Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 3, 420-426 (2017)

www.astesj.com

Special issue on Recent Advances in Engineering Systems

ASTESJ

ISSN: 2415-6698

A Highly-Secured Arithmetic Hiding cum Look-Up Table (AHLUT) based S-Box for AES-128 Implementation

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

School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798

ARTICLE INFO

Article history:
Received: 22 March, 2017
Accepted: 12 May, 2017
Online: 24 May, 2017

Keywords:
Arithmetic Hiding
Side-Channel Attack
AES-128
Substitution-Box
CPA
CEMA

ABSTRACT

Side-Channel Attack (SCA) is an effective method in extracting the secret key of cryptographic algorithms by correlating the physical leakage information with the processed data. In this paper, we propose an arithmetic hiding cum Look-up Table (AHLUT) based Substitution-Box (S-Box) in AES-128 cryptographic algorithm implementation to countermeasure against SCA. There are three key features in our proposed AHLUT S-Box. First, the arithmetic hiding performs four types of arithmetic operations such that their total physical leakage information sufficiently overshadows the correlated physical leakage information of the S-Box operation. This is to reduce the correlation of the AES-128 physical leakage information with the processed data. Second, the AHLUT S-Box pre-stores all the 256 bytes of possible output values based on the conventional S-Box and selects a corresponding output value with respect to the input accordingly. In this context, it dissipates significantly lower power when compared to the conventional S-Box which performs multiplication inversion and affine transformation. Third, we propose a methodology to determine a minimum number of the arithmetic operations to sufficiently overshadow the physical leakage information of the S-Box operation. Based on the measurement results of performing AES-128 algorithm on Sakura-X FPGA encryption-board and in term of power dissipation, our proposed AHLUT S-Box dissipates 1.6mW and features 11.56× lower power dissipation than the conventional S-Box. In term of security which is based on Correlation Power Analysis attack, it requires 73× more power traces to reveal the secret key for our proposed AHLUT S-Box than the conventional S-Box. As for the non-invasive Correlation Electromagnetic Analysis attack, it requires 25× more electromagnetic traces for our proposed AHLUT S-Box than the conventional S-Box.

1. Introduction

Side-Channel Attack (SCA) is an effective method to extract the secret key of cryptographic algorithms, such as Advanced Encryption Standard-128 (AES-128) algorithm, by correlating physical leakage information, generated during the encryption process, with processed data. The physical leakage information such as power dissipation [1], Electromagnetic (EM) emanation [2], temperature [3] and timing [4] information, which are measured during the encryption process, are dependent on the processed data, determined based on plaintext/ciphertext. Due to the simplicity, in term of measurement, the power dissipation and EM emanation are the most preferred by adversary to be employed in the SCA compared with other physical leakage information [1].

Fig. 1 depicts the attacking scenario of the SCA, by intercepting wireless communication, transmitting the encrypted plaintext, ciphertext, to receiver and at the same time, measuring the physical leakage information. In this scenario, the correlation based SCA, such as Correlation Power Analysis (CPA), is employed to compute and analyze the correlation between the processed data and power dissipation measurements (power traces). To protect the secret key against SCA, countermeasure techniques are employed to reduce (break) the correlation between the physical leakage information with processed data.

*Corresponding Author: Ali Akbar Pammu, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 | Email: ali1@e.ntu.edu.sg

https://dx.doi.org/10.25046/aj020354

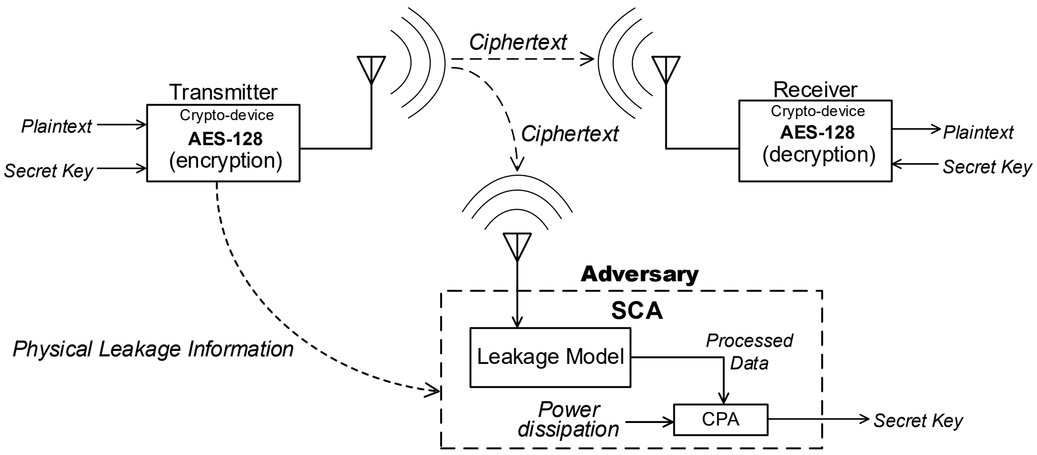


Fig. 1: Attacking scenario of SCA of wireless communication based on AES-128 implementation

The countermeasure technique is classified into two main classifications, hiding and masking, which are based on hardware and software approaches respectively [1]. The hiding technique breaks the correlation between power dissipation and processed data by balancing the power dissipation for different processed data whereas the masking technique employs masking variable (m) to mask the processed data against SCA. The main drawback of the masking technique is to mask and unmask of the m which can degrade the performance of the cryptographic algorithm implementations, such as low throughput, speed reduction and high power dissipation [2].

