High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation

Ali Akbar*, Kwen-Siong Chong, Kyaw Zwa Lwin Ne 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 a Multiplexer Look-Up-Table (MLUT) based Substitution-Box (S-Box) implementation for the Advanced Encryption Standard (AES) algorithm. There are two key features in the proposed MLUT based S-Box. First, it is implemented based on 256-byte to 1-byte multiplexer with a 256-byte memory instead of the conventional implementation of employing multiplication inversion in GF(2^8) and affine transformation. Thus, our proposed S-Box is simpler in circuit implementation and lower in power dissipation. Second, our S-Box is 30× more secured against the Side Channel Attack (SCA) based on Correlation Power Analysis (CPA), as our proposed S-Box exhibits small variance in its power dissipation profile for different processed data. Based on the measurement results of AES-128 implemented on the Sakura-X FPGA board, our proposed S-Box dissipates only 1.9mW and features 5.5× lower power than the conventional S-Box implementation. Our proposed MLUT S-Box design is also highly secured as the CPA attack on the AES with our proposed S-Box implementation requires 13540 power traces which is significantly higher than conventional S-Box, requires only 445 power traces to uncover the same secrete key.**

***Keywords* — Multiplexer, Look-Up Table (LUT), Substitution Box (S-Box), Side Channel Attack (SCA), Correlation Power Analysis (CPA)**

I. INTRODUCTION

Advanced Encryption Standard (AES) algorithms have been employed in a variety of security systems including the defense and banking applications since 2001. It has been proven to be more effective to protect the secret information when compared to other reported encryption algorithms including the Data Encryption Standard (DES), Triple-DES (3DES) and Elliptic Curve Cryptography (ECC) [1]. The AES encryption process as depicted in Fig. 1 requires multiple rounds of iterations, each round consists of 4 arithmetic and logical operations namely SubstitutionByte, ShiftRow, MixColumn and AddRoundKey except for the last round which does not have MixColumn operation. Despite its highly secured features, AES is vulnerable against Side Channel Attack (SCA) which can reveal the secret information (secret key and plaintext) by correlating its intermediate data with the leakage physical parameters. The leakage physical parameters can be the power dissipation, electromagnetic radiation and timing information generated during the encryption process. There are three types of power analysis based SCAs, namely Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). Among these 3 types of attacks, the CPA is the most effective attack [1].

The CPA attack is the byte-based attack employing the statistical properties of power traces and the intermediate data to reveal the secrete key. Many techniques have been reported to enhance the AES encryption systems as to countermeasure against the power analysis based SCAs [1], [2]. There are two main types of countermeasures against CPA attack, i.e. Hiding and Masking [1]. The hiding technique is hardware-based approach which aims to break the dependency between the processed intermediate data and the leakage parameter which eventually reduces their correlation. In masking technique, the intermediate data is randomized to mask the data against correlated leakage parameter. The masking technique can be categorized as the software-based approach.

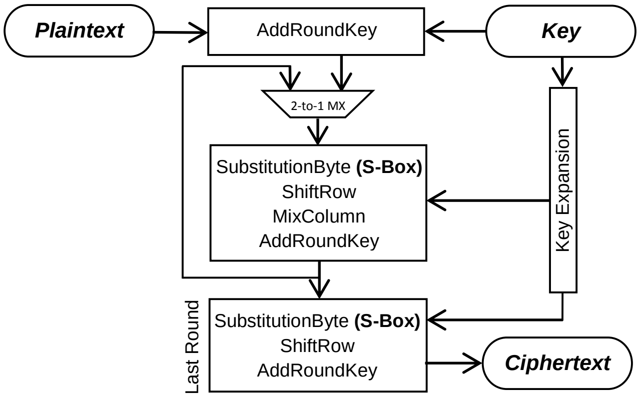


Fig. 1: The encryption process of AES algorithm

S-Box is one of the main modules in the AES implementation. This module is a non-linear operation which makes AES highly secured in protecting the secret information. In another perspective, S-Box dissipates the most power [5] and easily leak out the information of the processed intermediate data through CPA attack. Numerous literatures have reported to protect S-Box against CPA attack [2]-[4] and [9]. A Random of Dynamic Voltage Scaling (RDVS) design was reported in [4]. In this design, the supply voltage is randomly changed to countermeasure against the CPA attack. However, the voltage can be easily corresponded to its intermediate data through its synchronous clock signal. Hence, the resistance against SCA is rather low. The reconfigurable IC is implemented [6] to countermeasure against the CPA attack. The countermeasure technique utilized idle reconfigurable processing elements to generate dummy operations as to reduce the correlation. Although the resistance against CPA is relatively high, it has high area overhead. In another study, the Pre-Charge Static Logic (PCSL) [9] has been proposed to balance the internal charge of the circuits for different input data. However, in practical applications, the charge may not be perfectly balanced, hence the power dissipation profile correlates to the charging and discharging of the circuit activities can easily leak information.

