Title	Highly secured arithmetic hiding based S-Box on AES-128 implementation(Main Article)
Author(s)	Pammu, Ali Akbar; Chong, Kwen-Siong; Gwee, Bah Hwee
Citation	Pammu, A. A., Chong, K.-S., & Gwee, B. H. (2016). Highly secured arithmetic hiding based S-Box on AES-128 implementation. 2016 International Symposium on Integrated Circuits (ISIC). (pp. 1-4).
Date	2016
URL	http://hdl.handle.net/10220/42766
Rights	© 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/ISICIR.2016.7829736].

Highly Secured Arithmetic Hiding based S-Box on AES-128 Implementation

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*–We propose an arithmetic hiding technique on Advanced Encryption Standard (AES) algorithm implementation to highly secure the algorithm against Side-Channel Attack (SCA). The arithmetic operations run parallel with Substitution-Box (S-Box) operation of the AES to hide the correlated leakage power dissipation with processed data. There are two key features in our proposed hiding technique. First, the function of the arithmetic hiding is independent with S-Box operation and its power dissipation is dominant over the S-Box. Therefore, the dependency of the total power dissipation with processed data in the AES algorithm is relatively low. Second, the security level of proposed technique against SCA based on Correlation Power Analysis (CPA) and Correlation Electromagnetic Analysis (CEMA) attack are increased by 119× and 63× respectively, compared with unprotected S-Box. This is due to the leakage physical parameters (i.e. power dissipation and EM emanation) which is generated by the arithmetic operation hides the leakage parameters of the S-Box operation. Based on the measurement results on Sakura-X FPGA board, which performs AES-128 algorithm, our proposed technique dissipates 3.8mW and features 1.18× higher power dissipation than the unprotected S-Box implementation. However, our proposed arithmetic hiding technique is highly secured, as the result of CPA and CEMA attack require 38,000 power traces and 44,000 EM traces respectively to reveal the secret key. The required number of traces are significantly higher than the unprotected S-Box, which is only 319 power traces and 691 EM traces respectively to uncover the same secret key.**

***Keywords*–Arithmetic Hiding, Side-Channel Attack, AES, Substitution- Box, CPA, CEMA**

I. INTRODUCTION

Side Channel Attack (SCA) has been an emerging topic in cryptographic research for the last two decades. It is defined as method to extract the secret key of cryptographic algorithm implementation, such as Advanced Encryption Standard (AES) algorithm, by utilizing the leakage physical parameters [1]. This method is based on the fact that processed data in chip processor is corresponded with its physical parameters while running certain algorithm (i.e. AES algorithm). The physical parameters such as power dissipation [1], Electro-Magnetic (EM) emanation [2], temperature [3] and timing [4] are measured during the encryption (or decryption) activities to be statistically analyzed with processed data to reveal the secret key. However, due to its simplicity on measurement, power dissipation and EM are two major parameters used in SCA compared with other parameters [1].

In the real implementation of the SCA, the adversary (unauthorized party to receive the information) intercept the communication channel and acquire the ciphertext, at Antenna_3, as depicted in Fig. 1. In this context, the ciphertext is transmitted from Antenna_1 to receiver, Antenna_2. At the same time, the adversary also measures the physical parameters (i.e. power dissipation or EM emanation) of the encrypted devices.

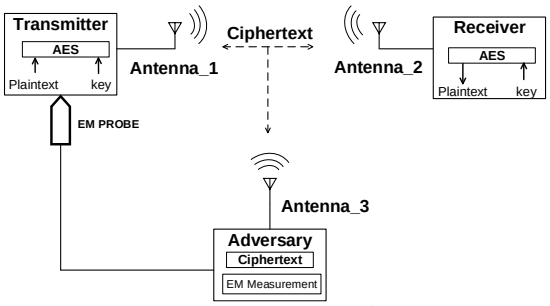


Fig. 1: Attacking scenario of SCA

Two common methods of SCA based on power dissipation and EM physical parameters, which are Correlation Power Analysis (CPA) and Correlation Electro-Magnetic Analysis (CEMA) respectively. These two correlation based method employ statistical analysis to evaluate the dependency between power dissipation/EM and processed data (i.e. in the function of ciphertext) [1] to reveal the secret key.