There are two main approaches of hiding technique, cell and block level approaches. In the cell level, several techniques have been reported such as Sense Amplifier Based Logic (SABL) [5], Wave Dynamic Differential Logic (WDDL) [6], Three-phase Dual-rail Pre-charge Logic (TDPL) [7] and Pre-Charge Static Logic (PCSL) [8]. The concept of SABL is to balance internal charges by fully charging and discharging all internal node for different processed data (i.e. bit-0 or bit-1). However, during the implementation in crypto-device, the internal charges is not fully discharged at high frequency (>100MHz) due to small variation on the internal parasitic capacitance [6]. The WDDL and PCSL implement Pre-charge and Evaluation cycle with differential logic to make a constant power dissipation for different logic transition. In the AES-128 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]. For the PCSL implementation, the power dissipations 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 speed compared with conventional CMOS implementation [1].

For the hiding approach at the block level, the power dissipation is balanced directly at the main power supply, V_{DD} point, of the crypto-device. The hiding techniques based on block level approach are a Switching Capacitor Current Equalizer (SCCE) [9], an intermittent Supply-Current Equalizer (iSCE) [10] and A Dynamic Voltage and Frequency Switching (DVFS) [11]. 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 iSCE 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 iSCE) are both vulnerable against EM based attack by measuring the EM emanation 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 by 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 secret key can be revealed with required low number of power traces.

In this paper, we propose an arithmetic hiding cum Look-up Table (AHLUT) based Substitution-Box (S-Box) in AES-128 cryptographic algorithm implementation to countermeasure against SCA. There are three key features in our proposed AHLUT S-Box. First, the arithmetic hiding performs four types of arithmetic operations such that their total physical leakage information sufficiently overshadows the correlated physical leakage information of the S-Box operation. This is to reduce the correlation of the AES-128 physical leakage information with the processed data. Second, the AHLUT S-Box pre-stores all the 256 bytes of possible output values based on the conventional S-Box and selects a corresponding output value with respect to the input accordingly. In this context, it dissipates significantly lower power when compared to the conventional S-Box which performs multiplication inversion and affine transformation. Third, we propose a methodology to determine a minimum number of the arithmetic operations to sufficiently overshadow the physical leakage information of the S-Box operation. Based on the measurement results of performing AES-128 algorithm on Sakura-X FPGA encryption-board and in term of power dissipation, our proposed AHLUT S-Box dissipates 1.6mW and features 11.56× lower power dissipation than the conventional S-Box. In term of security which is based on the CPA attack, it requires 73× more power traces to reveal the secret key for our proposed AHLUT S-Box than the conventional S-Box. As for the non-invasive Correlation Electromagnetic Analysis (CEMA) attack, it requires 25× more electromagnetic traces for our proposed AHLUT S-Box than the conventional S-Box.

This paper is organized as follows. Section II reviews the AES algorithm, various S-Box implementations, CPA and CEMA. Section III presents the proposed AHLUT S-Box. Section IV describes the measurement results on CPA and CEMA attack and finally, conclusions are drawn in Section V.

2. Advanced Encryption Standard, Substitution-Box operation, CPA and CEMA

In this section, an overview of the AES algorithm is briefly described followed by a description of the various topologies of the S-Box operation and the correlation based attack, the CPA and CEMA.

2.1. Advanced Encryption Standard

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 secret key for encryption and decryption respectively. The AES algorithm transforms a plaintext into a ciphertext using the secret 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 [1]. For the 128, 192 and 256 secret key length, there are 10, 12 and 14 round of iterations are required respectively.

Fig. 2 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 secret key. The decryption structure can be derived by inverting the encryption structure directly [12]. 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.