In this paper, we propose a Multiplexer Look-Up-Table (MLUT) based S-Box implementation for the AES algorithm. The AES implementation embodying our proposed MLUT S-Box requires only one 256-byte-to-1-byte multiplexer and one 256-bytes look-up-table. Our proposed S-Box features small variance of power dissipation measurement for different input data and is 30× more secured than the conventional S-Box against the CPA attack. Our proposed S-Box dissipates only 1.9mW and features 5.5× lower power than the conventional S-Box implementation and also features highly resistance against the CPA attack. To uncover the same secrete key, MLUT S-Box requires 13540 power traces which is significantly higher than the conventional S-Box, requires only 445 power traces.

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

II. S-Box of the AES Algorithm

The S-Box consists of two sub-modules [5], namely the multiplicative inversion sub-module in GF(2^8) and the Affine transformation (operates in matrix multiplication) 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 [2]. Based on these two sub-modules, the S-Box features a non-self-inverse function [7] which effectively protects the data against the CPA attack.

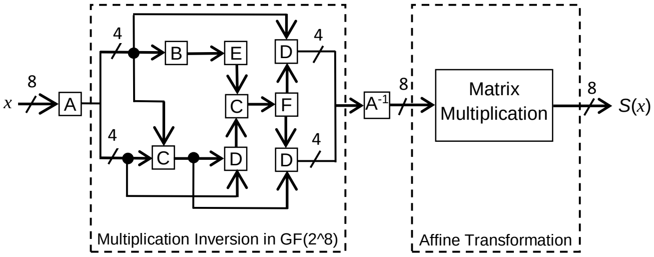


Fig. 2: The two sub-modules of a conventional S-Box

In Fig. 2, isomorphic and inverse isomorphic mappings are denoted as A and A^{-1} respectively [1]. The mapping A aims to decompose complex GF(2^8) to lower order GF(2), GF(2^2) and GF($(2^2)2^2$). In circuit implementation, A and A^{-1} require 24 and 23 XOR gates respectively. The square operation in GF(2^4) is denoted as B which requires 4 XOR gates. The sum operation in GF(2^4) is denoted as C requires 4 XOR gates. The multiplication in GF(2^4) is denoted as D, requires 21 XOR and 9 AND gates. The multiplication with constant operation is denoted as E, requires 3 XOR gates. The inverse operation in GF(2^4) is denoted as F, requires 22 XOR and 12 AND gates. The Affine transformation is performed based on matrix multiplication which requires 23 XOR gates. The total number of gates required in S-Box operation are 120 XOR and 21 AND gates as tabulated in Table I.

Table I. Number of logic gates required in conventional S-Box

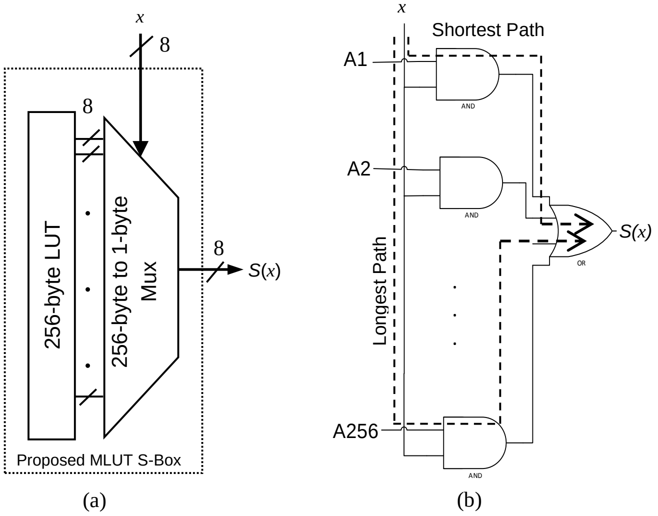
Logic Gate	Multiplication inversion in GF(2^8)	Affine transformation	Total
XOR	97	23	120
AND	21	0	21

As the 8-bit x, processed through all these operations to generate $S(x)$, it dissipates different power for different x. Thus, the power dissipation could be corresponded with the value of the processed data in the S-Box.

