A Novel Architecture of Masked Logic Cells for Side-Channel Attacks

Abhishek Kumar[1]*, Manoj Sindhwani[1], Shippu Sachdeva[1]
School of Electronics and Electrical Engineering, Lovely Professional University, Punjab, India.
E-mail: abkvjti@gmail.com (Corresponding author)

Received: 4 September 2022 Revised: 26 October 2022 Accepted: 17 November 2022

ABSTRACT:
Side-channel attacks are attacks against cryptographic devices that are based on information obtained by leakage into cryptographic algorithm hardware implementation rather than algorithm implementation. Power attacks are based on analyzing the power consumption of a corresponding input and obtaining access to this method. The power profile of the encryption circuit maintains an interaction with the input to be processed, allowing the attacker to guess the hidden secrets. In this work, we presented a novel architecture of masked logic cells that are resistant to power attacks and have reduced cell numbers. The presented masking cell reduces the relationship between the actual power and the mathematically approximated power model measured by the Pearson correlation coefficient. The security aspect of the logic cell is measured with the correlation coefficient of the person. The proposed mask-XOR and mask-AND cells are 0.0053 and 0.3respectively, much lower than the standard XOR and AND cells of 0.134 and 0.372, respectively.

KEYWORDS: Side-Channel Attack, Power Attack, Mask Cell, Correlation, Data Hiding, Hardware Security.

1. INTRODUCTION

Cryptographic device based on complex mathematical function leaks secondary information in terms of power, delay, fault, and radiation while computing, due to hardware limitation. Scaling offers an advantage in area reduction, but continuous scaling enhances power requirements. The data-dependent part of power consumption leads to a novel class of security attacks. The attacker targets the weak point of the cryptographic chip to reveal the secret from the internal node using side-channel analysis. Power attack is a widely studied side-channel attack threat to cryptographic circuits; observed in [1, 2], it bypasses the academic strength of the cryptographic algorithms. The most studied power analyses are simple power analysis (SPA) based on correlation coefficient and differential power analysis (DPA) based on the difference of mean discussed in [3] to try to obtain the hidden internal secret. The attacker exploits a mathematical model and predicts the relationship between approximated power and intermediate result ease to reveal the secret key discussed in [4-7].

It is not sufficient to include security in the integrated circuit (IC) at the algorithmic level. Protection aligns with various design levels during design and fabrication known as attack-resistant IC. The complementary metal-oxide-semiconductor field-effect transistor (CMOS) based cell library is the default standard for low-power VLSI circuit design. Dynamic power consumption is dependent on the input data to be processed. Protection aligns with various design levels during design and fabrication known as attack resistance. A power attack-resistant circuit must not maintain data-dependent power consumption. Two popular countermeasures approach is hiding and masking. The hiding approach makes the intermediate value data independent of power consumption by producing equal power consumption for all input and the masking approach randomized the circuit with the inclusion of redundant cells into the circuit. It modifies the circuit power consumption at various levels whereas the masking technique randomizes the input signals to bypass input-output data dependency. The hiding countermeasure technique presented in [8] makes power consumption independent and focused on detaching the power supplies, according to [9-10] insertion of an on-chip noise generator to equalize the power and insert a random delay highlighted in [11] into the critical path. The masking approach to counteract the power attack is to randomize the intermediate result in the cryptographic algorithm such that the power consumption of the device under test (DUT) randomized the intermediate results which are uncorrelated to the actual intermediate results. Masking

Paper type: Research paper
DOI:.30486/mjee.2023.1975092.1026
How to cite this paper: A. Kumar, M. Sindhwani and S. Sachdeva, **"A Novel Architecture of Masked Logic Cells for Side-Channel Attacks"**, *Majlesi Journal of Electrical Engineering*, Vol. 17, No. 1, pp. 75-80, 2023.

can employ at the algorithmic level or cell (cell) level. Masking at the algorithmic level highlighted in [12] elaborates the need to rewrite such that the intermediate result gets randomized; the alternative is a masked cell.

In the power analysis attack, one uses the dependency between actual power consumption with the mathematically approximated power via hamming weight (HW) or hamming distance (HD) of the input. The output of the cryptographic circuit relies on the HW/HD of the final output terminal. Power attack-resistant mask circuit creates multiple internal nodes; power value depends on all internal nodes instead of a single node. The HW of data is to be processed and looks random to attackers. The output of the non-linear module does not depend on the original data to be processed (unmask); it depends on masked data. Fig 1 presents that at the output terminal, the mask bit needs to unmask with a random bit generated internally or externally to the circuit.