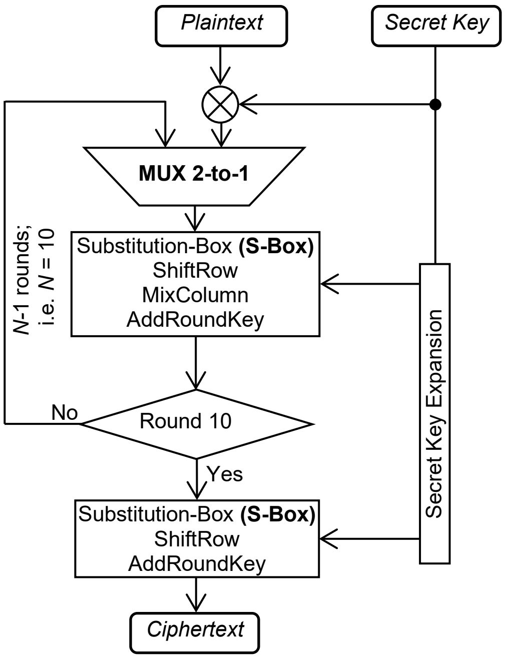
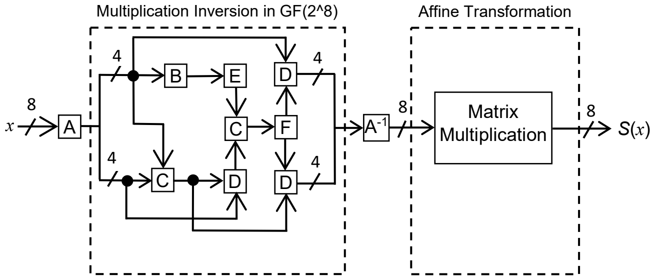


Fig. 2: Flow chart of the encryption process of the AES-128 algorithm with 10 round iterations

2.2. Substitution-Box

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 brute force attacks.



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. 3: The two sub-modules of a conventional S-Box of AES algorithm

The S-Box operation can be implemented in the form of the LUT, in which all the possible output (2^8 = 256) are pre-stored in the LUT memory, as depicted in Fig. 4. The analysis of the LUT S-Box [13] shows that the power dissipation is reduced significantly by 5.5× lower than conventional S-Box (reduces from 10.5mW to 1.9mW). However, the security features can only protect the key against CPA attack up to 13×10^3 power traces. This is due to the selection function (in the multiplexer) dissipates relatively small differences of the dynamic power for different input and output values of the S-Box.

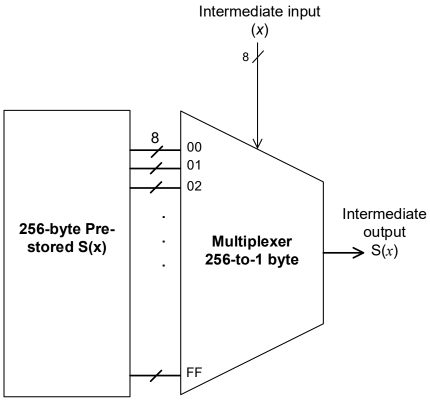


Fig. 4: LUT S-Box implementation

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 [13]. However, the low power dissipation at LUT architecture is possible to apply dummy operations, which hide the correlated power dissipation against CPA attack without sacrificing the power overhead.

2.3. CPA and CEMA

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 $i = 1, \ldots, 16$ sub-keys, $j = 1, \ldots, 256$ sub-key candidates, $t = 1, \ldots, N$ sampling points, as follows:

$$r_{i,j,t} = \frac{\sum_{m=1}^{n}\left(X_{i,j,m} - \overline{X}_{i,j}\right)\left(Y_{t,m} - \overline{Y}_{t}\right)}{\sqrt{\sum_{m=1}^{n}\left(X_{i,j,m} - \overline{X}_{i,j}\right)^{2}\left(Y_{t,m} - \overline{Y}_{t}\right)^{2}}} \tag{1}$$

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.

The CEMA attack applies the same procedure as the CPA attack. However, the process of acquiring the physical leakage information is less invasive compare with the CPA. The adversary can simply measure the EM emanation by placing the EM probe on the crypto-device and apply the Eq. (1) to reveal the secret key.

3. Proposed AHLUT S-Box

The power dissipation generated from the crypto-device is resulted from current (I_{DD}) and voltage (V_{DD}) consumed during the processing one plaintext (consists of 16 bytes). The collection of power dissipation ($P = I_{DD} \cdot V_{DD}$) measurements form power traces [1] and the power traces can be decomposed as the total sum of power dissipations of an operation, P_{OP}, processed data, P_{DATA}, noise, P_{NOISE} and constant power (static power dissipation), P_{CONST} as described in Equation (2).

$$P_{TRACES} = P_{OP} + P_{DATA} + P_{NOISE} + P_{CONST} \tag{2}$$

The P_{OP} and P_{DATA} are generated when performing the operations of the AES-128 algorithm with different value of input data, which are the main physical leakage information employed for the SCA. The P_{NOISE} can be generated from the crypto-device and measurement tools (i.e. oscilloscope) which exhibit different noise level for different application (i.e. ASIC or FPGA) and specification respectively. The P_{NOISE} can be filtered out by means of FIR filter with optimized parameters and hence increase the SNR value of the power traces. The P_{CONST} is relatively irrelevant to the SCA, since the value is generated constantly for different operation and processed data. In this context, the SCA only consider two power dissipation components, P_{OP} and P_{DATA}, to leak out the information of the secret key.