III. Proposed MLUT Based S-Box

The input to the S-Box is an 8-bit data, x, which has 256 combinations of input values (2^8 =256). The output from the S-Box, $S(x)$, for each possible input, x, can be pre-computed and stored in a Look-Up-Table (LUT). The corresponding output can then be retrieved directly from the LUT when a particular input arrives. In this context, a multiplexer can be used to select a corresponding output data from the LUT as depicted in Fig. 3(a). Hence, the $S(x)$ can be generated faster (with only one multiplexer operation) and this operation dissipates lower power when compared to the conventional S-Box operations.

As depicted in Fig. 3(a), the proposed MLUT S-Box which consists of a 256-byte-to-1-byte multiplexer and a 256-byte LUT. The 256 stored values, $S(x)$, in the LUT are based on the pre-computed values of S-Box operations for all possible 256 bytes of x. The longest and shortest path of the data of MLUT S-Box is depicted in Fig. 3(b). Although there is an interconnection delay difference in these paths, their power dissipation difference is small. We will show their power dissipation measurement results in Section V.



(a) (b)

Fig. 3: Multiplexer based S-Box (a) Proposed MLUT S-Box (b) Longest and Shortest Path delay

The dissipated power in MLUT S-Box is relatively low (when compared to the conventional S-Box) and highly uniform for different x, since only the selection of the corresponding $S(x)$, from the LUT is performed. As depicted in Fig. 3(b), the data, $S(x)$, selected from LUT passes through the AND gate and OR gate to the output, thus the power dissipation is low. However, the small differences of delay resulted from different paths of the data in multiplexer operation generates a small power dissipation variation for different x. Hence, the power dissipation of our proposed MLUT S-Box has a smaller correlation with the processed data when compared to the conventional S-Box and thus it is highly secured against SCA.

IV. Measurement Results on AES implementations

The CPA experiment on AES-128 implementation is conducted based on the Sakura-X FPGA board [8]. The 16-byte plaintext is randomly generated from the Sakura checker. The power dissipation is measured in oscilloscope with sampling rate of 2.5Giga samples/second. The focus of the CPA attack is at the last round of AES-128 which processes 128-bit size (16-byte) of input. Hamming Distance (HD) power model is employed in this experiment, measuring the changes of input and output of the last round of the AES-128 implementation. The power dissipation of MLUT S-Box is only 1.9mW as shown in Fig. 4. This low 1.9mW power dissipation is due to 2 logic gate (AND and OR) operations, and a very small power dissipation due to the interconnection. This is 5.5× lower power dissipation than the conventional S-Box implementation which dissipates 10.5mW.

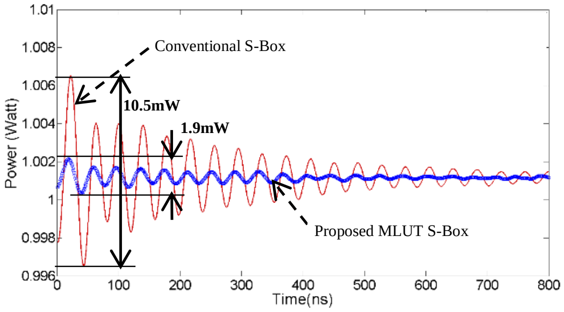


Fig. 4: Power dissipations of conventional S-Box and MLUT S-Box

The low power implementation on encrypted device does not imply highly secured against SCA. The security of the device against SCA is measured based on its power variance for different processed data. The lower value of variance the higher secured against SCA. In order to verify the dependency between power dissipation and the processed data, variance of 10000 power dissipation of the conventional and the proposed MLUT S-Box operations are computed and depicted in Fig. 5. The highest power dissipation variance can be observed in the conventional S-Box implementation. This is due to the 8-bit input data, x, is processed via 120 XOR gates and 21 AND gates to generated the $S(x)$, hence different values of processed data will generate different level of power dissipations. However, for our proposed MLUT S-Box, the variance of the power dissipations is mainly due to the different $S(x)$ undergo the AND and OR operations. It is also worthwhile to note that the difference in the interconnection delays contributes only a small variance in the power dissipation.