The countermeasure techniques have been developed as to prevent the leakage information in term of physical parameters to be corresponded with processed data of the encrypted devices. There are two main techniques in countermeasure, hiding and masking which are mainly on hardware and software approach respectively [6]. The fundamental idea of these countermeasure techniques is to break the dependency of the physical leakage parameters against the processed data.

The hiding technique is mainly focused on the physical parameters such as balancing the power dissipation to hide the correlation with the internal processed data of the encrypted device. There are two main approach in hiding technique, cell and block level approach. In the cell level, several techniques have been reported [1] such as Sense Amplifier Based Logic (SABL), Wave Dynamic Differential Logic (WDDL), Three-phase Dual-rail Pre-charge Logic (TDPL) and Pre-Charge Static Logic (PCSL) [6]. The concept of SABL is that it balances internal charges by fully charging and discharging all internal node for different processed data (i.e. '0' or '1'). However, during the implementation, the internal charges is not fully discharged due to small variation on the internal parasitic capacitance [6]. The WDDL and PCSL employ Pre-charge and Evaluation cycle with differential logic to make a constant power dissipation for different logic transition. In AES implementation, the WDDL occupies over 3.1× area, dissipate 3.7× dynamic power and 3.8× reduction in throughput compared with standard cell implementation [5]. In the PCSL implementation, the power dissipation tend to leak information during the pre-charge cycle [6] and hence vulnerable against CPA attack. The TDPL employs dual-rail dynamic logic with three-phase clocking system (Pre-charge, Evaluation and Discharge). The three-phase clock is to ensure that the remaining internal charge is fully discharge to

make a constant amount of charge for each cycle. However, the TDPL features 4.6× slower compared with conventional CMOS implementation [1].

Another hiding approach is at the block level in which the power dissipation is balanced directly at the main V_{DD} point of the encrypted device. The hiding techniques based on block level approach are a Switching Capacitor Current Equalizer (SCCE) [7], an intermittent Supply-Current Equalizer (SCE) [8] and A Dynamic Voltage and Frequency Switching (DVFS) [9]. The SCCE is the same principal as in the TDPL. The current equalizer implemented with integrated switching capacitors, which isolates the encryption circuits activity by equalizing the current. However, it is 33% power overhead 2× slower than conventional differential logic [8]. The SCE is an improvement of the SCCE performance, which is only at the vulnerable round of AES-128 (i.e. 1st and 10th rounds) implement the equalizer. The current equalizer techniques (i.e. SCCE and SCE) are both vulnerable against EM based attack by measuring the EM generated after the equalizer module. The DVFS hides the correlated power dissipation against SCA by dynamically changing the scale of the voltage and frequency during the encryption. The noise generated during the operation can be filtered (i.e. Finite Impulse Response (FIR) filter) with optimized parameters to increase the Signal-to-Noise Ratio (SNR). Therefore, the correlated power dissipation still can be detected and the key can be revealed with low number of power traces.

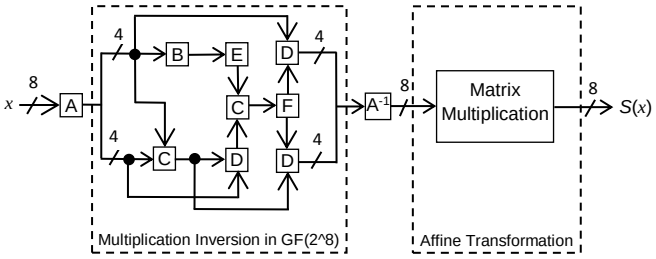
Another countermeasure technique is masking, where the main principal is to randomize the internal processed data to de-correlate with its physical leakage parameters. There are two main methods under the masking techniques, Boolean and Arithmetic masking. The main drawback of the masking technique is the requirement to mask and unmask of the masking variable, which affect the performance of the algorithm implementation.

