Strengthened of AES Encryption Algorithms within New Logic Topology

Vahid Rashtchi[1*], Seyyed Hamidreza Mosavi[2]
1- Department of Electrical and Computer Engineering, Zanjan University, Zanjan, Iran.
Email: rashtchi@znu.ac.ir (Corresponding Author)
2- Department of Electrical and Computer Engineering, Zanjan University, Zanjan, Iran.
Email: hamidreza@znu.ac.ir

Received: September 2017 Revised: November 2017 Accepted: December 2017

ABSTRACT:
Side-channel attacks are considered to be the most important problems of modern digital security systems. Today, Differential Power Attack (DPA) is one of the most powerful tools for attacking hardware encryption algorithms in order to discover the correct key of the system. In this work, a new scheme based on randomizing power consumption of a fixed-operation logic gate is proposed. The goal of this method is enhancing the immunity of AES algorithm against DPA. Having a novel topology to randomize the power consumption of each Exclusive-NOR gate, the proposed circuit causes random changes in the overall power consumption of the steps of the algorithm; thus, the correlation between the instantaneous power consumption and the correct key is decreased and the immunity of the AES implementations which the key is injected into their process through Exclusive-NOR gates is extremely increased. The proposed method can be used as a general hardening method in the majority of cryptographic algorithms. The results of theoretical analysis and simulations in 90-nm technology demonstrate the capability of the proposed circuits to strengthen AES against DPA. The CMOS area and power consumption overhead is less than 1%.

KEYWORDS: Advanced Encryption Standard (AES), Differential Power Analysis (DPA), Power Analysis (PA), Power Measurement, AND OR Invert (AOI), OR AND Invert (OAI).

1. INTRODUCTION

Today, the importance of information is absolutely higher than the past and security systems are becoming vital and ubiquitous [1]. Since the introduction of side-channel attacks which they extract the correct key of the algorithm using power consumption, run time, and electromagnetic radiation without destroying the device at the execution time of the algorithm [2], the demand for increasing the security of algorithms has been widely increased [3]. Digital devices such as smart cards, cell-phones, and RFID sets are vulnerable to side-channel attacks [4-6]; to reduce the vulnerability of these devices against threats, many methods have been proposed.

Power attack is a kind of side-channel attack which is based on power consumption of the chip at the execution time of the process; it was proposed by Paul-Kocher in 1999[7]. In Power analysis, there are two main study approaches: Simple Power Analysis (SPA) [7] and Differential Power Analysis (DPA) [7]. To find the key using SPA, the attacker must have knowledge about the implementation of the algorithm inside the chip. In contrast, in DPA, it is not necessary to have any details of the implementation. To countermeasure algorithms against DPA, researchers have proposed many methods [8-20]. The core activity of majority of the methods is to reduce the correlation between the power consumption and intermediate processed data. The methods could be categorized according to the fact whether they are implemented via software or hardware [21]. Software methods are mostly implemented within the code executed on the processors. Adding dummy power consumption [13], randomized jumping [9], arbitrary clocks and Random Delay Insertion (RDI) [22], exchanging combinational function [23], and adding random functions [7] could be examples of software-based methods. Most of the software methods are vulnerable against DPA; because the averaging function eliminates the added noise or disturbance to the power consumption trace [24].

On the other hand, in hardware-based methods, the designer of the circuits has more freedom and options to increase the immunity of algorithms [25]. The main goal of hardware strengthening methods is to disturb or flatten power consumption trace [25]. This work could be done by adding complementary blocks [26-27] or using dynamic structures which reduce the dependency of the power on transistors transition. The well-known methods which lie in this category are adding noise

while it has too much energy overhead, using multiple ring oscillators which disturbs the power consumption by random pulses [38], Garos and Firos uses ring oscillator blocks [30]. Furthermore, there are other methods which change the topology of gates and functions instead adding extra blocks or circuits [15]. Sense Amplifier Based Logic (SABL) and its improved version: TDPL [29], Dynamic and Differential Logic (DDL) [28], Simple Dynamic and Differential Logic (SDDL) , Wave Dynamic Differential Logic (WDDL) [15], Asynchronous Dual-Rail Transition Logic (ADTL) [31], the Masked Dual rail Pre-charge Logic (MDPL) [32], and the Random Switching Logic (RSL) which is based upon random gates [33], Random Multi-Topology Logic (RMTL)[34], and Faking method by injecting fake keys instead real keys in the process[35] are all famous methods which have been introduced for strengthening algorithms.

All the former methods suffer from overheads in terms of CMOS area, power consumption, and speed. In most of hardware contermeasuring methods in gate or cell level, the area and power consumption have been doubled compared to unprotected systems [36]. Therefore, this work focuses on reducing the overhead while increasing system's resistance.