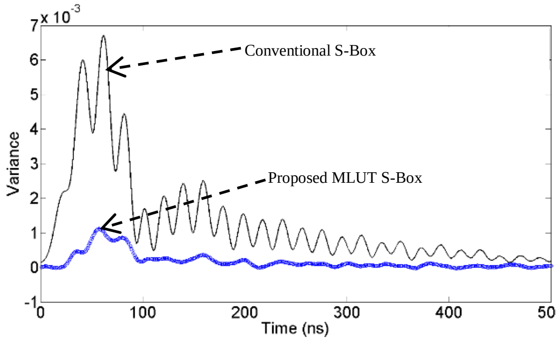


Fig.5: Variance of 10000 power dissipation of conventional S-Box and the proposed MLUT S-Box

V. Measurement Results on CPA Attack

The proposed MLUT S-Box is compared with the conventional S-Box based on their resistance against the CPA attacks. In this experiment, 1-byte key of the 16-byte keys was used to evaluate their levels of security. In the byte-based CPA attack, there are 256 possible values (1 byte = 8 bits and possibility is 2^8 = 256) and the correct key is one of the 256 key candidates. The CPA is performed at the last round of the AES-128 implementation. In this case, HD of the ciphertext is the intrinsic input for the CPA attack, see Fig. 1.

On the basis of the CPA attacks on the AES-128 implementations, 15000 power traces are measured to evaluate the level of security of the conventional S-Box and the proposed MLUT S-Box implementations. As depicted in Fig. 6, the conventional S-Box requires only 5000 power traces (shown in Fig. 7) to distinguish between the correct key of 240 with the absolute correlation coefficient of 0.13 and the incorrect key of average absolute correlation coefficient of 0.032.

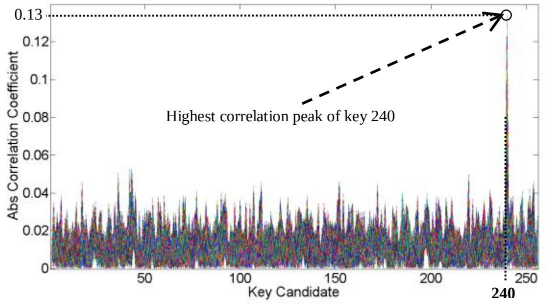


Fig. 6: Highest correlation peak of 0.13 shows at key 240 for the correct secrete key based on the conventional S-Box implementation

The low number of power traces required to reveal the secrete key of the conventional S-Box is clearly due to the variance of the power dissipation of the conventional S-Box is much higher than the variance of the power dissipation of the proposed MLUT S-Box which can be observed in Fig. 5. This also shows that the variance of power dissipation is linked to the power-data correlation and thus the resistance to the CPA attack. In order to exactly identify the ‘minimum’ power traces required to reveal the correct key, the correlation versus power traces is plotted in Fig. 7. It is shown that the conventional S-Box requires only a minimum of 445 power traces to reveal the correct key which implies that it is highly vulnerable against CPA attack.

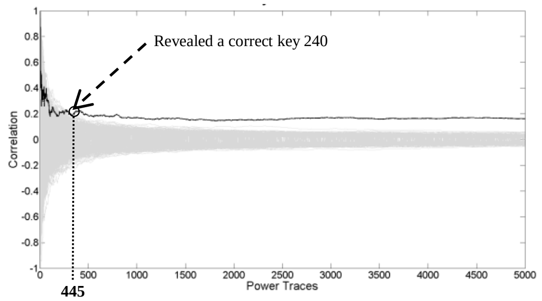


Fig.7: Correlation at different power traces for key 240 based on the conventional S-Box

Fig. 5 has shown that the MLUT S-Box has a smaller variance of power dissipations which implies that the data and the power dissipation is less correlated, hence it requires more number of power traces to reveal the correct key. The result of the CPA attack on MLUT S-Box with 15000 power traces is depicted in Fig. 8.

