fig. 4 depicts the block diagram of our proposed LUT based S-Box architecture with a compensator. The compensator is essentially generating logic complementary signals of the multiplexing circuits. In this way, the number of logic 1s and the number of logic 0s collectively propagating to the multiplexing circuits and the compensator is always the same. Viewed differently, the switching (dynamic) power in the S-Box would be likely the same for every input pattern.

Fig. 4. Proposed LUT based S-Box with a compensator; only the multiplexing circuits are (power) compensated

The architecture used to realize the compensator is the same in the multiplexing circuits. Fig. 5 (a) and (b) depicts the LUT based S-Box architectures with the compensator by using the MUX and AND/OR gates respectively. MUX gates are advantageous for lower hardware overheads and speed, but data-dependency still exists in the MUX when the input x changes from one pattern to another pattern. On the other hand, the architecture using the AND/OR gates is

Fig. 5: LUT based S-Box architectures with compensator: (a) Design based on MUX gates, and (b) Design based on AND/OR gates

advantageous to mitigate the data-dependency as discussed previously.

IV. RESULTS

To provide a comprehensive comparison, we implement three 128-bit AES (AES-128) designs containing three different S-Box architectures without any compensators. We also implement three AES-128 designs containing three different S-Box architectures with compensators. For easy reference, Table I tabulates these designs with a short description on their respective S-Box architectures. Designs #1, #2, #4 are based on the reported designs [12]-[14]. Particularly, for Design #4, WDDL logic is used for realize the multiplexing circuits. Designs #3, #5 and #6 are proposed designs in part leveraging on the architectures discussed in Sec. III earlier. All these designs are implemented using the Sakura-X FPGA board [7]. For fair comparison, a 24MHz global clock is used to synthesize all these designs.

Table I
AES-128 Designs embodying various S-Box architectures

AES-128	S-Box Architecture
#1	Computational means (see Fig. 2 (a))
#2	MUX LUT (see Fig. 3 (a))
#3 (proposed)	LUT with AND/OR gates (see Fig. 3 (b))
#4	Computational means with WDDL
#5 (proposed)	Mux LUT with compensator (see Fig. 5(a))
#6 (proposed)	LUT with AND/OR gates & compensators (see Fig. 5(b))

Fig. 6 depicts the experimental setup where a 10-bit ADC 2.5Giga samples/second oscilloscope is used to record the power dissipation for various AES-128 designs. Table II tabulates the sub-keys used for the encryption process during the experiments. We attack the last round of the AES-128 designs by using the Hamming Distance power model. The detailed comparisons are provided in the following sub-sections.

Fig. 6. The Experimental Setup

Table II
The sub-keys used for the experiments

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key	13	11	1D	7F	E3	94	4A	17	F3	07	A7	8B	4D	2B	30	C5

A. Security Robustness

We attack all the six designs in order to find out the minimum number of power traces required to break the keys. The higher number of power traces required, the higher security feature in the S-Box architecture. Fig. 7 depicts the correlation coefficients at the different sample points at the last round of AES algorithm for Design #3. The bold line represents the correct key whereas the grey lines represent other (incorrect) keys based on 20,000 power traces. The key is broken at the sample point 32 which has the highest correlation coefficient. Fig. 8 depicts the correction coefficient versus the number of power traces for various keys for Design #3. The real key is depicted in bold line. From Fig. 8, we can see the key can be retrieved by using at least 14,243 power traces.

Fig. 7. Correlation coefficients at various sample points for design #3. The bold line indicates the correction coefficients using the correct key where the highest correlation happens at the sample point 32.

Fig. 8. Correlation coefficients vs the number of power traces for design #3. The bold line indicates the correction coefficients using the correct key. The key is broken by using ~14k power traces.