In this paper, we propose arithmetic hiding technique on AES algorithm implementation by targeting the S-Box operation. This is due to the S-Box is non-linear operation which leaks more information compared with others AES operations such as AddroundKey, MixCoulumn and ShiftRow. Two key features in our proposed hiding technique. First, the function of the arithmetic hiding is independent with S-Box operation and its power dissipation is dominant over the S-Box. Therefore, the dependency of the total power dissipation with processed data in the AES algorithm is relatively low. Second, the security level is increased by 119× and 63× based on CPA and CEMA attack respectively compared with unprotected S-Box. This is due to the leakage physical parameters, which is generated by the arithmetic operation hides the leakage parameters of the S-Box operation. Based on the measurement results on Sakura-X FPGA board, which performs AES-128 algorithm, our proposed technique dissipates 4.8 mW and features 1.5× higher power dissipation than the unprotected S-Box implementation. However, our proposed arithmetic hiding technique is highly secured, as the result of CPA and CEMA attack require 19,000 power traces and 22,000 EM traces respectively to reveal the secret key.

This paper is organized as follows. Section II explains the S-Box of AES Algorithm. Section III describes the proposed arithmetic hiding S-Box. Section IV presents the measurement results on CPA and CEMA attack and finally, conclusions are drawn in Section V.

II. Substitution-Box (S-Box) of AES Algorithm

The S-Box is one of the critical operations in AES algorithm and it consists of two sub-modules [1], namely the multiplicative inversion sub-module in GF(2^8) and the Affine transformation sub-module as depicted in Fig. 2. 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 term of power, it dissipates 65% - 80% of the total power dissipation of the AES implementation [1]. Based on these two sub-modules, the S-Box features a non-self-inverse function, which effectively protects the data against the CPA attack.



A = isomorphic mapping
A^{-1} = inverse isomorphic mappings
B = square operation in GF(2^4)
C = sum operation in GF(2^4)
D = multiplication operation in GF(2^4)
E = multiplication with constant operation
F = inverse operation in GF(2^4)

Fig. 2: The two sub-modules of a conventional S-Box

Another implementation of the S-Box is Look-Up-Table (LUT) in which all the possible output (2^8 = 256) is stored in the LUT as depicted in Fig. 3. The analysis of the LUT [10] shows that the power dissipation is reduced significantly by 5.5× lower than conventional S-Box (10.5 to 1.9 in mW). However, the security features can only protect the key against CPA attack up to 13,000 power traces. This is due to the selection function (i.e. multiplexer) dissipates relatively small differences in dynamic power for different input and output of the S-Box.

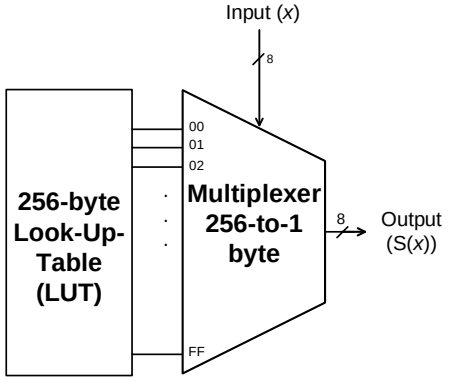


Fig. 3: LUT S-Box implementation

The data dependency with physical parameters is relatively high in the S-Box although the power dissipation can be significantly reduced by LUT technique. The variance of power traces for different input values is still detectable by CPA attack [10]. However, the low power dissipation at LUT architecture is possible to apply dummy operation, which hide the correlated power dissipation against CPA attack without sacrificing the power overhead.

III. Arithmetic Hiding on S-Box

The power dissipation of the encrypted devices is a measurement of the current (I_{DD}) and voltage (V_{DD}) consumed when processing one plaintext (i.e. 16 bytes). The power profile can indicate the number of iteration process of the AES algorithm to generate a ciphertext. During the measurement in oscilloscope, the sampling point of power measurement, contain a valuable information about the encryption algorithm which can be used to analyze the secrete information. Multiple of power dissipation measurement by making the operation (i.e. AES operation) occurs at the same sampling point is defined as power traces. The power traces is further applied in CPA attack by means of correlation coefficient with processed data.

