Mitigating the Side Channel Power Analysis Attacks using New Variable Mapping Substitution Technique

Hytham M. Hussein, Abd Elhamed Gaafer, Ahmed A. Abdel-Hafez, Eman H. Beshr

Abstract*—Side-channel attack has been a real threat against many cryptographic embedded systems. In this attack, the internal data is retrieved directly by analyzing the power magnitude according to the fact that there is a considerable difference in power when manipulating 0's and 1's. A commonly used algorithmic countermeasures incur large execution delay and resources overheads. In this paper, a novel technique using Variable Mapping Substitution (VMS) is proposed for mitigating side channel power analysis attack against Advanced Encryption Standard (AES). VMS-AES is a novel AES-like algorithm which uses Linear Feedback Shift Register (LFSR) to generate the required parameters used to remap the values of substitution box (S-box) randomly to another location depending on a secret key. This remapping also keeps the same good linear and differential properties of the AES S-box. VMS-AES algorithm can be easily deployed in most embedded applications because no architectural change is needed and only software modifications are performed. In our proposal, chipwisperer side channel attack analysis tool is used to verify the effectiveness of the proposed algorithm. Also VMS-AES with different number of rounds is evaluated using three methods: NIST statistical suite tests, correlation coefficient analysis, and cryptographic parameters evaluation to study the effects of this change upon the AES security

***Keywords*—Side-Channel Attack, S-box, Permutation, Variable Mapping Substitution.**

I. INTRODUCTION

Advanced Encryption Standard AES is a cryptographic algorithms used widely in embedded systems [1], and is deployed in many security devices such as security cards, cell phones and wireless applications. In 1996, Bruce Schneier summarizes the usefulness of randomly-generated S-boxes "Linear and deferential cryptanalysis work only if the analyst knows the composition of the S-boxes"[2]. One of the methods to overcome the drawbacks of the previous strategy is to generate strong algebraic s-boxes with good linear properties (nonlinearity, algebraic degree, immunity order, ..., etc.) and also differential properties (propagation criteria, maximum autocorrelation, ..., etc.)[3], then affine transformation is used to conceal the S-box content. [4]
Attackers have found many techniques to retrieve secret information using side channel information (time execution, difference in power consumption, electromagnetic radiated, sound, …etc.)[5]. Power Analysis Attacks (PAAs) are effective forms of the Side-Channel Attacks (SCAs) which are easy to be performed in practice at relatively low cost. The effectiveness of PAAs relies on the relation between the instantaneous current drawn from the power supply source to the Complementary Metal Oxide Semiconductor (CMOS) digital circuits and processed data. PAAs exploit this dependency to retrieve the secret data [5].

SCA can be further classified into Simple Power Analysis (SPA) and Differential Power Analysis (DPA). In SPA [5, 6], internal data is retrieved directly by analyzing the power magnitude, while in DPA, much advanced statistical analysis is performed to predict the secret information. DPA is more powerful and accurate than SPA and it exploits the fact that there is a observed difference in power when manipulating 0's and 1's [6].

Several solutions are proposed to countermeasure PAAs, such as: random masking, Quantitative Masking Strength [7], hardware balancing [8], Noise Injection [9], Equalization Power Designs in FPGA[10], and algorithmic balancing[11]. The Masking techniques can be attacked using advanced attacks as higher order DPA [12]. While the Hardware balancing techniques are known to be too cost in fields of size and consumption power.

In our proposal, a simple and effective technique "Variable Mapping Substitution (VMS)" is proposed to mitigate the effect of the side channel power against the AES encryption algorithm. In this technique, 128-bit Linear Feedback Shift Register (LFSR) [13] is used to generate the required parameters needed for remapping the substitution of AES S-box to another location randomly in each round execution to mitigate the side-channel leakage (correlated to an intermediate variable). The rest of the paper is organized as follow: section II introduces side channel attack (SCA) terminology, the related works are discussed in section III in section IV the proposed technique is introduced, section V shows the experimental evaluation results for the VMS-AES, and finally the paper is concluded in Section VI.