Table III tabulates the minimum number of power traces required to break at least one key and all the 16 keys in the AES-128 designs embodying various S-Box architectures. The readings in the parenthesis are normalized with respect to the reading of Design #1. We can comment the following. First, from breaking at least one key to all 16 keys, we require 29% to 53% more power traces. Second, Design #1 (by using the computational means) is very vulnerable to CPA where 455 power traces are sufficient to break all the keys. Third, of all the designs without compensators (Designs #1 to #3), our Design #3 is the best, about 31× more secured than Design #1 and slightly better than Design #2. Fourth, when

the compensators are included, the security feature is significantly enhanced. For example, when compared to Design #1, Designs #4 to 6 (with compensators) feature 89× to 308× more secured. Fifth, although Design #4, embodying the reported WDDL, is promising, our proposed designs (Designs #5 and #6) embodying the compensators in the multiplexing circuits, are even better. Specifically, Design #5 and Design #6 are respectively 1.6× and 3.5× more secured than Design #4.

Table III. The number of power traces to break keys

Design	Min Power Traces to break at least one key	Min Power Traces to break all the keys
#1	252 (1×)	455 (1×)
#2	9,495 (38×)	13,642 (30×)
#3	10,256 (41×)	14,258 (31×)
#4	21,030 (83×)	40,561 (89×)
#5	35,480 (140×)	65,345 (144×)
#6	65,200 (259×)	140,000 (308×)

B. Measured Characteristics on AES-128 Designs

We compare the hardware resources, the power dissipation and minimum delay for the AES-128 designs embodying various S-Box architectures. As before, the readings in the parenthesis are normalized with respect to the reading of Design #1.

For hardware resources, we collectively group the registers and the LUT logic together for analysis. Design #4 embodying WDDL has the largest overheads and Design #1 using the computational means is similarly having large overheads. As expected, the AES-128 designs embodying LUT based S-Box architectures have less overheads. Design #2 has the lowest overhead and it is expected as the MUX circuits can highly optimized by the Xilinx synthesis tool. Among all the AES-128 designs embodying LUT based S-Box architectures, our Design #6 has high overheads but it is comparable to Design #1.

For (average) power dissipation, Design #1 dissipates the highest followed by Design #4. This is despite Design #4 uses more resources. The AES-128 designs embodying the LUT based S-Box dissipate relatively low power. It is also expected that the LUT based S-Box architecture with compensator dissipate higher power than the same LUT based S-Box architecture without compensator. Particularly, Design #5 dissipates 1.17× more power than Design #2 and Design #6 dissipates 1.89× more power than Design #3. The almost doubling of power in Design #6 to Design #3 further justifies that the power is compensated due to a similar

amount dynamic power dissipation dissipated in the compensator (when compared to the multiplexing circuits). In other words, the compensator works well at the expense of higher power dissipation.

Although all the AES-128 designs are synthesized based on the 24MHz clock, we can still analyze the minimum delay of each designs. Design #2 embodying the MUX LUT S-Box can operate fastest followed by Design #3. Design #6 has the worst minimum delay, but is still achieving > 91MHz clock frequency – such frequency would be more than sufficient for many low-to-medium speed IoT applications.

C. Trade-off Comparison

We further tabulate in Table IV a composite trade-off figure-of-merit, the product of power dissipation and the inverse of the minimum number of power traces, to quantify various AES-128 designs. From Table IV, Design #1 is uncompetitive due to its high power dissipation and yet low security feature. Our Design #6 has the lowest value and is suitable for low power and yet high security robustness for IoT applications.

Table V

Composite Trade-off Figure-of-Merit: Product of Power and Inverse of Minimum Power Traces

Design	Power (P, mW)	Inverse of Min Power Traces ($\frac{1}{M}, 10^{-3}$)	Product ($P \times \frac{1}{M}$)
#1	7.3	2.198	16.045
#2	2.8	0.073	0.204
#3	2.7	0.070	0.189
#4	3.9	0.025	0.098
#5	3.3	0.015	0.050
#6	4.2	0.007	0.029

V. CONCLUSIONS

We have proposed an LUT based S-Bix architecture by using AND and OR gates to realize the multiplexing circuits to minimize the power variation for each input pattern. We have further augmented a compensator to compensate the power variation in the multiplexing circuits, reducing the power leakage information to mitigate CPA. We have shown that our AES-128 design, embodying our LUT based S-Box architecture with AND/OR gates and with a compensator, has the highest security than the reported designs. The power overhead in our AES design embodying our LUT S-Box architecture is low, we recommended our AES design for secured ubiquitous electronics, including IoTs applications.