The component of power traces [1] can be decomposed as the sum of an operation P_{OP}, processed data P_{DATA}, a noise P_{NOISE}, and constant component P_{CONST} as described in the Equation (1).

$$P_{TRACES} = P_{OP} + P_{DATA} + P_{NOISE} + P_{CONST} \quad (1)$$

The P_{OP} and P_{DATA} are two parameters of the power traces which highly affected by the algorithm and the processed data respectively. The P_{NOISE} is generated during the switching activities and the noise characteristic is different for different application (i.e. ASIC or FPGA). The noise could also could come from environment such as EM signal, which interfere the cable during measurement. However, the P_{NOISE} can be filtered out by means of FIR filter with optimized parameters and hence increase the SNR value. The P_{CONST} is relatively irrelevant to the CPA attack since the value is considered constant for different operation and processed data. In this context, the CPA attack only consider two components to leak out more information, which are P_{OP} and P_{DATA}.

In this research, the hiding technique is focused on the P_{OP} and P_{DATA} to de-correlate the physical parameters and the processed data. The main principal is to perform dummy operation ($P_{D.OP}$) and dummy variable ($P_{D.DATA}$) to hide the main power traces against CPA attack. Therefore, the total power traces is the summation the power dissipation of the two operations as described in Equation (2). Since the S-Box operation is the highly data dependent with the processed data, although at different architecture (i.e. LUT S-Box), the hiding is applied exclusively to the S-Box operation. The dummy operation and processed data are created independent and unrelated with S-Box to make each component in Equation (2) uncorrelated to each other.

$$Tot.\ P_{TRACES} = P_{OP} + P_{D.OP} + P_{DATA} + P_{D.DATA} \quad (2)$$

In order to hide completely the leak out information (P_{OP} and P_{DATA}), the power dissipation component of the dummy operations must be dominant over the correlated power dissipation. In this context, the total power traces is affected mainly by dummy operation as described in Equations (3) and (4).

$$Tot.\ P_{TRACES} = P_{OP}\downarrow + P_{D.OP}\uparrow + P_{DATA}\downarrow + P_{D.DATA}\uparrow \quad (3)$$

$$Tot.\ P_{TRACES} \simeq P_{D.OP} + P_{D.DATA} \quad (4)$$

The realization of the Equation (4) in arithmetic function is depicted in Fig. 4. The arithmetic operation is performed concurrently at the same clock cycle with S-Box LUT. The arithmetic hiding technique is applied at vulnerable rounds (i.e. the first and the last round of AES-128) due to consideration of power dissipation overhead. The controller is closed at vulnerable rounds and open for the rest of the rounds of AES-128 implementation.

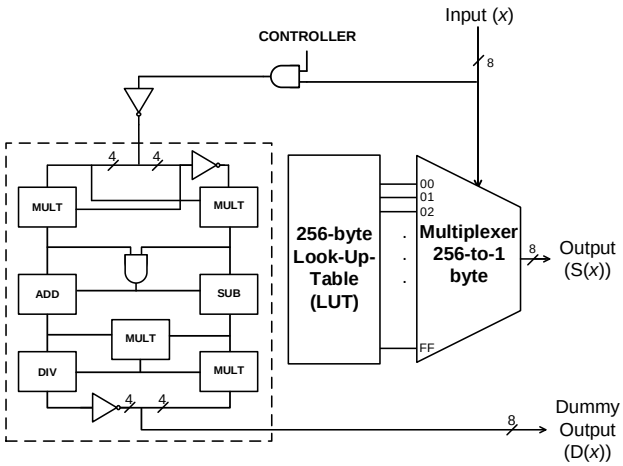


Fig. 4: Arithmetic operation is performed parallel with LUT based S-Box

The arithmetic-hiding negates the input (8-bit) of the S-Box and split into two 4-bits. The input is further processed by four types arithmetic function namely multiplications (MULT), a division (DIV), addition (ADD) and Subtraction (SUB) to generate independent power dissipation with LUT based S-Box. At the end of the operation, the two 4-bits is combined to produce the 8 bit dummy output (D(x)). The power dissipated by the arithmetic hiding is not randomly distributed and hence the values is unable to filter. This technique is highly secured compared with reported technique [9] in which the random power generated is filterable by simple FIR filter.