Manuscript published on November 30, 2019.
* Correspondence Author

Hytham M. Hussein*, Electrical and Control Eng. Dept. Arab Academy for Science & Technology, Cairo, Egypt. hythamahmed555@yahoo.com
Abd Elhamed Gaafer, Electronics and Communication Dept. Arab Academy for Science and Technology, Cairo, Egypt. abdelhamidgaafar@yahoo.com
Ahmed A. Abdel-Hafez, Communication Dept. Military Technical Collage
Cairo, Egypt. aabdelhafez@gmail.com
Eman H. Beshr, Electrical and Control Eng. Dept**.** Arab Academy for Science & Technology, Cairo, Egypt. eman.beshr@gmail.com

Retrieval Number: D4389118419/2019©BEIESP
DOI:10.35940/ijrte.D4389.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. SIDE-CHANNEL ATTACK TERMINOLOGY

Implementation of any cryptographic algorithm can be considered as processing of a sequence of intermediate variables.

Intermediate variable is critical if its distribution is a function of used data (for example, the plaintext) and the key, and is not constant with respect to the secret data.

Consequently, the statistical distribution of these variables relay on both the secret data and the distribution of the known data. If a sensitive intermediate variable appears in the execution of a cryptographic algorithm.

The AES implementation contains a first-order flaw. Information arising from a first-order flaw[14], that can be observed via a side-channel (such as timing information or power consumption), is termed first-order leakage. A first-order side-channel attack (SCA) against a hardware implementation is a SCA that exploits a first-order leakage to retrieve information about the secret data.

Similarly, an rth order SCA as Higher-Order SCA (HO-SCA) against a hardware implementation is a SCA that exploits leakages at *r* different times, which are respectively associated with *r* different intermediate variables. SCA are still a threat to the embedded system.

III. THE RELATED WORK

SCAs have been studied extensively by researchers and a number of countermeasures have been recently proposed countermeasures for PAAs. Authors in [15] introduced a masking technique that involve computation with random values to obfuscate the secret information from power profiles using arithmetic and Boolean masking. This masking was successful against SPA but the masked AES can be attacked using higher order DPA through joint probability distributions of power traces.

Sense Amplifier Based Logic (SABL) technique is introduced in [16] which utilizes Dynamic Differential Logic (DDL) circuits to maintain one switching event per cycle, which is independent of sequence and input. But SABL adds costs in design and development of standard cells and large clock. While the authors in [16] introduced a differential routing technique that occupy more routing resources and area.

Other hardware solutions based on Wave Dynamic Differential Logic (WDDL) are proposed in [17] and dual rail encoding protocol is proposed in [18]. A hardware current flattening architecture called PAAR is proposed in. [19] to internally flatten current at instruction level by using a feedback module and a pipeline current flattening module.

Also Secure Double Rate Registers (SDRR) as a register level countermeasure against power attacks analysis is introduced in[20], the hardware and power cost of these hardware balancing approaches are quite significant (mostly 2x and more).

Non-deterministic processors are proposed in[21] that schedule and execute instructions out-of-order, hence eliminating the correlation of the original program with the actual execution. The instruction level parallelism is limited to particular applications, restricting the level of security in non-deterministic executions.

Ambrose et al.[22] offer a multi- processor balancing technique, where two complementary AES encryption algorithms are executed in parallel to balance the power variations due to signal transitions. The authors said that their technique is better in terms of performance overhead and security provided against PAAs.

In terms of algorithmic modifications, they altered the AES algorithm to introduce inversion in various steps. The idea of this technique is to run typical AES in one core and the one with inversion in the other, in instruction lock-step mode. Hence the execution of these two cores balance the effects of signal transitions. When one core incurs 0 to 1 transition, the other triggers 1 to 0 resulting in suppression of switching effects in the power profile.

Algorithmic balancing is easier to implement and provides similar security as the other approaches mentioned above. However, uses 2x hardware. Furthermore, the lock-step implementation is complicated.

IV. THE PROPOSED TECHNIQUE

Most ciphers implemented in embedded processors typically use lookup tables to implement their S-box or nonlinear constructs. Since the focus of most SCAs and particularly PAAs are on the S-Box, it is essential to provide countermeasures for embedded processors that can be easily and efficiently applied to SBox tables or lookups[23].