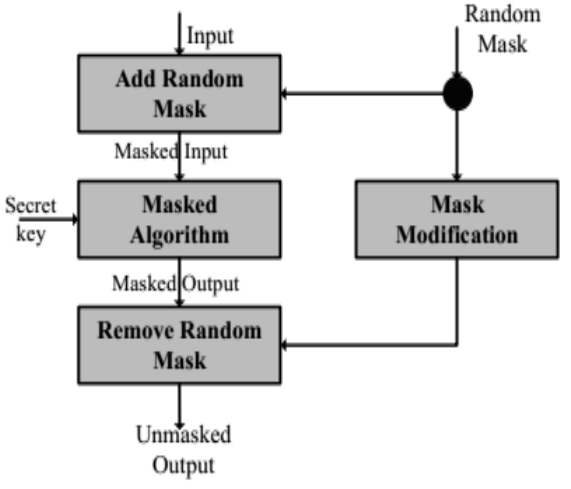

Fig. 1. Masking Flowchart.

The goal of power attack countermeasure is either completely remove or reduce the correlation. Practically it is not possible to remove the data dependency altogether, adding noise or reducing the power value at an internal terminal correlation between actual and predicted power could reduce. Masking is applied on an algorithmic level without modifying the power consumption properties and without changing the power characteristic of the cryptographic circuit. Masking is a method to randomize the internal result at the algorithmic or cell level. The Mask cell introduced in [13], is based on the method of an additional component such that the intermediate result shows equal power consumption. Existing work shows the input bits of the circuit masked with a mask generator and output unmasked with the same or different mask generator.

The contribution of this work is to the novel architecture of attack-resistant mask cells to implement the cryptographic module. The presented XOR and AND cell security aspects were evaluated with the person correlation coefficient. A higher correlation value indicates that power patterns are highly dependent on processed data and vice versa. The measure of dependency of power profile over data pattern shows a reduction in correlation coefficient by masked XOR and masked AND 96 % and 19.35%, respectively compared to standard cell.

The structure of the paper is organized as follows; section 2 briefly explains the basis of power attack with energy and power model. Section 3 presents the theoretical concepts of the mask cell. Section 4 presents the security aspect of mask XOR and mask AND cell with static unmask cell, and article is concluded in section 5.

2. REGULAR UNMASK CELL

CMOS-based circuit implementation is the default standard for low-power standard cell libraries. Power consumption of CMOS implementation is classified into (a) static unmask power Psw, (b) dynamic power Pdyn and (c) short circuit power Psw. Static unmask power also is known as leakage power when the circuit remains ideal comes up with minimal value. Dynamic power in equation (1) is the dominant factor and consumes more than 98% of the total energy of the circuit.

$$Pdyn = \alpha f_{clk} C_L V_{dd}^{\ 2} \qquad (1)$$

Where, α is the switching activity factor 0-1 or 1-0 transition during the clock, fclk is the frequency of the input, CL load capacitor, and Vdd is the power supply. Power attack arises with switching factors; a significant amount of information leaks during switching from low to high (0-1) or high to low (1-0) due to the charging and discharging nature of load capacitance. In [14], it is observed that a higher value of current observe during charging results in higher power consumption for 0-1 transition compared to 1-0 transition. For the constant output node, 0-0 or 1-1 consumes minimal power due to static current. In a CMOS-based digital circuit's maximum fraction of power governs by dynamic value while static reveal power is minimal. The dynamic power of the CMOS circuit is data-dependent because maintaining of same output voltage does not consume energy while switching of output level consumes a significant amount of energy. The energy requirement to transit output terminal presented as; $E_{0\text{-}0}$ and $E_{1\text{-}1}$ is energy consumed to maintain the same output level; $E_{0\text{-}1}$ and $E_{1\text{-}0}$ denote energy required to perform 0-1 and 1-0 transition. The energy consumption of a circuit is measured as a summation of instantaneous power

consumed by a circuit over t_0 to t_1 presented in equation (2).

