Journal of Computer Science

Original Research Paper

A Defense Mechanism for Differential Power Analysis Attack in AES

[1]M. Rajaram and [2]J. Vijaya

[1]Anna University, Chennai, India
[2]Vice Chancellor, Anna University, Chennai, India

Article history
Received: 16-05-2014
Revised: 19-05-2014
Accepted: 26-08-2014

Corresponding Author:
Vijaya, J.
Anna University, Chennai, India
Email: vijayajv@rediffmail.com

Abstract: In modern wireless communication world, the security of data transfer has been the most challenging task. In embedded system, AES is the most extensively used cryptographic algorithm in practice. But its functionality has been disrupted by the DPA attack. There have been several countermeasures to tackle those attacks, but this study proposes variably a new measure to defend this DPA attack. DPA attack is possible due to the power fluctuation happening due to sequential circuit clocking during the process of substitute byte in AES encryption in the first round and last round. Hence to prevent this, the power variation is maintained at a constant pace throughout the data processing. This is achieved by incorporating a combinational logic design instead of a sequential logic circuit in AES. The proposed design is implemented in Vertex III FPGA device and found even after 17230 power traces the secret key is not disclosed as the power fluctuations is completely random. The power consumption when experimented by micro wind software proves to be constant and the same power (almost) is obtained while implementing it hardware and no chance of identifying the instant of data processing is achieved.

Keywords: AES, Cryptography, DPA Attack, FPGA, Power Consumption

Introduction

In this modern world, the use of cell phones, smart cards and other wireless applications became unavoidable in human's everyday life. Simultaneously, the security of data transfer should also be taken into account. Some hackers technically disclose the secret key with the help of leakage of information like power consumption, output timing, electromagnetic radiation and thermal radiation as shown in Fig. 1.

DPA is the most popular attack made on AES, where the power analysis is done based on hamming distance and hamming weight models. Nowadays, few stretchy algorithms are designed for secured data transfer protocols and applications have been introduced to face the rising demand of cryptography. In this study, a preventive measure for threat of power analysis has been suggested and a preventive method for AES is examined and implemented.

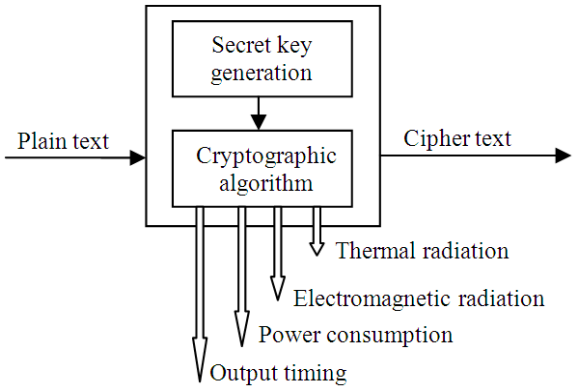


Fig. 1. Information leakage from Cryptographic devices

Related Work

The most distinguishing plan for power analysis attack is on the smart cards which are capable of performing secured computations. The cryptographic

architecture operates on 8 bit data blocks because of 8 bit architecture. The Simple Power Analysis and Differential Power Analysis were first introduced by (Kocher *et al*., 1999). With the leakage of information based power dissipation or power consumption in AES, the secret key can be successfully extracted without the knowledge of design of encryption algorithm. Masking and randomized masking (Wang and Ha, 2013) is common method to prevent DPA. Balanced Load Dual Rail CMOS (Sokolov *et al*., 2005; Batina *et al*., 2005; Kulikowski *et al*., 2005; Tiri and Verbauwhede, 2005; Bucci *et al*., 2005), where gates are balanced so that load switching capacitance is same. This has significant area and power overhead. Random Delay Insertion (Bucci *et al*., 2005; Strachacki and Szczepanski, 2008), where special flip-flops are inserted to interrupt the process throughout the data path. Most of the countermeasures concentrated on use of minimum signal strength and information (Boey *et al*., 2010; Mazumdar *et al*., 2012; Durga *et al*., 2013).

Power Analysis Attack

The most common method used by attackers is power analysis attack. They capture the leakage power or the power fluctuation occurring during the cryptographic process. Normally this is done by inserting a small resistor in series with the power source or the ground and monitoring it. There are two type of power analysis attack namely, Simple power analysis and Differential power analysis. Simple Power Analysis (SPA) is most common and useful only when the algorithm is known. The Differential Power Analysis (DPA) (Boey *et al*., 2011; Carlier *et al*., 2004; Waddle and Wagner, 2004) is the most powerful method based on statistical analysis and characteristics of the captured power traces. It is effective even when the algorithm is unknown. It is normally executed by comparing the power traces captured using the known key and the unknown key. They are correlated within each other to guess the correct key.