Masking of data involves exclusive-oring a mask, *n*, with the data in order to remove the relation between consumed power of the cryptographic device and intermediate values of the algorithm stated in (1) represents the S-box look up table, for 8-bit *p* plaintext, 8-bit subkey, *k*, and an output, *Y*, of 8-bits. Now if inputs data are masked with values n, respectively, as shown in (2), the data was permuted in the tables and stored at new addresses.

$$S(p \oplus k) = Y \quad (1)$$

$$S(p \oplus k \oplus n) = Y \oplus m \quad (2)$$

To mitigate the PAAs a Variable Mapping Substitution Technique (VMS) is proposed. In our technique, a 128-bit (16-byte) LFSR is added to the standard AES (VMS-AES) as shown in Fig.1.

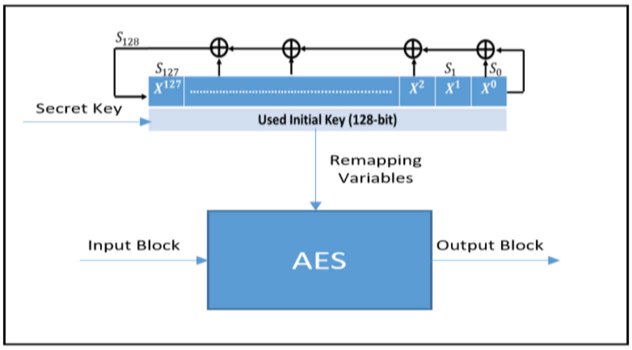

Fig. 1. VMS-AES Block Diagram

The LFSR contents are used to remap the contents of the AES S-boxes in all rounds so that the contents of the S-boxes will be different at each round. As a result, the attacker will not be able to trace the intermediate value to learn any information about the secrete key used.

In the proposed VMS-AES encryption algorithm, the secrete key is used as initial state of 128-bit LFSR. The contents of the LFSR is changed depending on primitive polynomial *f(x)* in (3) to ensure that the LFSR will achieve maximum length (2^{128} -1), the constrains of this polynomial are:

- Degree is 128.
- Not dense polynomial

$$f(x) = x^{128}+x^{95}+x^{57}+x^{45}+x^{48}+x^{36}+1 \qquad (3)$$

Fig. 2 shows the VMS-AES block diagram. Before the first round, we will run the LFSR for 128 times to be sure that all its states are updated. For each input block, LFSR will be run once to generate the remapping variables (16-byte). These bytes are used as a remapping layer to remap the contents of S-boxes in each rounds.

VMS-AES is the proposed block cipher algorithm which is a modified AES in which the block length, the key length and the round functions are specified according to AES specification. Fig.2(a) shows the VMS-AES encryption, while Fig.2(b) shows the VMS-AES decryption.

The function of remapping layer is used to remap the location of each byte in S-box to another location by XORing it with byte from updated state of LFSR. The index of the XORed byte in updated state of LFSR depending on the round number, the i^{th} byte in updated state of LFSR XORed with all the substituted bytes in i^{th} round number. In VMS-AES decryption, as shown in Fig.2(b), we obtain different values of the LFSR contents by (Call New Mapping) after (Inverse Shift Rows).

As a result, we will get a different Inverse Sub. bytes per each round of the block encryption. By using the proposed technique, the attacker which may try to follow the correlation at certain intermediate value by power trace will get different values each time because we use different S-box each round, as a results, it is so difficult to trace the intermediate value to learn the information

V. THE EXPERIMENTAL EVALUATION

A.Mitigating side channel evaluation

The first requirement in performing an analysis to power consumption attack is the ability of the attacker to success in acquiring power consumption traces from the target cryptographic device. The fundamental components that make up this setup include the target cryptographic device is chipwhisperer (CW1200 ChipWhisperer) An Open-Source Platform for Hardware Embedded Security Research. The chipwhisperer system in this work is modular design

architecture, and has more widely available code for the command computer control. Fig 3 shows the full setup using the chipwhisperer as capture platform and STM32F as a target board and lap top core i7 used to run the open source code chipwhisperer *ver*-5 to use the modules by python scripts to capture the power traces and make required analysis.

To investigate the efficiency of implementing a device using the new style, both unmasked AES and the new design were implemented on the target. In our experiments, the power consumption and of the entire AES processing sequence on the STM32F target were captured by using the modules in the capture platform that use the powerful well-known statistical tool, *Pearson's Correlation Coefficient* to estimate the relation between the key hypotheses and real measurements.