The proposed arithmetic hiding based LUT S-Box technique, in this paper, is focused on the P_{OP} and P_{DATA}, to decorrelate between the physical leakage information and the processed data, based on the CPA attack. The main idea is to generate dummy power dissipation by performing dummy operation (P_{D_OP}) with dummy input data (P_{D_DATA}). Therefore, the total power traces measurement is the sum of main power dissipation and dummy power dissipation as expressed in Equation (3).

$$TP_{TRACES} = P_{OP} + P_{D\_OP} + P_{DATA} + P_{D\_DATA} \tag{3}$$

To break the correlation between power dissipation measurement and processed data, based on the CPA attack, the dummy power dissipation must be able to dominate the total power traces. In other words, the dummy power dissipation is generated in such a way that overshadow the main power dissipation of the AES-128 algorithm, as expressed in Equation (4). In this context, the changes of P_{OP} and P_{DATA}, are negligible respect to the total power traces which are used in the CPA attack as expressed in Equation (5). Eventually, the broken correlation, between power dissipation and processed data, is achieved due to the total power traces measured during the encryption is always referring to dummy operation, which is performing irrelevant operation and data with the operations in the AES-128 algorithm.

$$TP_{TRACES} = P_{OP}\downarrow + P_{D\_OP}\uparrow + P_{DATA}\downarrow + P_{D\_DATA}\uparrow \tag{4}$$

When P_{OP} and P_{DATA} are negligible respect to P_{D_OP} and P_{D_DATA}, the Eq. (4) can be rewrite as follows.

$$TP_{TRACES} \simeq P_{D\_OP} + P_{D\_DATA} \tag{5}$$

The total power traces as expressed in the Eq. (5) can be realized by performing the arithmetic operations in parallel with the operation (i.e. S-Box) of the AES-128. The S-Box operation dissipates 80% of the total power dissipation [13] and leak more information about the secret key, whereas other three operations (AddRoundKey, ShifRow and MixColumn) insignificantly leak the information of the secret key [1] due to non-data dependent operations. To overcome the power overhead and yet secure S-Box, we adopt LUT S-Box which is performed in parallel with arithmetic operation to overshadow the P_{OP} and P_{DATA} of the S-Box. The LUT S-box is adopted due to the power dissipation is 5.5× lower than the conventional S-Box (1.9mW) [13]. Consequently, it is worthwhile to implement the arithmetic operation with sufficient power overhead to overshadow the power dissipation of the S-Box operation. Fig. 5 depicts our proposed AHLUT S-Box implementation, performed in parallel with LUT S-Box. Four types of arithmetic operations, implemented, Addition (ADD), Subtraction (SUB), Division (DIV) and Multiplication (MULT) are implemented which generate unused output, Dummy output, D(x).

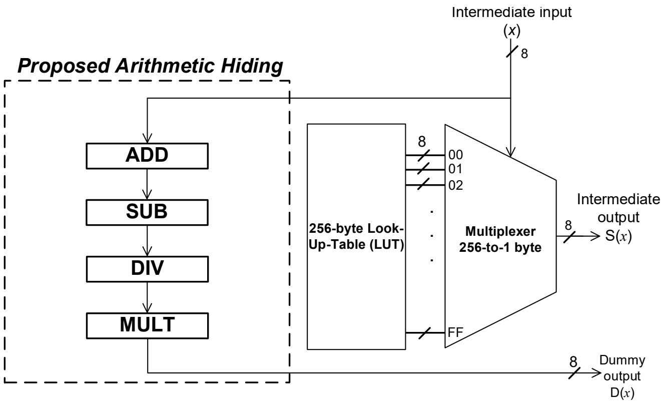


Fig. 5: Proposed arithmetic hiding is performed in parallel with LUT S-Box

In term of circuit implementation, each type of arithmetic operation requires different number of gates and dissipate different power. In addition to our proposed arithmetic hiding based LUT S-Box, we propose a methodology to select the number of arithmetic operations such that the power dissipation of these arithmetic operations sufficiently overshadows the S-Box power dissipation. Table I tabulates the number of gates and power dissipation for each arithmetic operation based on frequency of 16MHz.

TABLE. I. GATE COUNTS AND POWER DISSIPATION IN AHLUT S-BOX

Arithmetic Operations	Number of Gates			Power dissipation (mW*)
	XOR	AND	OR	
ADD	2	2	1	0.094
SUB	2	2	2	0.102
DIV	2	6	2	0.123
MULT	2	7	2	0.160

*dynamic power dissipation @16MHz

The methodology of selecting the number of arithmetic operations of our proposed AHLUT S-Box is explained as follow:

1. The power dissipation of the LUT S-Box is measured at the first stage to estimate the minimum power dissipation which will be generated by arithmetic hiding (overshadow power dissipation).
2. The power dissipation for each arithmetic operation is measured and sorted from lowest to highest, which are denoted as *a*, *b*, *c* and *d* in ascending order respectively.
3. The rule of thumb for estimating the overshadowed power dissipation is $P_{Arithmetic\_operations} > P_{LUT\_S\text{-}Box}$, in which $P_{Arithmetic\_operations} = a{\cdot}P_{ADD} + b{\cdot}P_{SUB} + c{\cdot}P_{DIV} + d{\cdot}P_{MULT}$; $a = b = c = d \geq 1$, as expressed in Equation (6).

$$a \cdot P_{ADD} + b \cdot P_{SUB} + c \cdot P_{DIV} + d \cdot P_{MULT} > P_{LUT\_S-Box} \qquad (6)$$

4. The number of arithmetic operations are increased starting from *d* and evaluating the power dissipation in the Eq. (6) every increment.
5. If power dissipation of arithmetic operation is overshoot as in Eq. (6), the selection is gradually descended from *c* to *a*.
6. The overshoot power dissipation is only allowed with incremental number of *a*, which is the lowest power dissipation in the arithmetic operation.
7. The selection process for the number of arithmetic operation is terminated when the $P_{Arithmetic\_operations}$ is slightly higher than $P_{LUT\_S\text{-}Box}$

The output of the arithmetic operation is unconnected to the AES-128 encryption process and therefore, the output ciphertext will not be affected. The flow chart of selecting the arithmetic operation is depicted in the Fig. 6.

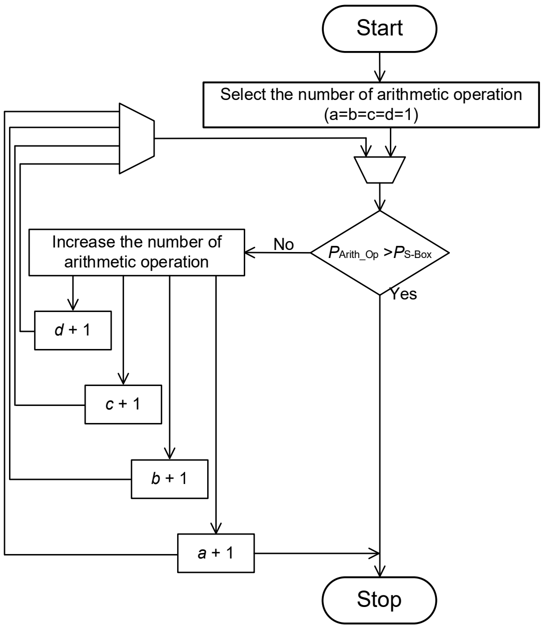

Start
Select the number of arithmetic operation (a=b=c=d=1)
Increase the number of arithmetic operation
No
$P_{Arith\_Op} > P_{S\text{-}Box}$
Yes
d + 1
c + 1
b + 1
a + 1
Stop

Fig. 6: Flow chart of selection the Arithmetic operations

4. Measurement Results

The experiment is performed based on Sakura-X, FPGA board [2], incorporating our proposed arithmetic hiding LUT S-Box in the AES-128 with operating frequency of 16MHz. The experimental setup comprises two parts, power dissipation and EM emanation measurements as depicted in Fig. 7. A 10-bit ADC 2.5Giga samples/second oscilloscope is used to record the power dissipation and EM emanation of the AES-128 implementation. We attack the last round of the AES-128 designs with the HD leakage model (power and EM model).