Table IV. Device utilization in FPGA of AES-128 algorithm implementation with and without compensator

S-Box Architecture	Hardware Resources			Power (mW)			Min Delay (ns)
	Registers	LUT Logic	Total	Max	Min	Average	
#1	952	3,117	4,069 (1.00×)	10.9	3.7	7.3 (1.00×)	9.1 (1.00×)
#2	868	1,706	2,574 (0.63×)	3.7	1.9	2.8 (0.38×)	5.6 (0.62×)
#3 (proposed)	1,021	2,947	3,968 (0.98×)	4.6	0.8	2.7 (0.37×)	6.1 (0.67×)
#4	948	7,445	8,393 (2.06×)	6.7	1.0	3.9 (0.53×)	10.7 (1.18×)
#5 (proposed)	868	2,563	3,431 (0.84×)	5.4	1.2	3.3 (0.45×)	7.9 (0.87×)
#6 (proposed)	1,060	3,132	4,192 (1.03×)	5.3	3.1	4.2 (0.58×)	10.9 (1.20×)

ACKNOWLEDGMENT

This research work was supported by Agency for Science, Technology and Research, Singapore, under SERC 2013 Public Sector Research Funding, Grant No: SERC1321202098. The authors thank A*STAR for the kind support in funding this research.

REFERENCES

- [1] M. Nitti; V. Pilloni; G. Colistra; L. Atzori, "The Virtual Object as a Major Element of the Internet of Things: a Survey," in *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1-1
- [2] S. Mangard, "Keeping Secrets on Low-Cost Chips," in *IEEE Security & Privacy*, vol. 11, no. 4, pp. 75-77, July-Aug. 2013.
- [3] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, Feb. 2014.
- [4] Xinmiao Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 957-967, Sept. 2004.
- [5] S. Chunghun, W. Jun, S. Yiyu, K. Yong-Bin, and C. Minsu, "Random dynamic voltage scaling design to enhance security of NCL S-box," *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1-4, 2011.
- [6] W. Jun, S. Yiyu, and C. Minsu, "Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, pp. 2765-2775, 2012.
- [7] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks*. US: Springer 2007.
- [8] Y. Hori, T. Katashita, A. Sasaki and A. Satoh, "SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA," *The 1st IEEE Global Conference on Consumer Electronics 2012*, Tokyo, 2012, pp. 657-660.
- [9] S. Ghosh and I. Verbauwhede, "BLAKE-512-Based 128-Bit CCA2 Secure Timing Attack Resistant McEliece Cryptoprocessor," in *IEEE Transactions on Computers*, vol. 63, no. 5, pp. 1124-1133, May 2014.
- [10] C. Teegarden, M. Bhargava and K. Mai, "Side-channel attack resistant ROM-based AES S-Box," *Hardware-Oriented Security and Trust (HOST)*, 2010 *IEEE International Symposium on*, Anaheim, CA, 2010, pp. 124-129.
- [11] K-S. Chong, K. Z. L. Ne, W-G. Ho, L. Nan, A. Akbar, B-H. Gwee and J. S. Chang, "Counteracting differential power analysis: Hiding encrypted data from circuit cells," *International Conference on Electron Devices and Solid-State Circuits (EDSSC)*, IEEE, 2015, pp. 297-300.
- [12] C. Teegarden, M. Bhargava and K. Mai, "Side-channel attack resistant ROM-based AES S-Box," *Hardware-Oriented Security and Trust (HOST)*, 2010 *IEEE International Symposium on*, Anaheim, CA, 2010, pp. 124-129.
- [13] K. Tiri and I. Verbauwhede, "Charge recycling sense amplifier based logic: securing low power security ICs against DPA [differential power analysis]," *Solid-State Circuits Conference*, 2004. *ESSCIRC 2004*. *Proceeding of the 30th European*, 2004, pp. 179-182.
- [14] Y. Li, K. Ohta and K. Sakiyama, "Revisit fault sensitivity analysis on WDDL-AES," *Hardware-Oriented Security and Trust (HOST)*, 2011 *IEEE International Symposium on*, San Diego CA, 2011, pp. 148-153.