$$Energy = \int_{t_0}^{t_1} P_{\text{int}} dt \qquad (2)$$

The energy required to maintain of same output level $E_{0\text{-}0}$ and $E_{1\text{-}1}$ is almost zero energy while $E_{1\text{-}1} > E_{0\text{-}0}$ to sustain a high output level. The energy required to charge the capacitor is more significant than discharge $E_{0\text{-}1} > E_{1\text{-}0}$ because of the charging current and time of the load capacitor. Power analysis is classified as a non-invasive attack without tampering with the hardware information that can extract statistically also known as reverse engineering. To prevent attackers against power attack, circuit should consume the same amount of energy in all transitions i.e., $E_{00} = E_{01} = E_{10} = E_{11}$. In the case of [Average E(y=0)], = [Average E(y=1)] circuit would not reveal information along with dynamic power; in other words, power consumption is independent of input data; a primary requirement of a power attack resistant circuit. Cadence specter-based simulation result at CMOS 90nm technology node reveals; a standard XOR exhibits energy requirement to compute low output average E(y=0) = 1.6475 fJ and high output E(y=1) = 1.47 fJ, while standard AND exhibits energy requirement to compute low output average E(y=0) = 0.715 fJ and high output E(y=1) = 1.555 fJ. Equation (3) presents a wider energy gap for standard XOR and standard AND to bring output node logic 1 and 0. During power, an attack gives clue to the input data and presents a high probability of a power attack.

Standard XOR: |E(Y=1) – E(Y=0)| = 0.1775 fJ
Standard AND: |E(Y=1) – E(Y=0) = 0.84 fJ| (3)

3. ATTACK RESISTANT MASK CELL

Attack resistant masked cell is based on the concept of distributing the power consumption equally on the internal terminal instead of lumped to the output node. A logic cell transforms into a mask cell by adding additional components to the circuit such that its power is uniformly distributed at the internal terminal without affecting the primary Output. A Mask cell randomized the power consumption of the devices such that the intermediate result is uncorrelated with the actual results. The essential properties of the masked cell are wire does not store intermediate computation value, and the circuit does not switch more than once per clock cycle. The first order of masking requires a random mask bit for each input; uncorrelated to the input and uniformly distributed. One of the significant limitations of the mask cell is glitches; Output switches randomly before settling to the final level.

A lower value of energy requirement for transition (0-1/1-0) lowers the information leaks. Average E(y=0) – Average E(y=1) = 0 the cell is considered as resistant to attack; ideally Average E(y=0) – Average E(y=1) = 0 for the cell used in the circuit [15-17]. It can be achieved by maintaining the same amount of energy required for all transitions i.e., $E_{00}=E_{01}=E_{10}=E_{11}$.

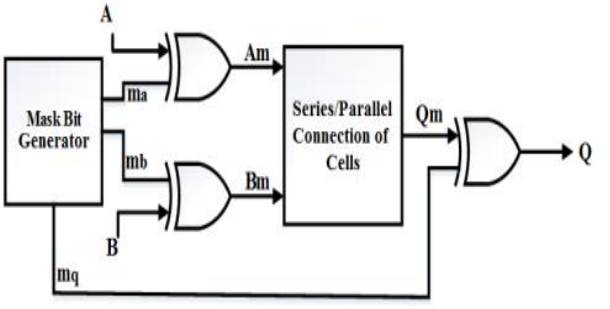

Fig. 2. Mask logic cell.

A free-running random mask generator generates a 1-bit mask bit m_a for A and m_b for B. Fig. 2 presents the block diagram of the mask cell with $Y_m = f(A, m_a, B, m_b)$. A regular 2-input cell is fuzzified with a random bit by inserting an XOR cell, preferably at the input shown by equation (4). Since the XOR cell energy difference is smaller to Output high or low, it is preferred for masking.

$$\begin{aligned} Q_m &= f\left(a_m,\ m_a,\ b_m,\ m_b,\ m_q\right) \\ a_m &= (a \oplus m_a) \\ b_m &= (b \oplus m_b) \\ q_m &= (q \oplus m_q) \end{aligned} \qquad (4)$$

The final output is unmasked with a mask bit generated by a random mask generator or computed by a circuit internally. The masked cell enhances the security level at the cost of added redundancy and extra power consumption. In the digital circuit, the logic level is presented by the voltage level at the primary input/output or intermediate terminal. Since the power consumption of the digital circuit is data-dependent, a significant amount of energy is required to switch logic to a level ($E_{0\text{-}1} \neq E_{1\text{-}0}$). In contrast, zero energy is drawn while the level ($E_{0\text{-}0}=E_{1\text{-}1} \equiv 0$). Maintaining the same logic level does not require energy.

3.1. Mask XOR Cell

Fig. 3 presents the novel architecture of mask XOR cell, which needs 4-XOR and 1-AND cell verified by boolean expression. The Mask bit can be the same or different. It is not necessarily a particular mask cell that works well for all four combinations of m_0m_1, mask

generator sets a particular mask bit for the selected mask cell.