In the majority of cryptographic algorithms, the key is usually injected to the encryption process through an Exclusive- NOR (XOR) gate array and existence of XORs in the first stage acts as a hint in device's power consumption to the attacker [37], thus, increases the vulnerability of the system against power analysis.

In a large number of strengthening techniques, researchers have focused on hardening the whole process. But to the best of our knowledge, there have not been any special works on the XOR gate itself while the XOR gate plays an important role in the process of the algorithm especially at the time of the injection of the data and the key to the process.

In this work, a new method for implementing Exclusive-OR gate has been proposed which it could hide and mask the moment in which the encryption key is injected to the algorithm's process. This approach could reduce the correlation between the power consumption and the input data. The main purpose of this article is to build an Exclusive-NOR (easily extended to a XOR) gate with a fixed operation but random power consumption (RPFL). For abstraction, our proposed structure will be called RPFL which stands for Random Power Fixed Logic. To verify the capability of the proposed Exclusive-OR circuit in strengthening AES encryption algorithm, we have compared the power consumption of an array of proposed random XORs to the power consumption of traditional XORs.

The rest of the paper is organized as the following. In section II, the overall structure of the proposed XOR is described. Section III is dedicated to hardening AES algorithm. Simulations results have been reported in section IV and discussed. Results of simulations have been compared to other works in section V. Finally, conclusion is presented in section VI.

2. THE PROPOSED EXCLUSIVE-NOR GATE

In CMOS circuits, to implement logic gates, one of the conventional methods is using the topology shown in Fig 8.

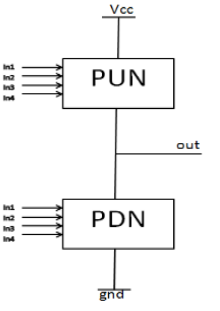


Fig. 1. Topology of construction of circuits and logic functions in CMOS.

In Fig 1, PDN[1] is a part of circuit which is built with NMOS transistors. In addition, PUN[2] is a dual functional circuit which is implemented using PMOS transistors. If two transistors are in parallel in PDN, duality of these transistors in PUN is in series. Similarly, if two transistors are in series in PDN, dual of them in PUN is in parallel. For example, we can refer to the XNOR circuit as shown in Fig 2. This design is called AND-OR-Invert (AOI).

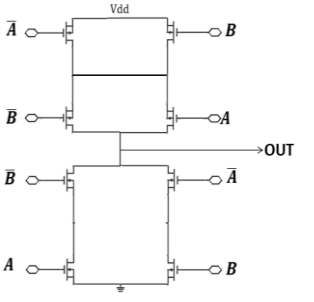


Fig. 2. AOI topology XNOR gate.

The logic function of the circuit above is described by Equation (1).

$$OUT = \overline{A\bar{B} + \bar{A}B} \quad (1)$$

Changing the connections in the above structure, we achieved circuit of Fig 3. This simple modification leads

7- Pull Down Network

8- Pull Up Network

to a change in the dynamic power consumption pattern of the circuit without changing logical operation of the XNOR gate. We call this structure OR-AND-Invert.

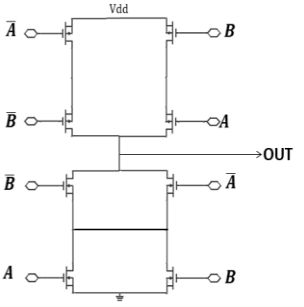


Fig. 3. XNOR gate circuit with OAI topology.

In the circuit shown in Fig. 3, series and parallel combination in PDN, PUN is changed completely. The output function of this circuit is expressed as Equation (2):

$$OUT = \overline{(A+B).(\bar{A}+\bar{B})} \quad (2)$$

As shown in Equation (2), logical operation of both direct and inverted topology is completely equal. By changing the structure of the XNOR gate without changing the logical operation of it, power consumption trace of the gate is changed drastically. By adding two MOS transistors to the circuit of the XNOR gate, the topology of the circuit could be changed by turning each switch on or off. The mentioned circuit is shown in Fig. 4 in which M1 and M2 transistors are used to select between two topologies. Making input signal of the added transistors (R) random, the circuit will be in transition between two so-called topologies randomly, thus, changing the dynamic power consumption of the gate.

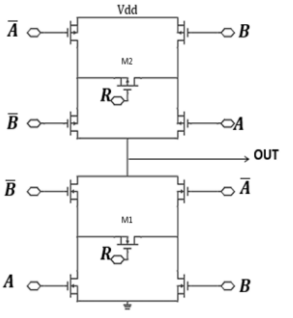


Fig. 4. XNOR circuit with selectable AOI and OAI topology.