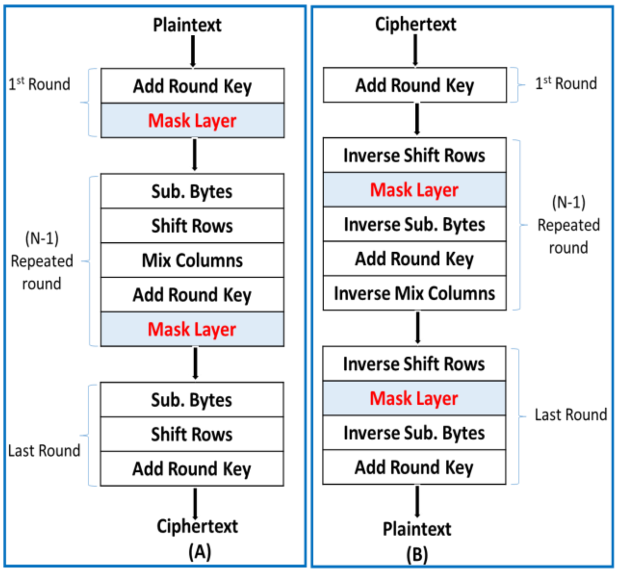

FIG. 2. VMS-AES ENCRYPTION /DECRYPTION

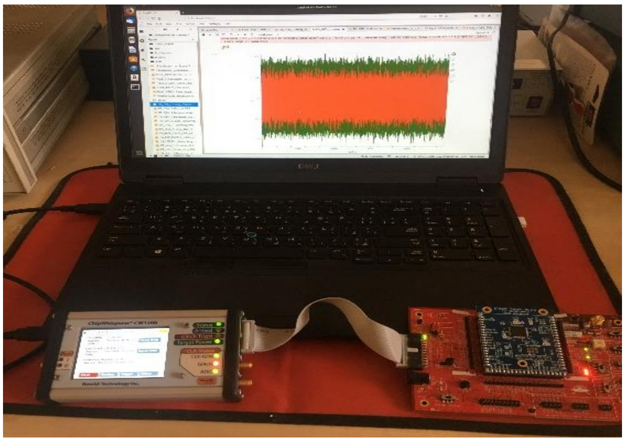

Fig. 3. Experimental setup for mounting PAAs

The variant of the DPA using the *Pearson's correlation* is called Correlation Power Analysis (CPA). Let t_i denote the i^{th} measurement data (i.e., the i^{th} trace) and *T* the traces set, and P_i is prediction for the i^{th} traces and P is the predictions set. Then we calculate:(4)

$$C(T,P) = \frac{E(T.P)-E(T)E(P)}{\sqrt{var(T)var(P)}} \qquad (4)$$

Here *E(T)* is the expectation average traces of the set of traces *T* also *Var (T)* is the variance of traces *T*. If this correlation is not low, so it assumed that the key hypothesis and prediction of the model, is correct[24, 25].In order to neglect the noise while capturing traces, all measurements were averaged over twenty times.

Fig. 4 shows the results of CPA against the unprotected AES implementation. As it is seen, the attack is successful and the correct subkey is recovered easily.

The plot confirms the assumption about the measurability of Hamming-Weights leakage. Fig. 5. Shows CPA result of the unmasked AES with 200 plaintexts. As it is seen the correct subkey hypothesis (Ox2B) is clearly distinguishable from false sub key hypotheses.

The attack was also successful in recovering all 16 subkeys as shown in

Fig. 6. The experiments were repeated for the proposed implementation. Fig. 7 shows the result of correlation analysis for the correct key guess in the new implementation. It is clear that the actual key can't be distinguished from the wrong keys. This experiment verifies the effectiveness of the proposed approach. As shown in Fig. 8, correct subkey is not distinguishable from the incorrect ones. The experiment was repeated again with 300 random plaintexts and the correct key was not recoverable.