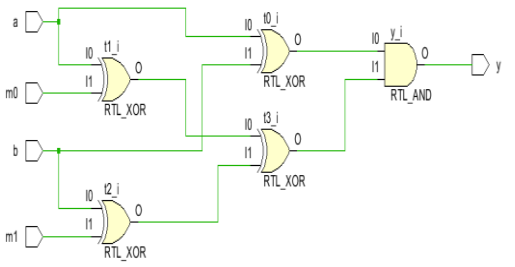

Fig. 3. Proposed mask XOR cell.

Masked XOR achieves the functionality for mask bits 00 and 11. Table 1 shows the truth table of mask XOR cell at the internal node (T0-T3). Equal distribution of HW on each internal node signifies that power is uniformly distributed to the internal node. XOR cell is preferred for uniform distribution of power pattern to each node.

Table 1. HW of Mask XOR with mask bits 00 and 11.

Input		Internal node and Output with mask bit m_0m_1 00					Internal node and Output with mask bit m_0m_1 11				
A	B	T0	T1	T2	T3	Y	T0	T1	T2	T3	Y
0	0	0	0	0	0	0	0	1	1	0	0
0	1	1	0	1	1	1	1	1	0	1	1
1	0	1	1	0	1	1	1	0	1	1	1
1	1	0	1	1	0	0	0	0	0	0	0
HW		2	2	2	2	2	2	2	2	2	2

3.2. Mask AND cell

Mask AND cell presented in Fig 4 is implemented with 5 XOR and 3 AND cell, and verified by boolean expression. Level 1 and level 2 include the XOR cell which is XORed with input with mask bit individually. Level 3 and final output cells compute the AND function by AND signal with their following. The truth table presented in Table 2 shows that the necessary mask bit should be by 00. The equal HW of each column signifies that power value is equal on the internal node, and does not lump on a single node. Invasive attack methods do not have access to the internal node and attackers cannot obtain power information to implement a power attack.

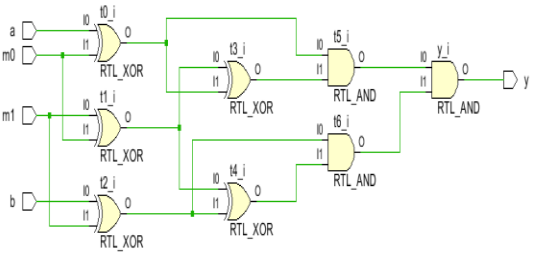

Fig. 4. Proposed mask AND cell.

Table 2. HW at the internal terminal of Mask AND.

Input		Internal node and Output with mask bit m_0m_1 00							
A	B	T0	T1	T2	T3	T4	T5	T6	Y
0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	1	0	1	0
1	0	1	0	0	1	0	1	0	0
1	1	1	0	1	1	1	1	1	1
HW		2	0	2	2	2	2	2	

4. SECURITY MEASURE OF MASK CELL

Mask cell enhances security level at the cost of increased cell count and power consumption [18-21]. The proposed two novel architectures of the mask XOR and mask AND cell, truth table approach verifies the distribution of logic level at the intermediate terminal. HW indicates that the amount of energy requires switching from level. In regular cells, a larger average energy gap is found between low of high and high to low transition (section II), while masked cell tries to achieve a difference of average energy as low as possible. Equation (5) presents the difference of energy to bring the output logic of the mask cell.

$$\text{Mask XOR } |E(y=1) - E(y=0) = 0.15fj| \\ \text{Mask AND } |E(y=1) - E(y=0) = 0.56\ fj| \quad (5)$$

Mask XOR and mask AND cell achieve a 15.49% and 33% reduction in switching energy respectively compared to the standard cell. Thus, it deduces that the proposed mask cells are strong candidates for attack countermeasures. Normalized energy deviation (NED) and moralized standard deviation (NSD) in equation (6) are two figures of merit to evaluate resistance to power attack [22, 23]. NED-NSD is the indirect measure of the resistance to a power attack; it indicates the ability of the logic cell against a power analysis attack. NED presents the percentage difference between the minimum and maximum energy difference for all possible transitions. The smaller value of NED presents a low variation in energy and the attacker requires more complex measurements to reverse engineering. NSD indicates the variation of consumed energy for each input pattern, calculated as (σ_E / e_{avg}) where σ_E is a

standard variation of energy. The largest value of NSD indicates that energy is widely spread across the mean and smaller value of NSD indicates that they are close to the mean. NED-NSD analysis is done at frequency of 1GHz, a smaller value of NED and NSD indicates a secure system, the attacker requires more complex measurement and resistance to power attack.