If r=0, M1 is off and M2 is on, the circuit is changed to the AOI topology. In contrast, if r=1, M1is turned on and M2 is turned off changing the circuit into the OAI topology. The circuit shown on Fig. 4 is called RPFL circuit which the added transistors disturb the power consumption trace in transition states of the gate. All the transition states are covered in Fig. 5. This figure consists of 4 states based on the value of R and A. In each state, active transistors are highlighted. In addition, according to the transition of B, the dynamic current trace has been presented for each state in Fig. 6.

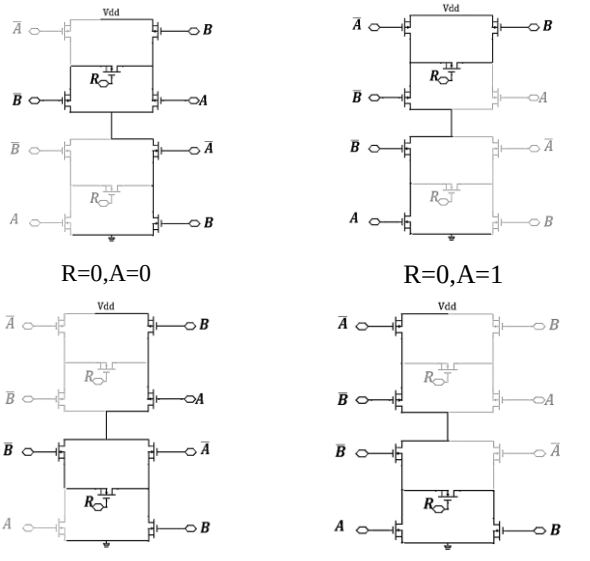
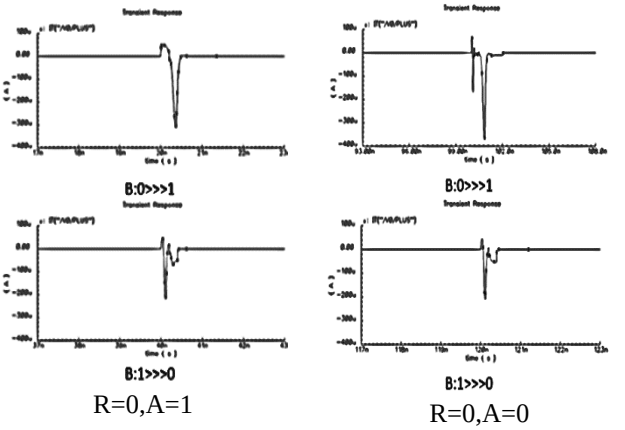
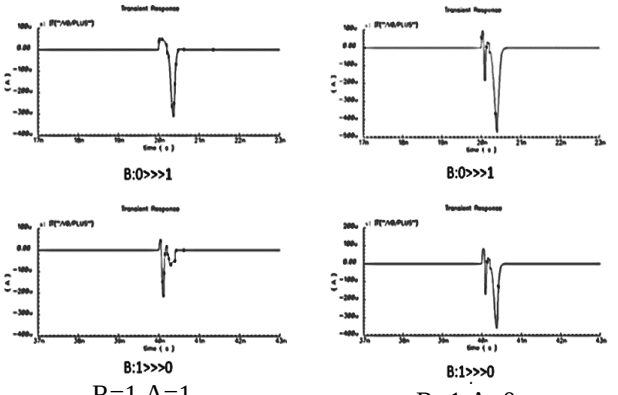


Fig. 5. Four states of RPFL.





R=1,A=1 R=1,A=0

Fig. 6. Four states of RFPL.

For different structures, the dynamic resistance, the resistance between VDD and GND in transition of a circuit, is presented in Table. 1; R_{pon} is the on-resistance of a PMOS transistor. R_{ptr} is the dynamic resistance of a PMOS which is in transition. R_{non} is the on-resistance of an NMOS transistor. R_{ntr} is the dynamic resistance of an NMOS which is in transition. Due to the general VLSI design fundamentals [39], it is assumed that $R_{pon} = 2\,R_{non}$, and $R_{ntr} = R_{ptr}$. Different path resistance in transition states of the modified XNOR gate disturbs the power consumption of the gate in contrast to the mode we have the general-purpose XNOR which its path resistance for all transition states is almost the same and equal to (3Ron+2Rtr). If the controller signal R is injected to the circuit randomly, it could increase the disturbance in the power consumption of the gate drastically due the probability of occurrence of different transition states; for instance, although states 1 and 3 represent the same logic state (A=0 and B is in transition), but their resistance is totally different which injecting a random input to R could disturb the dynamic current passing through the circuit. This disturbance in the power consumption decreases the correlation between the input data and power consumption.

