www.czasopisma.pan.pl PAN www.journals.pan.pl
POLSKA AKADEMIA NAUK
jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 4, PP. 749-754
Manuscript received November 8, 2021; revised November 2022. DOI: 10.24425/ijet.2022.143881

Lightweight PUF-Based Gate Replacement Technique to Reduce Leakage of Information through Power Profile Analysis

Mohankumar N., Jayakumar M., and Nirmala Devi M.

***Abstract*—The major challenge faced by electronic device designers is to defend the system from attackers and malicious modules called Hardware Trojans and to deliver a secured design. Although there are many cryptographic preventive measures in place adversaries find different ways to attack the device. Differential Power Analysis (DPA) attack is a type of Side Channel Attacks, used by an attacker to analyze the power leakage in the circuit, through which the functionality of the circuit is extracted. To overcome this, a lightweight approach is proposed in this paper using, Wave Dynamic Differential Logic (WDDL) technique, without incurring any additional resource cost and power. The primary objective of WDDL is to make the power consumption constant of an entire circuit by restricting the leakage power. The alternate strategy used by an adversary is to leak the information through reverse engineering. The proposed work avoids this by using a bit sequencer and a modified butterfly PUF based randomizing architecture. A modified version of butterfly PUF is also proposed in this paper, and from various qualitative tests performed it is evident that this PUF can prevent information leakage. This work is validated on ISCAS 85, ISCAS 89 benchmark circuits and the results obtained indicate that the difference in leakage power is found to be very marginal.**

***Keywords*—Design for Security; Hardware Security; PUF; TRNG; Wave Dynamic Differential Logic**

I. Introduction

DESIGNING a secured hardware to overcome the circuit vulnerabilities is a focal area of research in this decade. As the technology increasing in day-by-day, the usage of the ICs has been in-creased drastically. Due to the globalization of an IC, its design and fabrication is being exposed [1] [2]. Many third party companies will pirate the actual design of IC and reproduce the same with low cost. The attacks on the IC can be done at different stages of its fabrication. In order to protect the IC from malware attacks, there are certain countermeasures proposed. The countermeasures like watermarking, finger printing, obfuscation and metering are proposed [3]. Even though these countermeasures protect an IC from 3PIP attacks, there are other alternatives for an attacker to attack the design and manipulate its functionality.

The side channel attacks consist of different parameters like power leakage, delay, temperature analysis and timing analysis. The attacker can use the delay analysis in the circuit and extract the spots or the functionality where the delay is occurring [4]. Insertion of malware which changes the functionality of the circuit had been attempted. The attacker uses a technique called Differential Power Analysis (DPA) attack which analyzes the power leakage of a circuit and extract its functionality [5]. Wave Dynamic Differential Logic (WDDL) is used to protect the circuit from DPA. By employing the dual complementary gates of WDDL, one gate will provide the true output and the other complementary output. Thus the circuit by nullifying the effect of power leakage of a circuit, prevents the attacker knowing the functionality of it [5] [6]. The main aim of the proposed technique is to have constant power consumption throughout the operation of the circuit.

Along with the side channel attacks, data leakage is also a major issue [7]. The attacker can use a reverse engineering technique in order to analyze and study the circuit. The successful approach to protect the system is the use of Random Number Generators (RNG) to randomize the architecture of the circuit. In general, the dynamic and leakage power of the standard gates depend on the change in its signal activity i.e. the transition in input causes change in the static and dynamic power dissipation This is the main reason that the information can leak through the power analysis and the attacker will analyze the power dissipation of the entire circuit and extract the functionality of the circuit. In order to restrict this power analysis based information leakage a combination of Wave Dynamic Differential Logic (WDDL) and a modified version of butterfly PUF is proposed in this work.

Behnam Khaleghi et al [8] proposed a scheme to protect FPGA from hardware threats. A primitive FPGA protection scheme by filling the unused resources with a duplicate logic. Yier Jin proposed a method for protecting the internal information of the device. This work introduced the concept of security theorems which increases the security of the circuit [9]. A low-cost, reconfigurable NetFPGA hardware consisting of all the logical resources and memory required to construct a complete switch, router and other security system is used for high-speed networking. As it is entirely based on hardware, there are chances of attacking the hardware while implementation. Tushar Singh [10] proposed a cryptographic algorithm which encrypts the hardware at the time of implementation. Protecting a device from Side Channel Attacks is an important task. Differential Power Analysis attacks (DPA) depend upon the leakage of power analysis. Yuyu Zhang

Authors are with Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, INDIA (e-mail: {n_mohankumar, m_jayakumar, m_nirmala}@cb.amrita.edu).

proposed a novel design to secure the device from DPA attacks. Concentrating on cost and level of security, a design which combines Wave Dynamic Differential Logic (WDDL) and dynamic cryptosystem to secure the device is proposed [11], being a multi-level encryption design the procedure of implementing this system is complex.