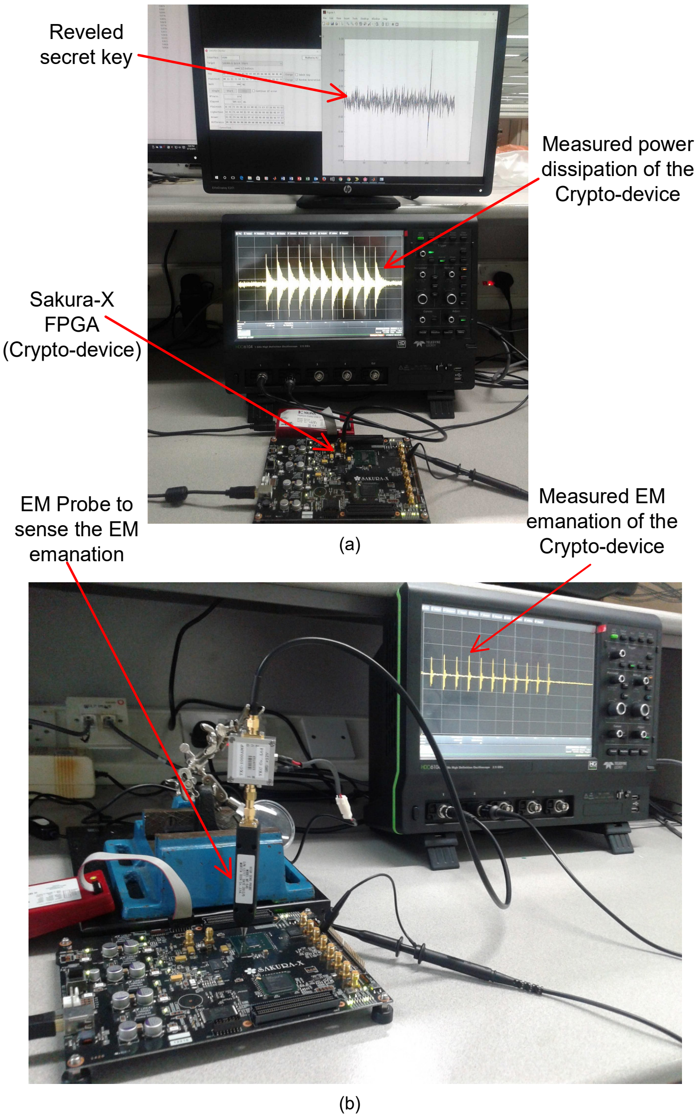

Reveled secret key
Measured power dissipation of the Crypto-device
Sakura-X FPGA (Crypto-device)
EM Probe to sense the EM emanation
Measured EM emanation of the Crypto-device
(a)
(b)

Fig. 7: The experimental setup (a) power dissipation measurement for CPA and (b) EM emanation measurement for CEMA attacks

Based on the power dissipation measurement of the AES-128 with LUT S-Box, we can estimate the number of the arithmetic operations can be employed to overshadow the power dissipation LUT S-Box as depicted in the Fig. 5. Table II tabulates the measurement result of LUT S-Box and the number of arithmetic operation required to overshadow the LUT S-Box.

TABLE. II. CIRCUIT MODULE IMPLEMENTATION OF AHLUT S-BOX

Circuit Module	Power dissipation (mW)
LUT S-Box	0.785
Arithmetic Operations*	0.813

*2 ADD; 1 DIV; 1 SUB; 4 MULT

The power dissipation of the arithmetic operation in the Table II is slightly higher than LUT S-Box with 0.028mW power overhead. The implementation of the arithmetic operation performed in parallel with LUT S-Box is depicted in Fig. 8. The AND logic gate is embedded to activate the arithmetic operations only when the LUT S-Box is performing the operation to prevent leakage current and dissipate additional power at the arithmetic operation (static power dissipation). The input data for arithmetic operation is 16-bit which comes from input LUT S-Box (*x*). The 8-bit input is inverted to make the input value opposite against the *x* such that uncorrelated with processed data.

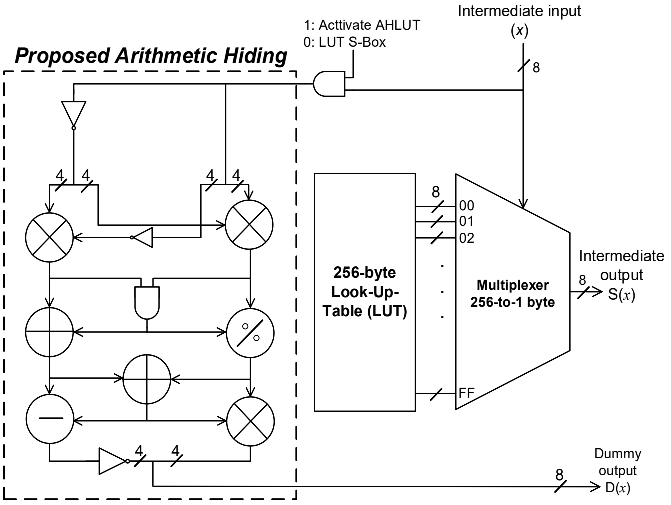


Fig. 8: Arithmetic operation is performed in parallel with LUT based S-Box

During the implementation in the circuit level, both modules (LUT S-Box and arithmetic operations) are performed at the same clock cycle, to hide the correlation with processed data, with the total power dissipation is 1.598mW. The power dissipation for AES-128 with LUT S-Box only and the AES-128 with arithmetic operation performed in parallel with LUT S-Box are depicted in Fig. 9. The grey color is indicated as arithmetic operations with LUT S-Box dissipates higher power as to overshadow the LUT S-Box as plotted in black color. As resulted from implementation of the controller, the static power dissipation is remined the same as in the LUT S-Box (~0.95mW) which implies the leakage current is negligible during the performance of arithmetic operations.

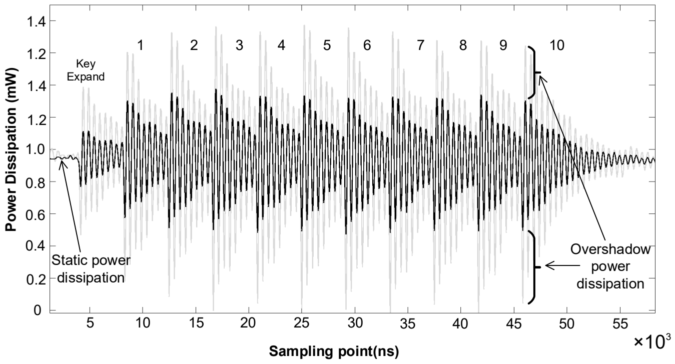


Fig. 9: Power dissipation measurement of 10 rounds iterations AES-128 with LUT S-Box and our proposed arithmetic hiding.