Power Characteristics: The possibility of power analysis attack depends on the availability of power approximation method using hamming distance and hamming weight power models. The DPA power trace database (Hnath, 2010) is shown in Fig. 2 and depicts the 10 rounds of AES-128 encryption.

Differences in instantaneous power consumption are related to the bit values that are being manipulated. As bit values change, the essential hardware related, consumes power on a much lower scale. Due to slight power variation, detection becomes more difficult. It requires modifications to the hardware or statistical techniques to identify and correlate the values. As more number of data bit transition from logic 0 to logic 1 takes place, more power is consumed.

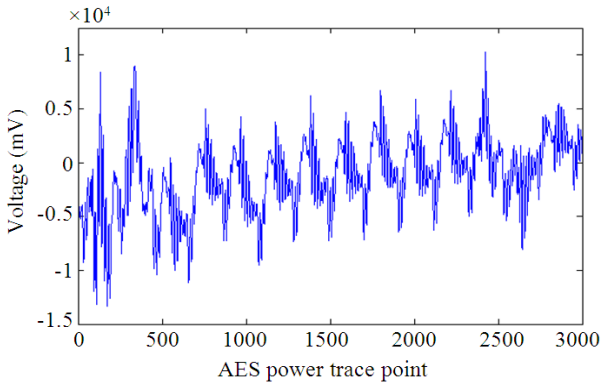


Fig. 2. A sample AES power trace showing the power consumption over 10 rounds of an AES-128 encryption

Proposed Work

In general, it is clear that the DPA is possible because of the power radiated or leaked during the process by the registers used. As stated earlier, one possible way, as proposed by Rijndael, the randomization of information has been implemented. The attack in the first round of AES is not possible because of the use of XOR gate [combinational circuits] between plain text and key before loading them into the register for successive processing. In addition to randomization, instead of registers, the processing [Key generation and encrypting] has been implemented using combinational circuit to minimize the power leakage due to state change in registers. The proposed architecture is compared with the previous architectures proposed by Rijndael. The proposed architecture consists of random delay combinational circuit design for initial and final round processing, preventing the uniform power fluctuation.

In AES attack program, the 128-bit cipher text message is split into byte long blocks. AES decryption algorithm operates on each byte individually and key guess is done for each 8-bit portion of the round key. The relationship between the hamming distance of the bits in the data registers before and after 10th round of encryption and power fluctuation has been used to decode the key/data. Figure 3 shows that the correlation between the data and power consumption for all 16 bytes. The correlation group between sensitive data and the power consumption show a complete randomness making the hamming distance model, a difficult one to be used for extracting data and it is clear that the power consumption and information cannot be correlated for finding the key/data.

In AES, the final round sub key is recovered with large amount of power traces by the attackers. Our

method shows that the power consumption is almost constant as shown in Fig. 4 and even after 17,230 power traces the correct key was not successfully traced.

The Proposed Change in the Circuit

In AES algorithm the sequential circuit used in the circuit can be modified to combinational logic circuit as shown in the Fig. 5a and b so that processing does not change the output for the given input combination. By removing clock signal, the chance for the hacker to grasp the information is entirely avoided thereby preventing the Differential Power Analysis attack.

By replacing sequential circuit to combinational circuit the power variations in the circuit become constant and no chance of identifying the instant of data transfer. Fig. 6 shows the power variation in the existing method using sequential circuit and Fig. 7 shows the power variation in the proposed method where only combinational circuit is being used.

The experimental results for power variations are obtained using for existing and proposed methods using micro wind software are shown as in Fig. 6 and 7 respectively.