Table 1. Simplified resistance between VDD and GND in transition of the XNOR gate

	New mode	AOI	OAI
State1 R=0 A=0	2Rnon+2Rntr	3Rnon+2Rntr	3Ron+2Rntr
State2 R=0 A=1	2Rnon+2Rntr	3Rnon+2Rntr	3Rnon+2Rntr
state3 R=1 A=0	2.5Rnon+2Rntr	3Rnon+2Rntr	3Rnon+2Rntr
State4		3Rnon+2Rntr	
R=1 A=1	2.5Rnon+2Rntr		3Rnon+2Rntr

3. HARDENING AES AGAINST DPA

3.1. Description of AES

AES is a safe symmetric encryption algorithm which its general flowchart has been shown in Fig 7. According to this chart, there are four main parts in this algorithm which each of them, acts as a function in encryption and decryption process. The main functions include: Sub Byte, Shift Rows, Mix Columns, and Add Round Key.

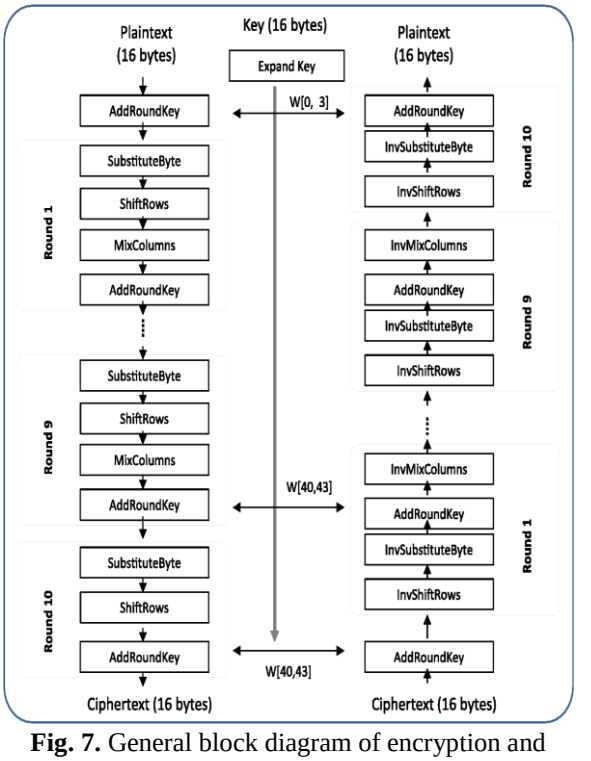


Fig. 7. General block diagram of encryption and decryption in AES.

Sub Byte Function

This unit is the first part of the AES which it is completely nonlinear; it maps each byte of data to a new byte of data based upon a permutation table. This step, leads to a high level of complexity in the algorithm's procedure. It must be pointed out that this step increases the complexity of the power consumption pattern.

On the other hand, other steps of AES are linear. One of the techniques which attackers use for handling successful attacks is dividing the power consumption trace to different parts which each part specifies each step out of the AES steps.

Shift Rows Function

In this section, each row of the data table is shifted to the left side. The value of data does not change, but its location may be changed. There are two methods for

implementing this step: sequential and wires. The traditional method for implementing this section is arrangement of routes, to the extent that without using any extra gates and just using wires it could be accomplished.

Mix Columns Function

In this step, four bytes of each row are combined with another row using reverse linear conversion. This function has 4 bytes of input and 4 bytes of output and operates using multiplication in the Galois field. Each output byte is affected by any of the 4 inputs. Adding this section to the Shift Rows, a challenge emerges in the encryption process. This stage may be implemented with combinational or sequential logic.

Add Round Key Function

The last part of AES rounds, which adds the sub-key to the process, is of high importance for two reasons. First, this part is related to the arrival value of the key to the encryption process. Second, this step combines the data and the key using a simple process easily implemented by an array of XOR gates. This function is illustrated in Fig 8.

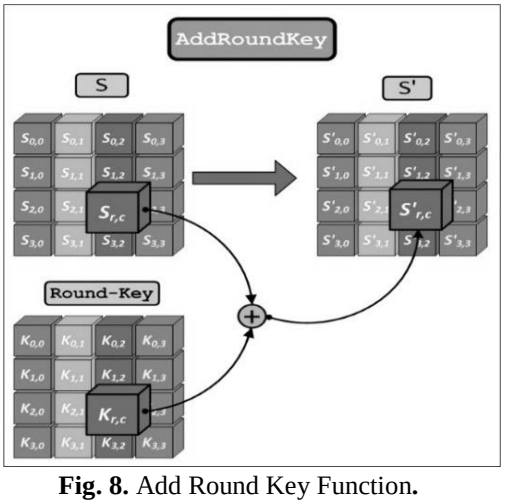


Fig. 8. Add Round Key Function**.**

If the former XOR gates are substituted by the modified XORs (RPFL topology) in Fig. 5, in each round of AES within the Add Round Key Function, the power consumption pattern is intensely disturbed and its correlation with intermediate data in the process is decreased. The improved version of the Add Round Key function is shown on Fig. 9. In this architecture, to harden the system against DPA, the control bit (R) is generated randomly using input data. According to the fact that each of the elements of the arrays in the Add Round Key Function is 32-bits wide, we need 32 XOR gates which they have been visualized in Fig. 9. These 32 gates are randomly operating in AOI or OAI.