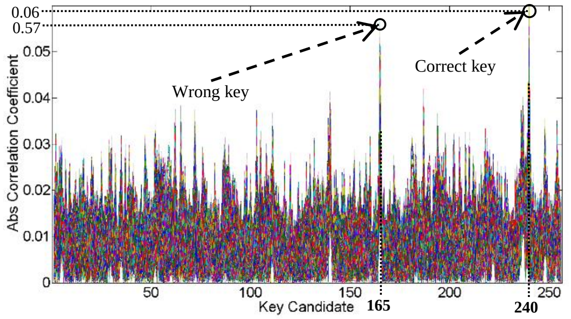


Fig. 8: Correlation peak for key 240 measured at 15000 power traces based on the proposed MLUT S-Box

In Fig. 8, it is shown that the highest correlation coefficient of the correct key of 240 is 0.06 whereas the second highest correlation coefficient of the wrong key of 165 is 0.57, which the difference is very marginal. The correct key correlation coefficient of 0.06 is also smaller than conventional counterpart of 0.13. In Fig. 8, the absolute correlation coefficients of the correct key and the average absolute correlation coefficients of the rest of the keys are 0.06 and 0.027 respectively. The small difference imply the difficulty of disclosing the correct key using MLUT S-Box when compared to the conventional S-Box. The minimum power traces required to reveal the correct key is plotted and depicted in Fig. 9.

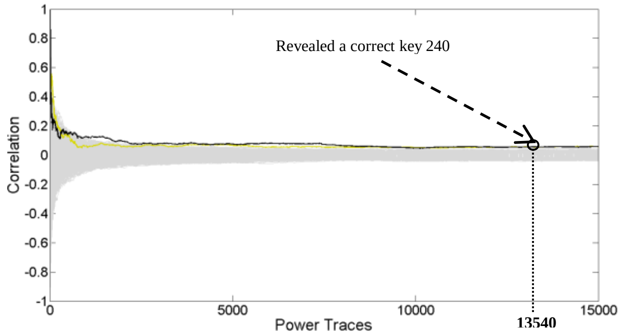


Fig.9: Correlation at different power traces for key 240 based on the proposed MLUT S-Box

The comparison of the conventional S-Box and the proposed MLUT S-Box is tabulated in TABLE II. It is clearly shown that the MLUT S-Box increased the minimum number of power traces from 445 to 13540 traces. This is approximately 30× more secured than conventional S-Box. In addition, the power dissipation for the conventional S-Box is 10.5mW whereas our proposed MLUT S-Box dissipates only 1.9mW. In summary, our proposed MLUT S-Box features higher security and lower power dissipation against the conventional counterpart.

TABLE II. COMPARISON OF THE CONVENTIONAL S-BOX AND THE PROPOSED MLUT S-BOX

S-Box Topology	Number Of Gates			Delay (ns)	Power Dissipation (mW)	Number of Power Traces
	XOR	AND	OR			
Conventional S-Box	120	21	-	164# 82*	10.5	445
MLUT S-Box	-	256	1	21# 17*	1.9	13540

#longest path delay
*Shortest path delay

VI. CONCLUSIONS

We have proposed a MLUT S-Box for AES-128 implementation to reduce the power dissipation and to increase the resistance against SCA, in particular the CPA attack. Our proposed MLUT S-Box design requires only one 256-byte-to-1-byte multiplexer and one 256-byte of LUT memory based on AES-128 implementation. The power dissipation of the AES-128 based on our proposed MLUT S-Box has significantly reduced from 10.5mW to 1.9mW. In addition, the power dissipation for different processed data is highly uniform resulted in lower variance. The measurement results obtained from the experiment has shown that the proposed MLUT S-Box is 30× more secured than the conventional S-Box based on the CPA attack. The secret key can only be revealed after measuring a significant 13540 of power traces.

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] 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.

[3] F. Gurkaynak, S. Oetiker, H. Kaeslin, N. Felber, and W. Fichtner, "Improving DPA security by using globally-asynchronous locally-synchronous systems," in *Solid-State Circuits Conference, ESSCIRC 2005. Proceedings of the 31st European*, pp. 407-410, 2005.

[4] S. Chunchun, 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.

[5] D. Canright, "A Very Compact S-Box for AES," in *Cryptographic Hardware and Embedded Systems – CHES 2005*. vol. 3659, J. Rao and B. Sunar, Eds., ed: Springer Berlin Heidelberg, pp. 441-455, 2005.

[6] 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.

[7] W. Stallings, *Cryptography and Network Security: Principles and Practice*: Pearson Education, 2002.

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

[9] 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*, pp. 297-300, 2015.