It is worthwhile to note that although in our proposed AHLUT S-Box, the power dissipation overhead is ~2× higher than LUT S-Box, but it is much lower than conventional S-Box implementation, which is 5.6× lower than conventional S-Box. Table III depicts the power dissipation of three S-Box implementations, LUT S-Box, proposed AHLUT S-Box and conventional S-Box.

TABLE. III. POWER DISSIPATION OF THREE DIFFERENT S-BOX TOPOLOGIES

S-Box Topology	Power dissipation (mW)	Normalized Power
LUT S-Box	0.785	0.5×
Conventional S-Box	18.37	11.56×
Proposed AHLUT S-Box	1.589	1×

In this experiment, the CPA attack is performed based on the proposed AHLUT S-Box and compare the result against LUT S-Box. Fig. 8 depicts the number of traces required to reveal the most difficult sub key of AES-128. It shows that the Fig. 10(a) requires 516 power traces to reveal the secret key while with our proposed AHLUT S-Box requires 1,751 power traces to reveal the same secret key as depicted in Fig. 10(b). Based on the CPA attack on single byte secret key, our proposed arithmetic hiding features 3.4 × secured than LUT S-Box implementation with ~2× power dissipation overhead.

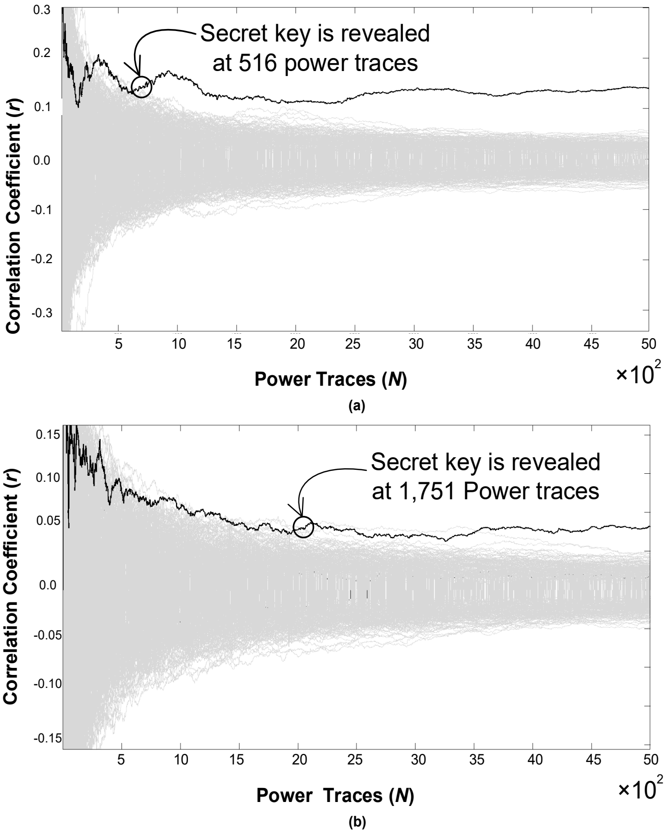


Fig. 10: Evaluation of the CPA as security features of (a) LUT S-Box and (b) our proposed AHLUT S-Box

Fig. 11 depicts the CPA and CEMA attack based on the proposed AHLUT S-Box. It shows that the 16-byte sub-secret key has been successfully revealed at 38×10^3 and 44×10^3 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 73× and 25× respectively when compared with conventional S-Box.

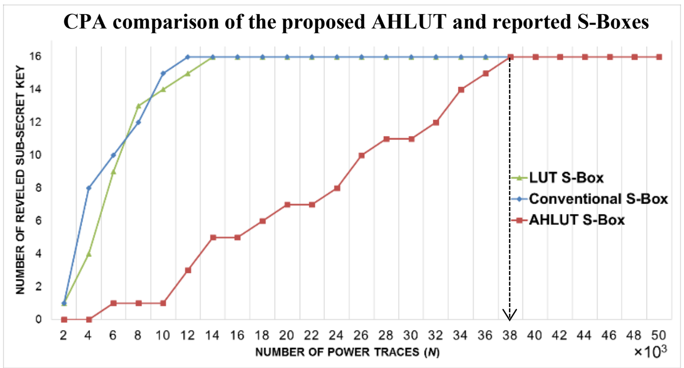


Fig. 11: Comparison of proposed AHLUT S-Box and reported hiding based on CPA attack