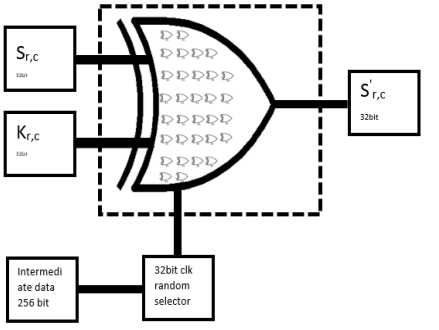


Fig. 9. Implementation for Add Round Key Function using modified XOR.

4. SIMULATIONS AND DISCUSSION

4.1. Area Overhead and Power Consumption

To measure the maximum clock frequency in the system, the critical path from input to output must be considered. According to 90nm fabrication technology, the amount of time required for the data to be ready in an XNOR gate has been presented in Table 2 along with the occupied area and consumed power.

Table 2. Area and consumed power.

	Area	Power	F_max
Unprotected (AOI / OAI)	4 nmos 4 pmos	0.120mw/0 .124mw	100MHz
Protected	5 nmos 5 pmos	0.130mw	99.5MHz

The above results have been obtained from Cadence simulator using TSMC 90nm technology. Area overhead of a single XNOR is 25%, but this overhead is ignorable in the whole system; in other words, it is approximately less than 1%. The speed does not change too much because we have not inserted any dummy gates in the path of data propagation; but, due to the required actions to avoid overlapping of random controller on transition state of the XNOR gate, the maximum clock frequency would be decreased. The power consumption overhead is also negligible; the power overhead for a single XNOR gate is about 10% out of the whole consumed power of the gate which this amount similar to the other overheads is ignorable in the whole system.

4.2. Differential Power Attack (DPA) Test

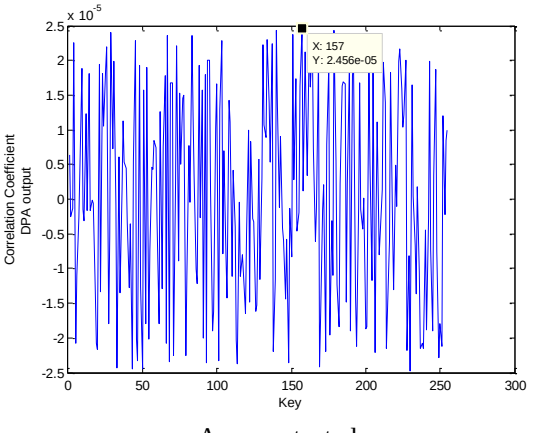
To evaluate the proposed hardening scheme, this plan is applied to the output of the S-Box in Add Round Key step; in detail, the output of the S-Box is XORed with the sub-key and their output will be forwarded to the next step. In this step within AES, 256 bits of the intermediate data is divided into 16 groups of 32-bit elements; each group is XORed to its corresponding sub-key.

To study robustness of the system, the amount of power consumption derived from this step is considered and the correlation between measured power consumption and data for a 4-bit sub-key has been presented in Table 3.

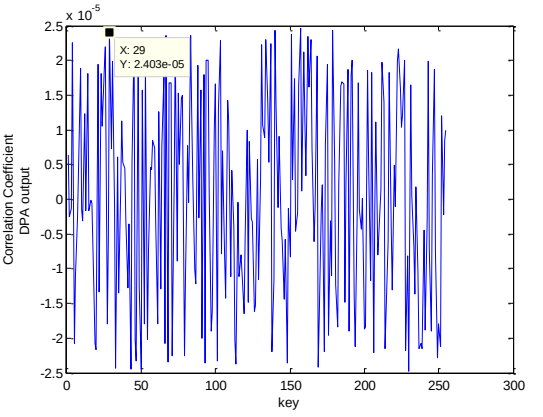
Table 3. Correlation between measured power consumption and data.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Correlation	-0.0160	0.0478	-0.0212	0.0698	-0.0071	0.0129	0.0730	-0.0187	0.0524	0.0488	-0.0959	0.0438	-0.0151	-0.0221	-0.0708	-0.0188

About 35000 samples have been recorded from the power trace. To find a few special bits of the key (sub-key), the 30000 samples have been divided into two groups based on the value of the so-called special bits of the key. Then, the difference between averages of the two groups has been calculated. When a sub-key is guessed correctly, the averages would diverge and the difference between averages of two groups would be maximum. In Fig 10, the output of DPA is shown for 10000 samples of power consumption trace; as it is shown on this Fig, in both of the unprotected and protected implementations, the key has not been found. But, when the number of samples is increased to about 40000 samples, only the protected system with our proposed method remains immune against the attack. This is shown on Fig 11.