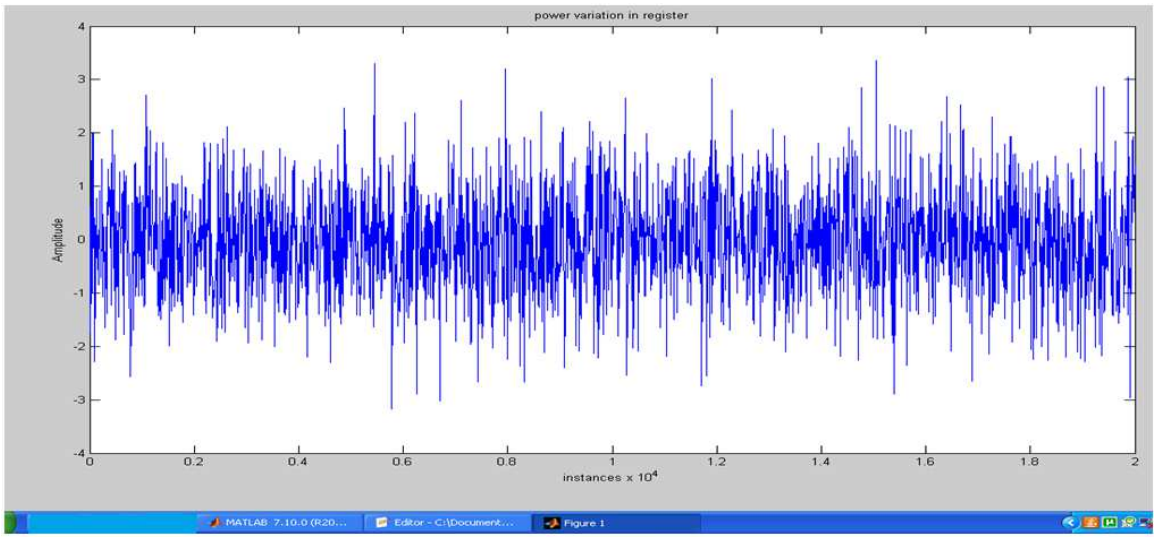


Fig. 3. The correlation between the sensitive data and the power consumption for the 128 key guesses for all 16 bytes