IV. Measurement Results

The experiment is conducted based on the Sakura-X board [2], to measure the power dissipation exclusively for the AES-128 implementation. The values of the 16 sub-keys are selected for the AES-128 algorithm in hexadecimal = (15, AE, A2, 3C, 07, 91, 3D, 38, 9F, 99, 2E, 95, AE, 50, 59, 88). The CPA and CEMA attack are a byte-based analysis attack. Each byte of key (sub-key) is estimated by means of 256 possible values (1 byte = 8 bits and possibility is 2^8 = 256), hence the correct sub-key is one of the 256 sub-key candidates. The CPA and CEMA attack are performed by analyzing the correlation coefficient ($r_{i,j,t}$) of two variables, power/EM model ($X_{i,j,m}$) and power/EM traces ($Y_{t,m}$), for i = 1, ⋯, 16 sub-keys, j = 1, ⋯, 256 sub-key candidates, t = 1, ⋯, 1000 sampling points, as shown in Equation (5):

$$r_{i,j,t} = \frac{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})(Y_{t,m}-\bar{Y}_t)}{\sqrt{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})^2}\cdot\sqrt{\sum_{m=1}^{n}(Y_{t,m}-\bar{Y}_t)^2}} \quad (5)$$

The correct sub-key, i, corresponds to the highest $r_{i,j,t}$ at particular sub-key candidate, j, and sampling point of power traces, t.

The power dissipation, measured during the encryption processed, is 3.8 mW at the last round iteration, which is 1.1875× higher than LUT based S-Box (3.2mW). However, the arithmetic hiding implementation is still satisfied when compared with conventional S-Box implementation, which

is 1.4× lower than conventional S-Box (5.3mW) as depicted in Fig. 5. The power overhead is mainly contributed from four multiplications operations in arithmetic hiding which run parallel with LUT based S-Box.

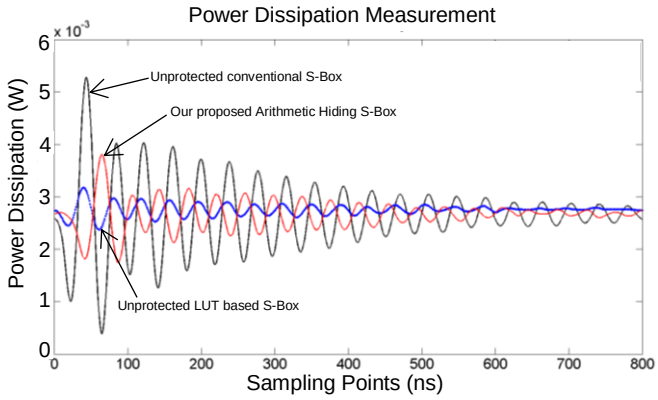
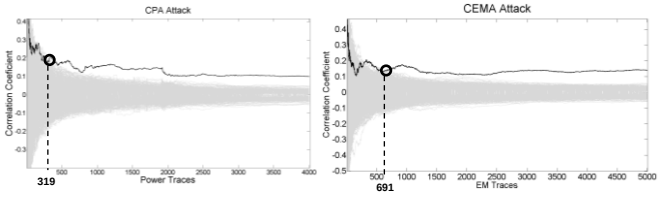


Fig. 5: Power dissipation measurement of AES-128 based on three different S-Box architectures

The evaluation of power dissipation is not directly imply the security features of the hiding technique. Particularly, the CPA and CEMA attacks, which require more number of measurement to reveal the secret key. In this experiment, the CPA and CEMA attacks are performed and compare the result against unprotected conventional S-Box and the proposed arithmetic hiding technique. Fig. 6 depicts the number of traces required to reveal the most difficult sub key of AES. It shows that the Fig. 6(a) requires 319 power traces to reveal the secrete key while CEMA attack requires 691 EM traces to reveal the same secrete key as depicted in Fig. 6(b). The low number of traces required due to the dependency between physical measurement and processed data is relatively high.