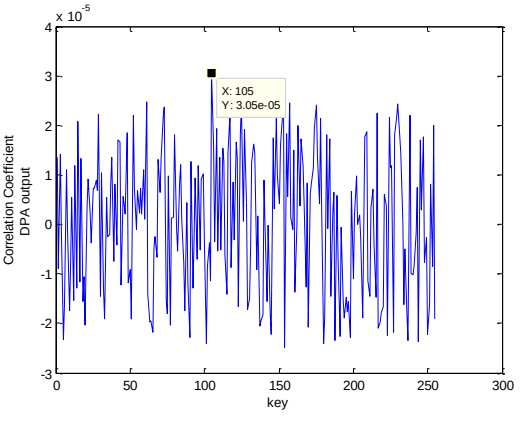


A: unprotected

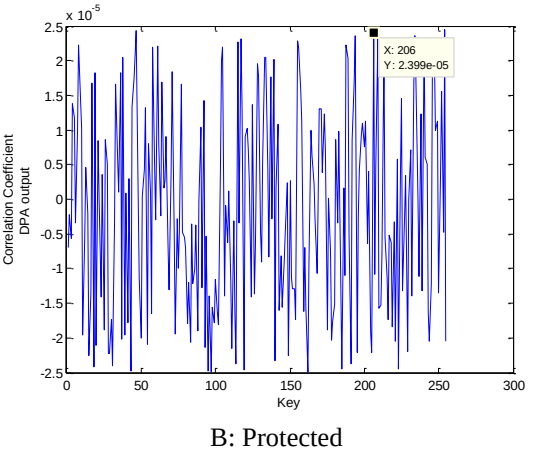


B: Protected

Fig. 10. The output of DPA in unprotected and protected system by 10000 power trace samples.



A: unprotected



B: Protected

Fig. 11. The output of DPA in unprotected and protected system by 40000 power trace sample**.**

Overall, if the number of samples increases to a very large number, this structure will not countermeasure against DPA anymore; because the injected noise is eliminated in a large number of samples, for the existence of the intrinsic averaging property and

subtracting average. In our simulations, our proposed structure was analyzed by DPA for about 70000 samples and DPA could not attack successfully to the system while the unprotected structure failed in less than 40000 samples.

5. OUR CONTRIBUTION

In order to compare the proposed structure with other works, parameters including area, power consumption, and speed have been provided in Table 4.

Table 4. Compare the proposed structure with other works.

	[34]	[38]	[15]	[40]	[41]	[42]	Our method
Technology	40nm	90nm	180nm	65nm	130nm	130 nm	90nm
method	RMTL	CBRO	WDDL	CP-PLL	Current equalizer	Duplicated complement	RPFL
Area overhead	10%	19%	210%	3.5 %	25%	104%	1%
Power consumption Unprotect	-	-	54 mW	14.5 mW	33.2 mW	-	35mW
Vs. Protect			200 mW	15.5 mW	44.3 mW		37mW
Over head		-	270%	3.5 %	33%	-	1%

As it is clear in Table 4, the overheads of our proposed method for contermeasuring in gate level are acceptable. Our recommendation is using the enhanced and modified XOR gate as a contermeasuring device in most cryptographic algorithms.

6. CONCLUSION

In this paper, a new method for strengthening the XOR gate to be used in cryptographic algorithms especially AES, against DPA has been presented. The base of this method relies on injecting power noise using RPFL which has been implemented on 90nm.

The results of simulation demonstrate that the system has an acceptable strength against DPA. The hardware and power overhead were negligible which reduced amount of operational frequency less than 1%. The future work could be implementation of these methods in ASIC to optimize the area overhead and other parameters.

REFERENCES

[1] Katz J, Lindell Y. **"Introduction To Modern Cryptography,"** *CRC press*, 2014 Nov 6.

[2] T. Messerges, E. Dabbish, and R. Sloan, **"Examining Smart-Card Security Under the Threat of Power Analysis Attacks,"** *IEEE Trans. Comput.*, Vol. 51, No. 5, pp. 541–552, May 2002.

[3] Biryukov A, Daemen J, Lucks S, Vaudenay S. **Topics and Research Directions for Symmetric Cryptography,"** *In Proceedings of Early Symmetric Crypto workshop*, 2017 (pp. 4). University of Luxembourg.