Table 3. Figure of merit mask cell

	Energy Parameter						
	E_{Min}	E_{Max}	NED	E_{Avg}	σ_E	NSD	Pearson Coefficient (ρ)
Standard XOR	0.06	2.52	0.9762	0.1538	1.5748	0.6402	0.134
Mask XOR (mask bit 00)	0.01	7.9	0.9987	0.4931	5.4026	0.6847	0.0053
Mask XOR (mask bit 11)	0.1	12.1	0.9917	0.75	7.984	0.6653	0.0239
Standard AND	0.004	2.17	0.9982	0.1354	1.2715	0.587	0.372
Mask AND (mask bit 00)	0.06	40	0.9985	2.4963	17.401	0.4357	0.3

$$NED = \frac{E_{\max} - E_{\min}}{E_{\min}} \quad NSD = \frac{\sigma_E}{E_{avg}}$$
$$\sigma_E = \sqrt{\sum_{i=1}^{n} \frac{(E_i - E_{avg})^2}{n}} \qquad (6)$$
$$E_{avg} = E_{\max} - E_{\min}$$

Where, E_{max} and E_{min} present maximum and minimum energy consumption respectively for all possible transitions. σ_E and E_{avg} are the standard deviation and average respectively calculated per complete cycle. Table 3 presents a comparative performance analysis of masked XOR-and cell compared to standard architecture with their mask bit. It is observed that the proposed masked XOR exhibits improvement in NED by 2.3% and 1.5% and improvement in NSD by 6.95% and 3.29% for mask bits 00 and 11. Whereas mask AND cells exhibit improvement in NED by 0.03% and improvement in NSD by 25.75% with mask bit 00 at an input frequency of 1GHz.

A statistical parameter, the Pearson correlation coefficient is used to measure the dependency of the dynamic component of power consumption with input data. A high value of correlation estimates larger dependency and vice versa. The last column of Table 3 lists the Correlation coefficient value of the standard and mask cells. The lower value of the correlation coefficient for mask cells exhibits power consumption patterns independent of the input pattern. Compared to standard cell mask XOR shows that mask AND cell achieve a reduction in person coefficient by 96.12% with mask bit 00, 82.16% with mask bit 11, and 19.35% with mask bit 00, respectively. Thus, cryptographic circuit implementation with a masked cell improves the algorithm's security level at the increased hardware cost. Implementation of the cryptographic unit with mask cell withstand better security standard but enhances the cell counts.

Optimization of the architecture results in a simple circuit. The presented mask XOR requires 5 cells and mask AND requires 8 cells which is much lower than the masking scheme presented in [24] 10 cells for mask XOR, in [25] 9 cells for mask AND.

5. CONCLUSION

This research investigates the architecture of a functional mechanism capable of power attack by obscuring logic cells. Mask cells try to distribute power information equally to internal terminals; therefore, attacks cannot obtain enough leakage information when observing only output nodes. Mask cells do require the additional component to randomize the signal but the difference in average energy require to compute high and low output levels reduces by 15.49% and 33.33% compared to normal XOR and AND gate, respectively. The Pearson correlation coefficient values of XOR masks are 96% lower and 19.35% of mask AND masks verify that power consumption patterns are weekly related to processed data. The cells presented can function as the basic blocks of cryptographic modules, which stand for an attack-resistant cell library

6. ACKNOWLEDGMENT

We are thankful to VLSI Lab, Lovely Professional University.

REFERENCES

[1] Popp, T., Mangard, S. and Oswald, E. "**Power analysis attacks and countermeasures**" *IEEE Design & test of Computers*, 24(6), pp.535-543, 2007.

[2] Kumar, A. and Tripathi, S.L., "**SBOX under PVT variation**." *Analog Integrated Circuits and Signal Processing*, 105(1), pp.73-82, 2020.