(a) (b)

Fig. 6: Evaluation of security features of conventional based S-Box (a) CPA (b) CEMA attacks

Fig. 7 depicts the CPA and CEMA attack based on the proposed arithmetic hiding. It shows that the 16-byte sub key has been successfully revealed at 38k and 44k of the power and EM traces respectively. In this context, the security features of the AES-128 has been increased against CPA and CEMA by 119× and 63× respectively when compared with unprotected conventional S-Box.

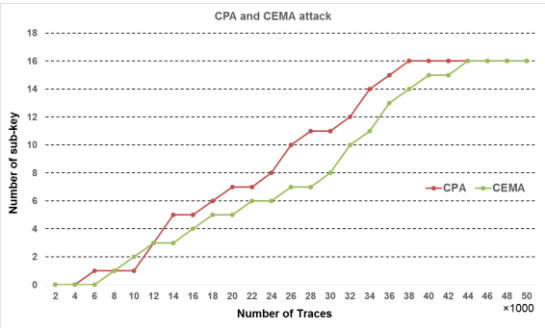


Fig. 7: CPA and CEMA attack of the proposed arithmetic hiding technique

V. Conclusions

We have proposed arithmetic hiding technique on the AES algorithm implementation to highly secure the algorithm against SCA. The arithmetic operations run parallel with the S-Box operation of the AES to hide the correlated leakage power dissipation with processed data. There are two key features in our proposed hiding technique. First, the function of the arithmetic hiding is independent with S-Box operation and its power dissipation is dominant over the S-Box. Therefore, the dependency of the total power dissipation with processed data in the AES algorithm is relatively low. Second, the security level of proposed technique against SCA based on CPA and CEMA attack are increased by 119× and 63× respectively, compared with unprotected S-Box. This is due to the leakage physical parameters which is generated by the arithmetic operation hides the leakage parameters of the S-Box operation. Based on the measurement results on Sakura-X FPGA board, which performs AES-128 algorithm, our proposed technique dissipates 3.8mW and features 1.18× higher power dissipation than the unprotected S-Box implementation. However, our proposed arithmetic hiding technique is highly secured, as the result of CPA and CEMA attack require 38,000 power traces and 44,000 EM traces respectively to reveal the secret key.

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] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks. US: Springer 2007.

[2] 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.

[3] Z. Martinasek, V. Clupek and K. Trasy, "Acoustic attack on keyboard using spectrogram and neural network," *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, Prague, 2015, pp. 637-641. (2015)

[4] B. Coppens, I. Verbauwhede, K. De Bosschere and B. De Sutter, "Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors," *Security and Privacy, 2009 30th IEEE Symposium on*, Berkeley, CA, 2009, pp. 45-60. (2009)

[5] 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.

[6] Kwen-Siong Chong *et al*., "Counteracting differential power analysis: Hiding encrypted data from circuit cells," *IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC) 2015*, Singapore, 2015, pp. 297-300.

[7] C. Tokunaga and D. Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," in *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23-31, Jan. 2010.

[8] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda and M. Nagata, "An intermittent-driven supply-current equalizer for 11x and 4x power-overhead savings in CPA-resistant 128bit AES cryptographic processor," *Solid-State Circuits Conference (A-SSCC), 2014 IEEE Asian*, KaoHsiung, 2014, pp. 225-228.

[9] S. Weiwei, F. Xingyuan, and X. Zhipeng, "A Secure Reconfigurable Crypto IC With Countermeasures Against SPA, DPA, and EMA," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, pp. 1201-1205, 2015.

[10] A. A. Pammu, K. S. Chong, K. Z. L. Ne and B. H. Gwee, "High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation," *2016 International Conference on Information Systems Engineering (ICISE)*, Los Angeles, CA, USA, 2016, pp. 3-7.