[4] Y. Zhang, L. Yang, and J. Chen, **"RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations,"** (Wireless Networks and Mobile Communications). *New York, NY, USA*: Taylor & Francis, 2010.

[5] W. Rankl, W. Effing, "Smart Card **Handbook"**, *New York, NY, USA: Wiley*, 2004.

[6] K. Finkenzeller, **"RFID Handbook: Fundamentals and Applications in Contactless Smart Cards"**, *Radio Frequency Identification and Near-Field Communication*, 3rd ed. New York, NY, USA: Wiley, 2010.

[7] P. C. Kocher, J. Jaffe, and B. Jun, **"Differential Power Analysis,"** *in Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 1999, pp. 388–397.

[8] K. Wu, H. Li, T. Chen, and F. Yu, **"Electromagnetic Analysis On Elliptic Curve Cryptosystems: Measures and Counter-Measures for Smart Cards,"** *in Proc. 3rd Int. Symp. IITA*, Vol. 1, pp. 40–43, 2009.

[9] B. Gammel, H. Bock, and M. Goessel, **"Cryptographic Unit and Method for Operating A Crytographic Unit,"** *U.S. Patent* 7 694 156, Apr. 6, 2010. J.-S. Coron, **"Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems,"** in Cryptographic Hardware and Embedded Systems. New York, NY, USA: Springer-Verlag, 1999, pp. 292–302.

[10] J.-S. Coron, L. Goubin, **"On Boolean and Arithmetic Masking Against Differential Power Analysis,"** *in Proc. 2nd Int. Workshop CHES*, pp. 231–237, 2000.

[11] H. Qu, J. Xu, and Y. Yan, **"A Random Delay Design Of Processor Against Power Analysis Attacks,"** in *Proc. 10th IEEE ICSICT*, pp. 254–256, 2010.

[12] K. H. Boey, Y. Lu, M. O'Neill, and R. Woods, **"Random Clock Against Differential Power Analysis,"** *in Proc. IEEE APCCAS*, pp. 756–759, 2010.

[13] M. Joye, P. Paillier, and B. Schoenmakers, **"On Second-Order Differential Power Analysis,"** *in Proc. 7th Int. Workshop CHES*, Vol. 3659. Edinburgh, U.K., Aug./Sep. 2005, pp. 293–308.

[14] K. Tiri, M. Akmal, and I. Verbauwhede, **"A Dynamic and Differential Cmos Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis On Smart Cards,"** *in Proc. 28th ESSCIRC*, 2002, pp. 403–406.

[15] K. Tiri and I. Verbauwhede, **"A Logic Level Design Methodology for A Secure Dpa Resistant Asic Or Fpga Implementation,"** *in Proc. Des., Autom. Test Eur. Conf. Exhibit*., Vol. 1. 2004, pp. 246–251.

[16] D. Hwang et al., **"Aes-Based Security Coprocessor Ic In 0.18-Mm Cmos With Resistance To Differential Power Analysis Side-Channel Attacks,"** *IEEE J. Solid-State Circuits*, Vol. 41, no. 4, pp. 781–792, Apr. 2006.

[17] C. Tokunaga and D. Blaauw, **"Securing Encryption Systems with A Switched Capacitor Current Equalizer,"** *IEEE J. Solid-State Circuits*, Vol. 45, No. 1, pp. 23–31, Jan. 2010.

[18] D. Kamel, M. Renauld, D. Bol, F.-X. Standaert, and D. Flandre, **"Analysis of Dynamic Differential Swing Limited Logic For Low-Power Secure Applications,"** *J. Low Power Electron. Appl.*, Vol. 2, No. 1, pp. 98–126, 2012.

[19] S. Mangard, **"Masked Dual-Rail Pre-Charge Logic: Dpa-Resistance Without Routing Constraints,"** in *Proc. 7th Int. Workshop Syst. CHES*, 2005, pp. 172–186.

[20] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, **"Evaluation Of The Masked Logic Style Mdpl On A Prototype Chip,"** *in CHES (Lecture Notes in Computer Science)*, Vol. 4727, P. Paillier and I. Verbauwhede, Eds. New York, NY, USA: Springer-Verlag, 2007, pp. 81–94.

[21] Clavier C, Coron JS, Dabbous N. "**Differential Power Analysis in The Presence of Hardware Countermeasures,"** *In Cryptographic Hardware and Embedded Systems—CHES* 2000, pp. 13-48, Springer Berlin/Heidelberg.

[22] Lu Y, O'Neill MP, McCanny JV**.** "**Fpga Implementation and Analysis of Random Delay Insertion Countermeasure Against DPA,"** *In ICECE Technology, 2008. FPT 2008. International Conference on 2008* Dec 8, pp. 201-208, IEEE.