[3] Zhang, L., Vega, L. and Taylor, M., "**Power side channels in security ICs: hardware countermeasures**". *arXiv preprint arXiv*:1605.00681, 2016

[4] Sakamoto, J., Fujimoto, D. and Matsumoto, T., "**Laser-induced controllable instruction replacement fault**

attack" *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences*, 103(1), pp.11-20, 2020

[5] Huang, L., Jia, G., Fang, W., Chen, W. and Zhang, W, "**Towards Security Joint Trust and Game Theory for Maximizing Utility: Challenges and Countermeasures**" *Sensors*, 20(1), p.221., 2020

[6] Kumar, A., Tripathi, S.L. and Mishra, R.S. "**METAPUF: A challenge response pair generator**" *Periodicals of Engineering and Natural Sciences*, 6(2), pp.58-63, 2018

[7] Kumar, A., Mishra, R.S. and Kashwan, K.R., "**Challenge-response generation using RO-PUF with reduced hardware**" *In proceeding of International Conference on Advances in Computing, Communications and Informatics*, Jaipur, India, September 2016.

[8] Shamir, A., "**Protecting smart cards from passive power analysis with detached power supplies***" In proceeding of International Workshop on Cryptographic Hardware and Embedded Systems*, August 2000.

[9] Tiri, K. and Verbauwhede, I.,"**Securing encryption algorithms against DPA at the logic level: Next generation smart card technology***" In proceeding of International Workshop on Cryptographic Hardware and Embedded Systems*, September 2003.

[10] Tiri, K. and Verbauwhede, I., "**A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation**" *In Proceedings of Design, Automation and Test in Europe Conference and Exhibition*, Vol. 1, pp. 246-251, February 2004.

[11] Koc, L.K., "**Cryptographic Hardware and Embedded Systems-CHES**" *In Proceeding of 2nd International Workshop Worcester*, MA, USA, August 2000

[12] Mangard, S.,"**Hardware countermeasures against DPA–a statistical analysis of their effectiveness**" *In proceeding of Cryptographers' Track at the RSA Conference*, pp 222-235, February, 2004.

[13] Coron, J.S., "**Resistance against differential power analysis for elliptic curve cryptosystems***" In proceeding of International workshop on cryptographic hardware and embedded systems*, August 1999.

[14] Ishai, Y., Sahai, A. and Wagner, D. "**Private circuits: Securing hardware against probing attacks**" *In proceeding of Annual International Cryptology Conference*, August 2003.

[15] Peeters, E., Standaert, F.X. and Quisquater, J.J., "**Power and electromagnetic analysis: Improved model, consequences and comparisons**" *Integration*, 40(1), pp.52-60, 2007.

[16] Liu, J., Gu, D. and Guo, Z., "**Correlation power analysis against stream cipher mickey v2**" *In proceeding of International Conference on Computational Intelligence and Security*, December 2010.

[17] Zarrinchian, G. and Zamani, M.S., "**Combinational Counters: A Low Overhead Approach to Address DPA Attacks**" *Journal of Circuits, Systems and Computers*, 29(06), p.2050097, 2020

[18] Mamiya, H., Miyaji, A. and Morimoto, H., "**Efficient countermeasures against RPA, DPA, and SPA**" *In proceeding of International Workshop on Cryptographic Hardware and Embedded Systems* , August 2004.

[19] Zhang, Y., Wu, N., Zhou, F., Zhang, J. and Yahya, M.R. "**A Countermeasure against DPA on SIMON with an Area-Efficient Structure**" *Electronics*, 8(2), p.240, 2019.

[20] Yu, W. and Köse, S.,"**Exploiting voltage regulators to enhance various power attack countermeasures**" *IEEE Transactions on emerging topics in Computing*, 6(2), pp.244-257, 2016.

[21] Kumar, A., Tripathi, S. L., & Subramaniam, U.. **Variability Analysis of SBOX With CMOS 45 nm Technology**. *Wireless Personal Communications*, 124(1), 671-682, 2022

[22] Lama, S.,"**The Interrogation of Traumatic Brain Injury with MR Spectroscopy and Molecular Imaging**" *Doctoral dissertation, University of Calgary*, Canada, 2016

[23] Zhao, J., Mili, L. and Wang, M., "**A generalized false data injection attacks against power system nonlinear state estimator and countermeasures**" *IEEE Transactions on Power Systems*, 33(5), pp.4868-4877.

[24] Y. Zhou, G. Qian, Y. Xing, H. Liu, S. Goto, and Y. Tsunoo, "**An approach of using different positions of double registers to protect AES hardware structure from DPA**," *In proceeding of 3rd International Symposium on Electronic Commerce and Security*, pp. 223-227, 2010

[25] Zeng, Juanli, Yi Wang, Cheng Xu, and Renfa Li., "**Improvement on masked S-box hardware implementation,**" *In proceeding of International Conference on Innovations in Information Technology (IIT)* , pp. 113-116., 2012.