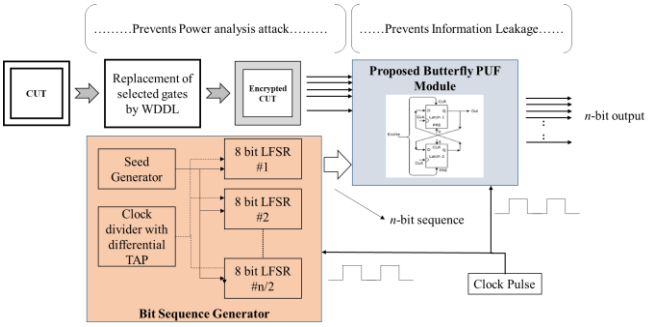

Fig. 1. Proposed two tier scheme based on WDDL and PUF

By performing Power analysis attacks, the secret key of a cryptographic device can be extracted by analyzing the variation in power signatures. A generic model of differential power analysis (DPA) is tested for attacks on static logic circuits. Massimo Alioto [11] provides an analysis that focuses on the vulnerability of cryptographic circuits. The different parameters of the DPA attacks are analyzed and an improvised result is proposed for the measurement of the DPA attacks. It examines certain methods for the power consumption measurements in order to find the rare occurring regions in a circuit. In order to restrict the DPA attacks, building of a strong cryptosystem has to be built for all the hardware devices. N. Avirneni proposed a novel counter-measure that uses reliable and aggressive designs to protect against side-channel analysis such as DPA and Correlation Power Analysis (CPA) attacks [12]. Though this approach consumes less area and power, implementing a Random dynamic voltage frequency scaling (RDVFS) will not prevent power attack due to the frequency-voltage one-to-one mapping. So the WDDL technique having similar characteristics of RDFS but having the capability of preventing power attack is chosen.

II. LITERATURE SURVEY

The design security is often thought of in terms of protecting Intellectual Property; however, potential losses extend beyond just the financial. With the increasing use of programmable logic beyond commercial markets to avionic, space and military applications, design security takes on the additional aspects of safety and national security. An attacker cannot derive these stable states from the bit stream since it does not contain these values.

A. PUF

When paired with the traits of unclonability, a different family of physical systems extract secrets from complicated physical aspects of integrated circuits, resulting in a highly safe approach of constructing volatile secret keys for cryptographic operations. [15]. The major advantage of using public-key based protocol is that it allows the design in which the private key is always stored in a FPGA. As PUFs implemented on FPGAs are intrinsic to the FPGAs, it provides better security. A PUF structure that is unusual in that it is built into FPGAs and hence does not require any changes to the hardware or manufacturing process. So the need for a modified an 8-bit Butterfly PUF for protecting the IP originates. Any architecture include and incorporates the butterfly PUF for providing keys to the security blocks, such as secure boot and remote attestation of the System on Chip (SoC).

As a result, the Butterfly circuit is an FPGA matrix version of a PUF circuit whose attributes are solely determined by the integrated circuit's intrinsic physical features and may be utilised for identification

A lightweight error correction code (ECC) encoder/decoder is employed in Paper [5] to extract reliable PUF bits from chip manufacturing differences. The security of the syndrome bits is based on a novel security argument that depends on what machine learning cannot learn. [6] only calls the PUF response once, after which it is hardened into a one-time programmable pad. When the scan chains are locked, rather than being read directly, the PUF response required by the designer to extract a test key for each crypto chip can only be recovered. The manufacturer can test the chip normally before the passed chips are locked, with no delay penalty. All bits within a single PUF response should be random and unpredictable, according to the study [7]. Entropy in the source is sufficient across devices. This means that each device is statistically distinct, and the chances of two devices having a PUF response that is "near" to each other are extremely unlikely. The study [8] begins with a summary of the different PUF models and their relevance, as well as the problems that come with them, and how Machine Learning-based modelling approaches are the most relevant for powerful PUFs, using Arbiters and variations as examples. The results of analyzing the Arbiters and PUF variations depending on parameters are examined. The powerful PUFs investigated are unsecure and can be made more secure by increasing their size. The possibilities of adding new design aspects to the standard model to enhance attacker complexity, as well as the future prospects of code breakers and code makers in the field of powerful PUFs and their resilience against known attacks, are also discussed.