[23] Guilley S, Sauvage L, Flament F, Vong VN, Hoogvorst P, Pacalet R. **"Evaluation of Power Constant Dual-rail Logics Countermeasures Against dpa with Design Time Security Metrics. Ieee Transactions on Computers"** Vol. 59(9), pp. 1250-63, 2010.

[24] Messerges TS. **"Using Second-Order Power Analysis To Attack Dpa Resistant Software,"** *In International Workshop on Cryptographic Hardware and Embedded Systems 2000* Aug 17, pp. 238-251, Springer, Berlin, Heidelberg.

[25] Mangard S. **"Hardware Countermeasures Against Dpa-A Statistical Analysis of Their Effectiveness,"** In ct-rsa 2004 Feb 10, Vol. 2964, pp. 222-235.

[26] J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor, **"Security Evaluation of Asynchronous Circuits,"** *Proc. International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 125-136, 2003.

[27] K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, **"Prototype Ic with Wddl and Differential Routing-Dpa Sesistance Assessment,"** *Proc. International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 354-365, 2005.

[28] Verbauwhede, Ingrid M., and Kris JV Tiri. "**Dynamic and Differential Cmos Logic with Signal-Independent Power Consumption To Withstand Differential Power Analysis.**" *U.S. Patent 7,417,468, issued August 26*, 2008.

[29] Bucci M, Giancane L, Luzzi R, Trifiletti A. **"Three-Phase Dual-Rail Pre-Charge Logic"**. *In CHES 2006 Aug*, Vol. 4249, pp. 232-241.

[30] Dichtl M, Golić JD. **"High-Speed True Random Number Generation With Logic Gates Only,"** *In International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 45-62, Springer, Berlin, Heidelberg, 2007.

[31] T.S. Messerges, E. Dabbish, and R. Sloan, **"Investigations of Power Analysis Attacks on Smartcards,"** *Proc. USENIX Workshop Smartcard Technology*, pp. 151-161, 1999.

[32] Popp T, Mangard S. **"Masked Dual-Rail Pre-Charge Logic: Dpa-Resistance Without Routing Constraints,"** *In International Workshop on Cryptographic Hardware and Embedded Systems 2005 Aug 29*, pp. 172-186, Springer, Berlin, Heidelberg.

[33] Suzuki D, Saeki M, Ichikawa T. **"Random Switching Logic: A Countermeasure against DPA based on Transition Probability,"** IACR *Cryptology ePrint Archive*. 2004, 346.

[34] Fish A, Avital M, Dagan H, Keren O, **"Inventors; Bar-Ilan University, assignee. Multi-topology logic gates,"** *United States patent application US 15/301,409*. 2015 Apr 29.

[35] Lumbiarres-Lopez R, Lopez-Garcia M, Canto-Navarro E. **"Hardware Architecture Implemented On Fpga For Protecting Cryptographic Keys Against Side-Channel Attacks,"** *IEEE Transactions on Dependable and Secure Computing*. 2016 Sep 19.

[36] Moradi A, Poschmann A. **"Lightweight Cryptography and DPA Countermeasures: A Survey,"** *InFinancial Cryptography Workshops 2010 Jan 25*, pp. 68-79.

[37] Tuyls P, Hollmann HD, Van Lint JH, Tolhuizen LM. **"XOR-based visual cryptography schemes. Designs, Codes and Cryptography,"** Vol. 37(1), pp.169-86, 2005.

[38] Liu PC, Chang HC, Lee CY. "**A Low Overhead Dpa Countermeasure Circuit Based On Ring Oscillators,"** *IEEE Transactions on Circuits and Systems II:* Express Briefs, Vol. 57(7), pp. 546-50, 2010.

[39] Taur Y, Ning TH. "**Fundamentals of modern VLSI devices,"** *Cambridge university press*; 2013 May 2.

[40] Attaran, A. and Mirhassani, M., 2015, July. "**An Embedded Low-"Overhead Pll-Based Countermeasure Against Dpa Side Channel Attack,"** *In Signals, Circuits and Systems (ISSCS), 2015 International Symposium on*, pp. 1-4, IEEE.

[41] C. Tokunaga, D. Blaauw, **"Secure Aes Engine with A Local Switched-Capacitor Current Equalizer,"** *In Proceedings of ISSCC Dig. Tech. Papers*, pp. 274-275, Feb. 2009.

[42] M. Doulcier-Verdier, et al., **"A Side-Channel and Fault-Attack Resistant Aes Circuit Working On Duplicated Complemented Values,"** *In Proceedings of ISSCC Dig. Tech. Papers*, pp. 274-275, Feb. 2011.