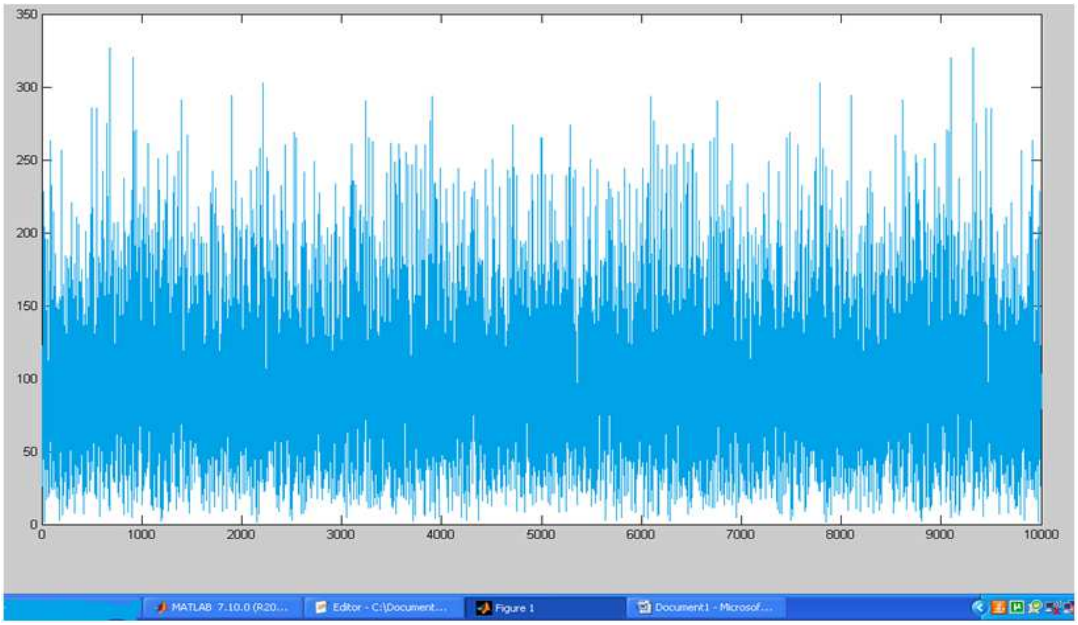


Fig. 4. Captured Power variation during the final round of the AES Encryption

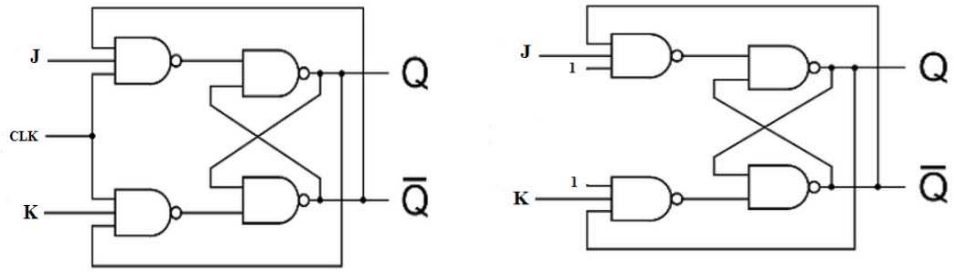


Fig. 5. (a) Sequential circuit (b) Combinational circuit

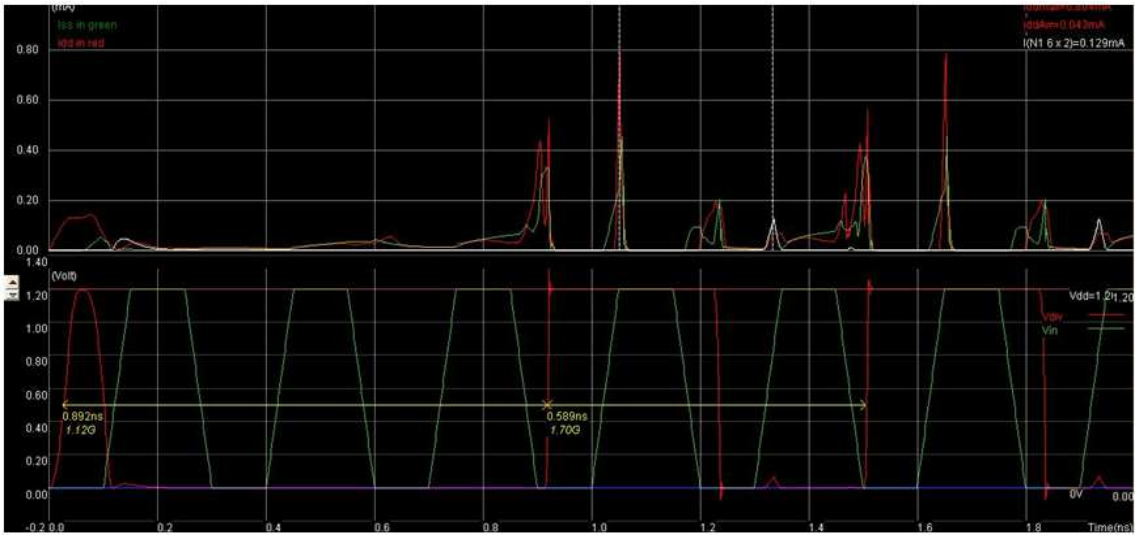


Fig. 6. Power variation of existing method

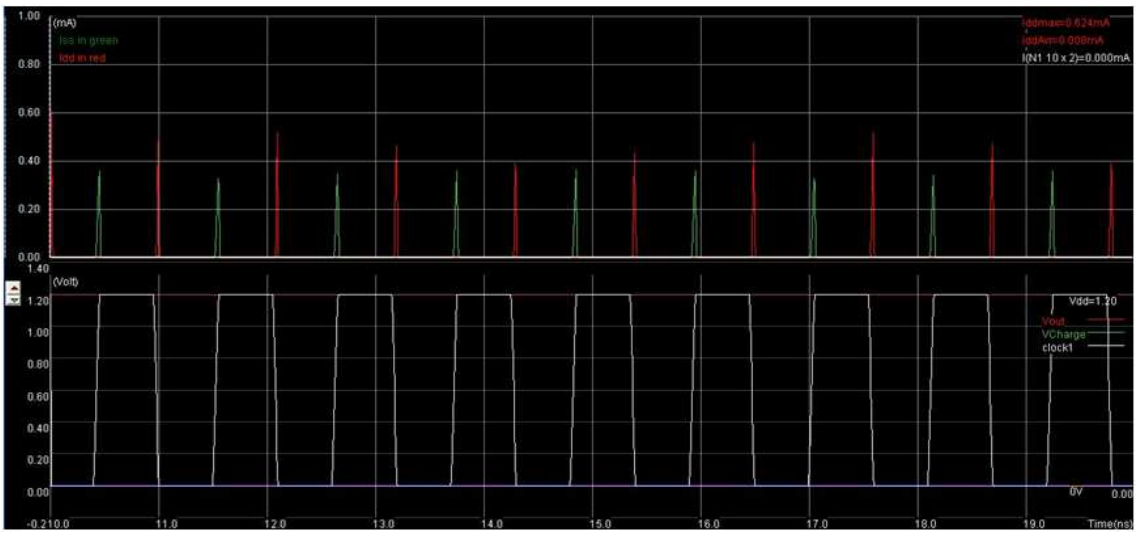


Fig. 7. Power variation of proposed method

Experimental Results

The realization of pipelined architecture of high-through put 128 bits AES cipher processor in Vertex III FPGA by new high-speed and hardware sharing functional blocks are shown in Fig. 8a (Hardware Setup) and 8b (VHDL Simulation).