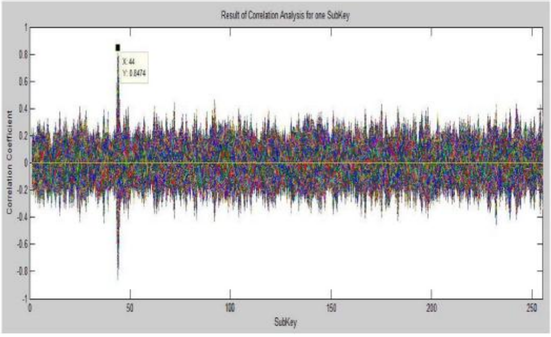

Fig. 4. correct subkey with real measurements in the unprotected implementation

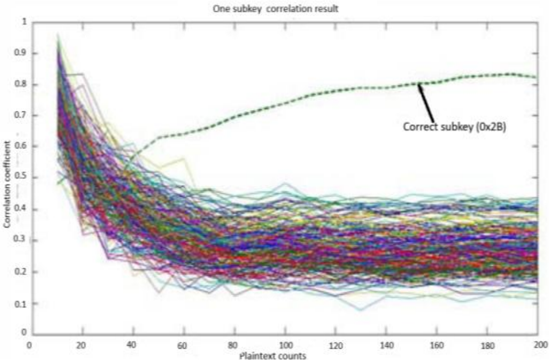

Fig. 5. CPA analysis of the unmasked AES with 300 plaintexts.

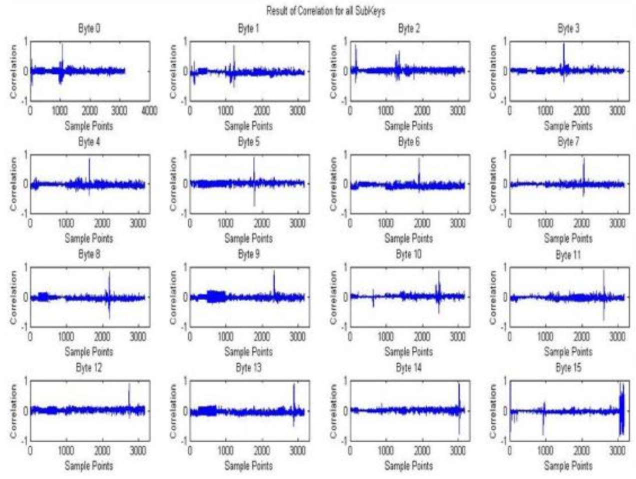

Fig. 6. Recovering all 16 subkeys using CPA with real measurements in the unprotected implementation.

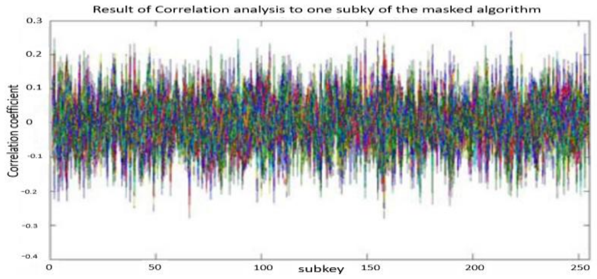

Fig. 7. Result of CPA for in the proposed implementation.

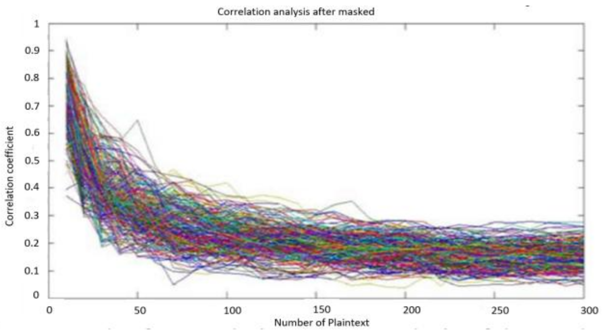

Fig. 8. Result of the masked AES with 300 plaintexts..

Table-I shows the comparison of the proposed masked implementations of AES in terms of memory size and number of cycles required with some other software implementation of the masked AES reported in the literature. As it is seen, the proposed technique slightly reduces speed and requires only 486 bytes more memory.

B. Proposed algorithm evaluation

In order to evaluate the security strength of the VMS-AES, three verification methods are used;

1) NIST STATISTICAL SUITE

The National Institute of Standards and Technology (NIST) develop a test Suite to evaluate AES algorithm is described in the NIST AES document[26] .as a statistical software package consisting of fixed number of tests that used to test arbitrarily long binary sequences randomness. These tests focus on an assortment of various types of non-randomness that could exist in a sequence. Some tests are decomposable into a deferent subtest.