When comparing with reported hiding counterparts, SCCE [9] and iSCE [10], which can only protect the AES-128 algorithm against CPA attack, our proposed AHLUT S-Box can protect the AES-128 algorithm against EM based attack (CEMA) as well as in the CPA. Fig. 10 depicts the performance result of the CEMA attack for various hiding techniques. As shown in the Fig. 12, our proposed AHLUT S-Box outperforms the reported hiding techniques, which is requires 44×10^3 EM traces to reveal all the 16-byte secret key. The result is 5.5×, 4.8× and 44× higher than SCCE, conventional S-Box, iSCE and LUT based S-Box respectively. This is due to the physical leakage information (EM emanation) is generated by arithmetic operation, can dominate the EM generated by LUT S-Box and reduce the correlation between the EM signal of the LUT S-Box and the processed data of the AES-128 algorithm.

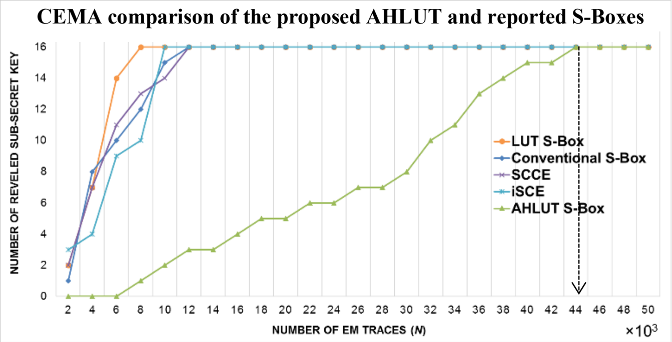


Fig. 12: Comparison of proposed AHLUT S-Box and reported hiding based on CEMA attack

5. Conclusions

We have proposed an AHLUT S-Box in the AES-128 cryptographic algorithm implementation to countermeasure against SCA. There are three key features in our proposed AHLUT S-Box. First, the arithmetic hiding performs four types of arithmetic operations such that their total physical leakage information sufficiently overshadows the correlated physical leakage information of the S-Box operation. Second, the AHLUT S-Box pre-stores all the 256 bytes of possible output values based on the conventional S-Box and selects a corresponding output value with respect to the input accordingly. Third, we propose a methodology to determine a minimum number of the arithmetic operations to sufficiently overshadow the physical leakage information of the S-Box operation. Based on the measurement results of performing AES-128 algorithm on Sakura-X FPGA encryption-board and in term of power dissipation, our proposed AHLUT S-Box dissipates 1.6mW and features 11.56× lower power dissipation than the conventional S-Box. In term of security of the CPA attack, it requires 73× more power traces to reveal the secret key for our proposed AHLUT S-Box than the conventional S-Box. As for the non-invasive CEMA attack, it requires 25× more EM traces for our proposed AHLUT S-Box.

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: Revealing the secrets of smart cards*. 2007.

[2] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, "SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA," in *1st IEEE Global Conference on Consumer Electronics 2012, GCCE 2012*, 2012, pp. 657–660.

[3] S. Ghosh and I. Verbauwhede, "BLAKE-512-based 128-bit CCA2 secure timing attack resistant McEliece cryptoprocessor," *IEEE Transactions on Computers*, vol. 63, no. 5, pp. 1124–1133, 2014.

[4] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in *Proceedings of the 12th ACM conference on Computer and communications security - CCS '05*, 2005, vol. V, no. November, p. 373.

[5] K. Tiril and I. Verbauwhede, "Charge Recycling Sense Amplifier Based Logic: Securing Low Power Security IC's against DPA," 2004, pp. 179–182.

[6] K. Tiri *et al.*, "AES-based cryptographic and biometric security coprocessor IC in 0.18-µ;m CMOS resistant to side-channel power analysis attacks," *IEEE Symposium on VLSI Circuits, Digest of Technical Papers*, vol. 2005, pp. 216–219, 2005.

[7] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 11, pp. 2128–2132, 2012.

[8] K.-S. Chong *et al.*, "Counteracting Differential Power Analysis: Hiding Encrypted Data from Circuit Cells," in *2015 IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC)*, 2015, pp. 297–300.

[9] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2010.

[10] 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," in *IEEE Asian Solid-State Circuits Conference*, 2014, pp. 9–12.

[11] T. Güneysu and H. Handschuh, "SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip," in *Cryptographic hardware and embedded systems – CHES 2015: 17th international workshop Saint-Malo, France, september 13–16, 2015 proceedings*, 2015, vol. 9293, pp. 620–640.

[12] A. A. Pammu, K.-S. Chong, and B.-H. Gwee, "Secured Low Power Overhead Compensator Look-Up-Table (LUT) Substitution Box (S-Box) Architecture," in *IEEE International Conference on Networking, Architecture and Storage (NAS), Aug. 2016*, 2016, pp. 1–7.

[13] 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," in *2016 International Conference on Information Systems Engineering (ICISE)*, 2016, pp. 3–7.