Herder et.al, have presented a tutorial on ongoing work in security analysis, physical-disorder-based security, and the choice of implementation of the same. The paper motivates the use of Physical Unclonable functions against existing conventional non-volatile memories, in low-cost authentication (strong PUFs) and key generation applications (weak PUFs). The error correction schemes, like index-based coding and pattern matching are discussed concluding with emerging concepts such as public model PUFs and new PUF implementation technologies. U. Rührmair et.al, presented the necessity of PUFs in security protocols. In the paper they have classified attack models as stand-alone, bad and re-use are defined, compared and the security analyses of the same is carried out. While several models are certainly secure in their original attack models, a few of the others are not so for new or realistic scenarios[21]. The work done on strong PUFs thus needs to be strongly re-considered, through addition of features and making the whole of it erasable.

A lightweight hybrid PUF using Arbiter and Ring Oscillator for enhancing the security in IoTs is proposed by Sriram

Sankaran et. al. [19] The architecture evaluation shows that the the hybrid PUF is also power efficient.

III. PROPOSED POWER ANALYSIS BASED ATTACK PREVENTION TECHNIQUE

The requirement of a lightweight approach requires the use of WDDL gates, which are two positive complementary gates connected in parallel, one providing true output using true inputs and the other providing false output. Conventional AND logic and OR logic are common examples of positive logic gate. The key significance of the proposed approach is to maintain a near constant power consumption in a challenging functional operation conditions. Several strategies with WDDL were employed to avoid the security threat. Fig. 1 highlights the outline of the proposed scheme. By integrating the gate replacement technique by WDDL and PUF module is proposed in this paper. A quantifiable number of gates in the CUT are replaced by the WDDL gate replacement technique, this restricts the power analysis attack. The main aim of the gate replacement technique is to reduce the power signature variation across the entire CUT [13]. In addition, WDDL-based gate replacements are performed for selected very few gates based on node transitions, so there is only negligible overhead in terms of power consumption and area.

A. Proposed Information Leakage Prevention Technique

In order to prevent the information leakage, a LFSR based bit sequence generator module with an arbiter PUF is designed. The LFSR performance is based on the position of the tap-points and the linear combination logic used, while the seed generation module often changes the seed on a regular basis. Hence the sequence generated by the LFSR gains high periodicity, making the sequence unpredictable [14]. A series of 8-bit LFSR is used in the proposed design. The characteristic polynomial guiding the LFSR is different for the individual 8 bit LFSR modules used. The seed generator module using the metastability phenomena is used in the proposed seed generator module, this ensures easy design and achieves better randomness. The output temporarily latches to a metastable state when the input transits from ‘0’ to ‘1’ and then settles to either logic ‘0’ or ‘1’ state, whereas the output is stable when input is stable at logic ‘0’ or ‘1’. This phenomenon of metastability is exploited to generate the seed value of the proposed TRNG. Bit sequence generator and modified butterfly PUF module acts as a True random number generator.

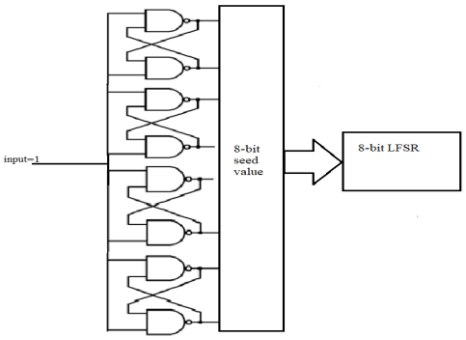

Fig. 2. LFSR 8-bit seed generator [15]