A number of files (with different types) were encrypted using (VMS-AES, AES) algorithms. The encrypted files were entered as inputs parameters to the 15 tests of NIST statistical suite. The average values (p - values) of the statistical tests for both algorithms were given in TABLE-II the tests were applied to a different number of rounds for VMS-AES, and this feature clarifies the VMS-AES flexibility. Note that VMS-AES have passed all NIST Statistical tests.

2) Correlation Coefficient

Correlation coefficient is a number between -1 and 1 which measures the degree to which two variables are linearly related. The correlation is 1 in the case of an increasing linear relationship, −1 in the case of a decreasing linear relationship, and some value in between in rest cases, pointing the degree of dependence linearity between variables.

Retrieval Number: D4389118419/2019©BEIESP
DOI:10.35940/ijrte.D4389.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

If variables are independent, then the correlation is 0. Fig. 9 (a) and (b) show the correlation distribution of two horizontally adjacent codes in the plaintext/ciphertext for VMS-AES block cipher. The Correlation Coefficient in a numerical form is measured by Matlab package [27] and had a value of (-0.07491) which represent the departure of the plain/cipher text from independence.

Table - I: Comparison of some Implementations of Masked AES Resistant to PAA

Ref	platform	More memory	Cycles (Unprotected)	Cycles (protected)
[28]	AVR	1536	4626	13600
[29]	AVR	-	1190	4212
[30]	AVR	-	4427	8420
This work	STM32F	486	7443	8647

Table- II: VMS-AES vs. AES Statistical tests average p – values

NO	Test	Calculated Test Statistic		Threshold	Test Final Result
		AES	VMS-AES		
1	Frequency Test	0.0493	0.2647	6.5855	Passed
2	Runs Test	1.7562	0.6031	6.5855	Passed
3	Serial Test	1.8046	0.8658	9.2202	Passed
4	Cumulative Sums Test	1.3228	0.8439	6.5855	Passed
5	Autocorrelation Test	0.0489	0.0002	6.5855	Passed
6	Poker Test	101.57	123.781	166.998	Passed
7	Maurer's Test	0.1887	0.498	6.5855	Passed
8	Longest Run of 1's Test	0.7693	3.6382	16.8429	Passed
9	Binary Matrix Rank Test	0.7707	1.8379	9.2202	Passed
10	Lempel-Ziv Compression Test	0.197	0.631	6.5855	Passed
11	Approximate Entropy Test	12.863	10.3792	20.1209	Passed
12	Random Excursions Variant Test	0.7433	0.5852	6.5855	Passed
13	Non-Overlapping Template	8.9759	8.5912	20.1209	Passed
14	Overlapping Template Matchings	6.1028	3.5997	15.1168	Passed
15	Random Excursions Test	4.3402	4.6993	15.1168	Passed