By using the decryption program operated on 8-bit portion of the cipher text for 256 times i.e., for all possible combination the correlation value

does not seem to be differentiated from the correct key guess.

The memory complexity is dramatically reduced using the Content-Addressable Memory (CAM) compared to the SRAM based S-box and Inverse S-box look-up tables. The new hardware sharing architecture is applied to implement the proposed high-speed secure encryption. The resource utilized is given in Table 1. The description of the measured parameter for the proposed method is compared with conventional methods shown in Table 2.

Discussion

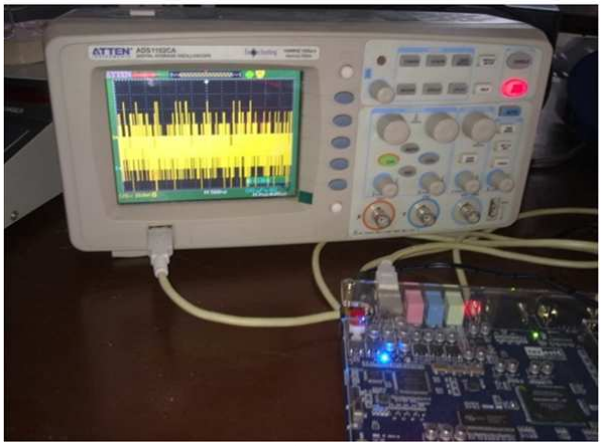
In this study, an effective and more powerful enhanced DPA method to protect the secret key from an AES hardware implementation is presented. The implemented combinational circuit design for AES is highly inaccessible for power analysis attack. The implementation result shows reduced resource utilization of minimum 50% and the increased number of traces. The power traces are captured and the key extraction is also done.

Table 1. Comparison of the different AES implementation

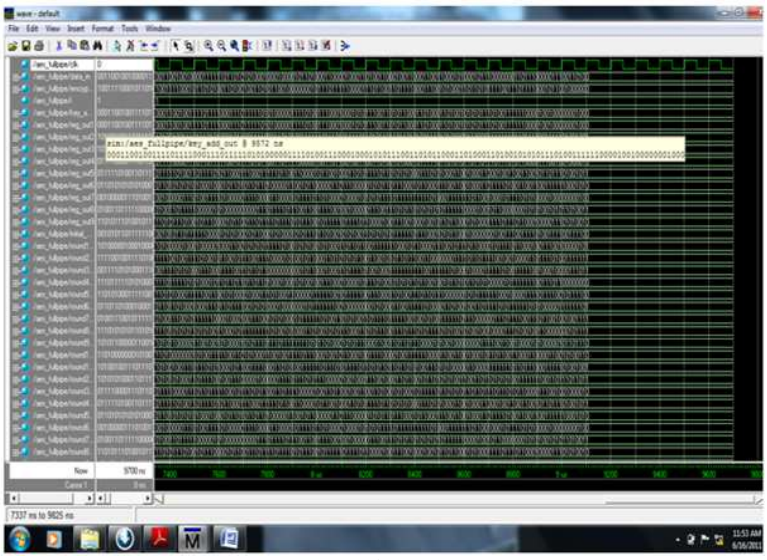
	Device	Device utilization	Type
L.T. Emmanuel 802.11i	Spartan3	2154	Parallel
D.H. Bae	Spartan3	5605	Sequential
Proposed method	Vertex3	260	Combinational

Table 2. Number of power traces for proposed Vs existing methods

Author	No. of power traces
Chin Chi Tiu	9000
Yu HAN *et al*.,	6000
Proposed method	17230



(a)



(b)

Fig. 8. (a) Fully pipelined combinational AES (Hardware setup) (b) Fully pipelined combinational AES (VHDL Simulation)

Conclusion

The proposed work illustrates the significant reduction in resource utilization and the secret key cannot be guessed even after 17230 traces are when compare to previous method requires 9000 traces. Thus, our proposed method strongly outshine in effectiveness, computational requirement and robustness. This performance improvement is with the introduction of first round XOR combinational circuit design AES architecture. As this is a general structure improvement for the prevention of attack towards the existing architecture all limitation of implementation in existing architecture is applicable but it's highly immune to DPA attack.