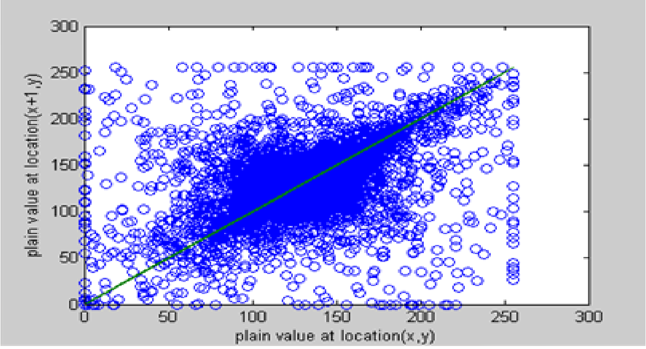

Fig. 9. (a) Correlation Coefficient for selected plain text

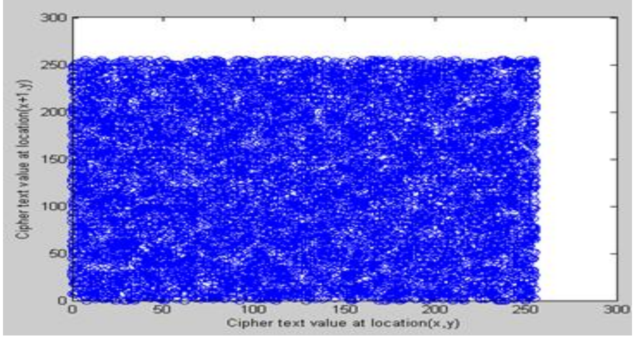

Fig. 9. (b) Correlation Coefficient for selected cipher text

Table- III: Test Results for 10 samples of new S-Boxes generated by VMS

No	Parameters Key Sequence	AD	NL	PC	CI	BL
1	0123456789AACDEF	6	112	0	0	1
2	C60D3A781BE2F495	7	112	0	0	1
3	D195AF73E028B46C	6	112	0	0	1
4	50D1C773EA29BF46	6	112	0	0	1
5	9FCD45EA172AC8FB	6	112	0	0	1
6	B5D1428AE73C69F0	6	112	0	0	1
7	AE73C69F0B5D1428	6	112	0	0	1
8	D391E61CA4257B8F	6	112	0	0	1
9	A4277B8FA391E60C	6	112	0	0	1
10	7FC02AA814B5D69E	7	112	0	0	1
11	**Standard AES**	**7**	**112**	**0**	**0**	**1**

3) Cryptographic Parameters Evaluation of new S-box

Testing S-box contents after masking layer is mainly used to insure that all required parameters of S-box are achieved by VMS-AES. Evaluation Software Package can be used for evaluating the S-box parameters [31]. Which measures the parameters of S-box such that: *algebraic degree* (AD), *non-linearity* (NL), *propagation criteria* (PC), *correlation immunity* (CI), and *balancedness* (BL). The output results of these tests on the generated masked S-boxes are illustrated in the TABLE-III.

VI. CONCLUDETION AND FUTURE WORK.

In this paper, a novel technique is proposed using the Variable Mapping Substitution (VMS) to mitigate to power consumption analysis of the SCA against AES encryption algorithm. Our experiments with the AES encryption algorithms demonstrate that the proposed solution is very effective in preventing information leakage due to power analysis. Moreover, it does not contradict the security, simplicity and easy software implementation of AES However, a lot of questions concerning the physical and hardware security of encryption algorithms remain open.

Protecting against sophisticated side-channel attacks exploiting the sensitive information, is still a challenge, costly and must be done with care.

REFERENCES

1. Daemen, J. and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. 2013: Springer Science & Business Media.
2. Schneier, B., Applied cryptography: protocols, algorithms, and source code in C. 2007: john wiley & sons.
3. Heys, H.M. and S.E. Tavares, Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of cryptology, 1996. **9**(1): p. 1-19.
4. Canteaut, A. and J. Roué. On the behaviors of affine equivalent sboxes regarding differential and linear attacks. in Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2015. Springer.
5. Kocher, P., J. Jaffe, and B. Jun. Differential power analysis. in Annual International Cryptology Conference. 1999. Springer.
6. Ostrowski, Ł., K. Marcinek, and W.A. Pleskacz. Implementation and Comparison of SPA and DPA Countermeasures for Elliptic Curve Point Multiplication. in 2019 MIXDES-26th International Conference" Mixed Design of Integrated Circuits and Systems". 2019. IEEE.
7. Gao, P., et al. Quantitative Verification of Masked Arithmetic Programs Against Side-Channel Attacks. in International Conference on Tools and Algorithms for the Construction and Analysis of Systems. 2019. Springer.
8. Lima, V.G., et al. Maximizing Side Channel Attack-Resistance and Energy-Efficiency of the STTL Combining Multi-V t Transistors with Current and Capacitance Balancing. in 2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019. IEEE.
9. Das, D., et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. in 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2017. IEEE.
10. Ender, M., A. Wild, and A. Moradi. SafeDRP: Yet another way toward power-equalized designs in FPGA. in International Workshop on Constructive Side-Channel Analysis and Secure Design. 2017. Springer.
11. Arora, A., et al. A double-width algorithmic balancing to prevent power analysis side channel attacks in aes. in 2013 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). 2013. IEEE.
12. Han, M., et al., Higher-Order Masking Scheme against DPA Attack in Practice: McEliece Cryptosystem Based on QD-MDPC Code. TIIS, 2019. **13**(2): p. 1100-1123.
13. Devika, K. and R. Bhakthavatchalu. Design of reconfigurable LFSR for VLSI IC testing in ASIC and FPGA. in 2017 International Conference on Communication and Signal Processing (ICCSP). 2017. IEEE.
14. Prouff, E. and R. McEvoy. First-order side-channel attacks on the permutation tables countermeasure. in International Workshop on Cryptographic Hardware and Embedded Systems. 2009. Springer.
15. Debraize, B., Countermeasure method against side channel analysis for cryptographic algorithms using boolean operations and arithmetic operations. 2015, Google Patents.
16. Manoj, P. and D.V. Ramana, Designing of DPA Resistant Circuit Using Secure Differential Logic Gates, in Computational Intelligence in Data Mining—Volume 1. 2016, Springer. p. 447-457.
17. Kim, H., et al. STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay. in 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). 2017. IEEE.
18. Bongiovanni, S., et al., Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks. Journal of Cryptographic Engineering, 2015. **5**(4): p. 269-288.
19. Muresan, R. and C. Gebotys. Current flattening in software and hardware for security applications. in Proceedings of the 2nd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis. 2004. ACM.
20. Bellizia, D., et al., Secure double rate registers as an RTL countermeasure against power analysis attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2018. **26**(7): p. 1368-1376.
21. Keramidas, G., et al., Non deterministic caches: A simple and effective defense against side channel attacks. Design Automation for Embedded Systems, 2008. **12**(3): p. 221-230.
22. Ambrose, J.A., et al., Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks. IET computers & digital techniques, 2011. **5**(1): p. 1-15.
23. Masoumi, M. and M.H. Rezayati, Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis. IEEE Transactions on Information Forensics and Security, 2014. **10**(2): p. 256-265.
24. Masoumi, M., Differential power analysis: a serious threat for FPGA security. International Journal of Internet Technology and Secured Transactions, 2012. **4**(1): p. 12-25.
25. Masoumi, M., P. Habibi, and M. Jadidi. Efficient implementation of masked AES on side-channel attack standard evaluation board. in 2015 International Conference on Information Society (i-Society). 2015. IEEE.
26. Heavner, T., et al., NIST-F1: recent improvements and accuracy evaluations. Metrologia, 2005. **42**(5): p. 411.
27. Gazzola, S., P.C. Hansen, and J.G. Nagy, IR Tools: a MATLAB package of iterative regularization methods and large-scale test problems. Numerical Algorithms, 2019. **81**(3): p. 773-811.
28. Schramm, K., Advanced Methods in Side Channel Cryptanalysis. 2006: Europäischer Univ.-Verlag.
29. Herbst, C., E. Oswald, and S. Mangard. An AES smart card implementation resistant to power analysis attacks. in International conference on applied cryptography and network security. 2006. Springer.
30. Bayrak, A.G., et al. A first step towards automatic application of power analysis countermeasures. in Proceedings of the 48th Design Automation Conference. 2011. ACM.
31. Picek, S., et al., Evolutionary algorithms for boolean functions in diverse domains of cryptography. Evolutionary computation, 2016. **24**(4): p. 667-694.

AUTHORS PROFILE

Hytham M. Hussein He received his B.Sc. from the Electrical Engineering Department, Faculty of electronic engineering, Menofia, Egypt in 2001 Electronics and Communication Department, Arab Academy for Science, Technology and Maritime Transport.

Abdelhamid A. Gaafar He received his B.Sc. from the Electrical Engineering Department, Military Technical College, Cairo, Egypt in 1977. M.Sc. from Al-Azhar University in 1983. Ph.D. from George Washington University in 1989. Currently Professor in Electronics and Communication Department, Arab Academy for Science, Technology and Maritime Transport.

Ahmed A. Abdel-Hafez He received his B.Sc. and M.Sc. from the Communication Engineering Department, Military Technical College, Cairo, Egypt in 1990., 1997 respectively. Ph.D. from Ottawa University in 2003. Currently Head of cryptography research center since 2012, Egyptian Armed Forces. His research interests including Applied cryptograph, and Information Security

.

Eman H. Beshr She received the B.Sc. And M.Sc. degrees from Arab academy for science and technology, Alexandria, Egypt, in 2000 and2003, respectively, and the Ph.D. Degree from Ain shams university Cairo, Egypt. Currently, she is assistant professor at the electrical and control engineering department, Arab academy for science and technology, Cairo, Egypt. She served as the head of the student advising and practical training in the department. Her research intersects including power system analysis, micro grids, renewable energy, demand response, and sustainably of power system