Acknowledgment

I thank Anna University, Chennai and Thanthai Periyar Government Institute of Technology, Vellore, for providing the necessary software and hardware facility towards this research work.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Batina, L., N. Mentens and I. Verbauwhede, 2005. Side-channel issues for designing secure hardware implementations. IEEE Int. Test. Sympos. DOI: 10.1109/IOLTS.2005.64

Boey, K.H. M. O'Neill and R. Woods, 2011. How resistant are S boxes to power analysis attacks? Proceeding of the 4th IFIP International Conference on New Technologies, Mobility and Security, Feb. 7-10, IEEE Xplore Press, Paris, pp: 1-6. DOI: 10.1109/NTMS.2011.5720614

Boey, K.R., P. Hodgers, Y. Lu and M. O'Neill, 2010. Security of AES Sbox designs to power analysis. Proceedings of the 17th IEEE International Conference on Electronics, Circuits and Systems, Dec. 12-15, IEEE Xplore Press, Athens, pp: 1232-1235. DOI: 10.1109/ICECS.2010.5724741

Bucci, M., R. Luzzi, M. Guglielmo and A. Trifiletti, 2005. A countermeasure against differential power analysis based on random delay insertion. Proceedings of the 2005 IEEE International Symposium on Circuits and Systems, May 23-26, Kobe, Japan, IEEE Xplore Press, pp: 3547-3550. DOI: 10.1109/ISCAS.2005.1465395

Carlier, V., H. Chabanne, E. Dottax and H. Pelletier, 2004. Electromagnetic side channels of an FPGA implementation of AES.

Durga, N., P. Avirneni and A.K. Somani 2013. Countering power analysis attacks using reliable and aggressive designs. Student Member, IEEE Trans. Comput., 63: 1408-1420. DOI: 10.1109/TC.2013.9

Hnath, W., 2010. Differential power analysis side-channel attacks in cryptography. Project Submitted to the Faculty of Worcester Polytechnic Institute.

Kocher, P.C., J. Jaffe and B. Jun, 1999. Differential power analysis. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, Aug. 15-19, Springer-Verlag London, UK, 388-397. DOI: 10.1007/3-540-48405-1_25

Kulikowski, K.J., M. Su, A. Smirnov, A. Taubin and M.G. Karpovsky *et al*., 2005. Delay insensitive encoding and power analysis: A balancing act. Proceedings of the 11th IEEE International Symposium on Asynchronous Circuits and Systems, Mar. 14-16, IEEE Xplore Press, Washington, DC, USA, pp: 116-125. DOI: 10.1109/ASYNC.2005.18

Mazumdar, B., D. Mukhopadhyay and I. Sengupta, 2012. Design for security of block cipher S-boxes to resist differential power attacks. Proceedings of the 25th International Conference on VLSI Design, Jan. 7-11, IEEE Xplore Press, Hyderabad, pp: 113-118. DOI: 10.1109/VLSID.2012.56

Sokolov, D., J. Murphy, A. Bystrov and A.M. Yakovlev, 2005. Design and analysis of dual- rail circuits for security applications. IEEE Trans. Comput., 54: 449-460. DOI: 10.1109/TC.2005.61

Strachacki, M. and S. Szczepanski, 2008. Implementation of AES algorithm resistant to differential power analysis. Proceedings of the 15th IEEE International Conference on Electronics, Circuits and Systems, Aug. 31-Sept. 3, IEEE Xplore Press, St. Julien's, pp: 214-217. DOI: 10.1109/ICECS.2008.4674829

Tiri, K. and I. Verbauwhede, 2005. Design method for constant power consumption of differential logic circuits. Proceedings of the conference on Design, Automation and Test in Europe, Mar. 7-11, IEEE Xplore Press, pp: 628-633. DOI: 10.1109/DATE.2005.113

Waddle, J. and D. Wagner, 2004. Towards efficient second-order power analysis. Proceedings of the 6th International Workshop Cryptographic Hardware and Embedded Systems, Aug. 11-13, Springer Berlin Heidelberg, Cambridge, MA, USA, pp: 1-15. DOI: 10.1007/978-3-540-28632-5_1

Wang, Y. and Y. Ha, 2013. FPGA-based 40.9-gbits/s masked AES with area optimization for storage area network. Circuits Sys. Express Briefs IEEE Trans., 60: 36-40. DOI: 10.1109/TCSII.2012.2234891