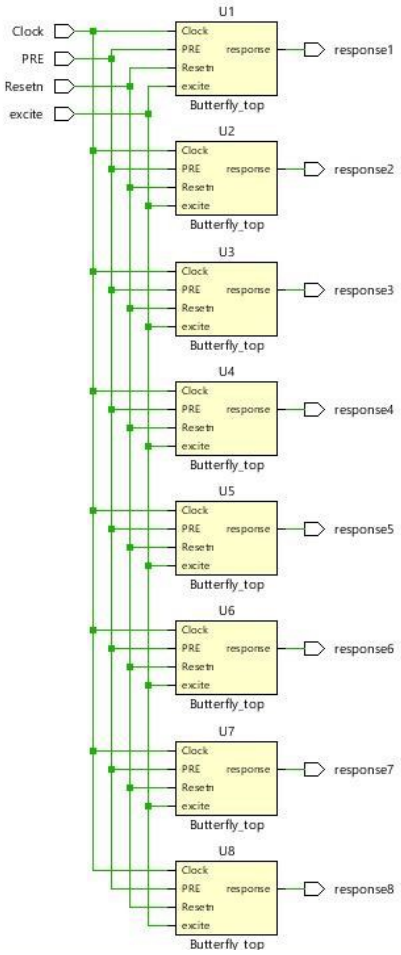

Fig. 3. RTL of the proposed modified butterfly PUF

B. WDDL based prevention for Power attacks

The proposed work mainly focuses on the effects of Side Channel Analysis. The work is concentrated on DPA and a methodology to overcome the difference in power signature by employing Wave Dynamic Differential Logic (WDDL). Even though the proposed technique in this paper overcomes the issue of power leakage, there is a possibility of leaking data from the circuit. One of the alternative method can use by an attacker is reverse engineering, through which the attacker can analyze the output of the circuit.

The DPA attacks are restricted through Wave Dynamic Differential Logic technique and in addition the PUF module is included in the design to secure the design from reverse engineering. The arbiter based PUF delivers two purposes, primarily it generates an unpredictable sequence and acts as an irreversible function due to the characteristics of PUF module [15] [17] . So an attacker is restricted from analyzing the circuit by reverse engineering the output. This combination of WDDL and PUF restricts the power attacks and provides high security for the data and reduces the information leakage through power analysis.

WDDL is tested on variation in power profile and area. From the analyzed results based on the power profile with ISCAS 85 and ISCAS 89 benchmark circuits , this combination of techniques proved to be successful methodology.

Inherent characteristics of butterfly PUF module is used to restrict the adversary from knowing the output logic function.

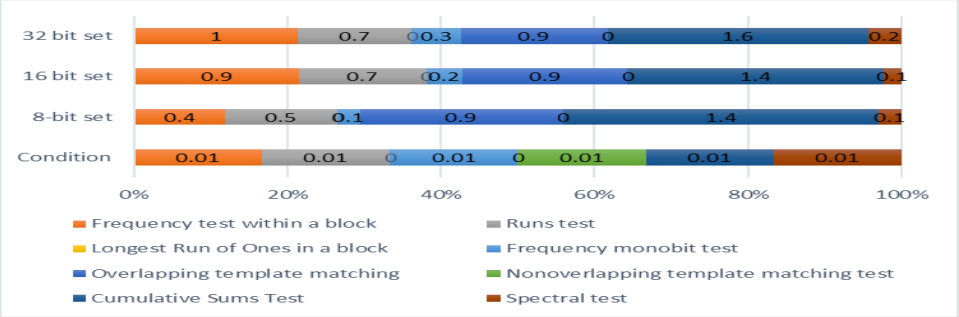

Fig. 4. NIST Test Results of PUF based TRNG

It's a cross-coupled bistable circuit that may be taken to an unstable state before settling into one of two potential stable states. For each set time interval, the PUF will provide a random output that will change [16]. The behavior of the circuit is concealed using PUF, which prevents the attacker from using the reverse engineering approach.

IV. RESULTS AND DISCUSSION

PUF based TRNG is modeled for three bit lengths namely 8, 16 and 32 bits. The randomness of the sequence generated by the PUF based TRNG is validated using a set of standard NIST tests. Initially 8, 16 and 32 bit PUF based TRNG configurations are allowed to generate 1000 sequences and four such trials are used to generate the sequences in each case. Upon testing every sequence for randomness in the generated sequences, it was found that almost 7 tests out of 8 prove that the sequences are random. Hence the TRNG module will switch the arbiter block of the PUF module with high randomness. This action will make the PUF module robust and prevent the design from being reversed engineered. The average of the individual test results are shown in Fig.3. which highlights that the NIST tests namely Spectral test, cumulative sums test, overlapping template matching test, runs test, frequency test within a block and frequency monobit test was over the threshold mark of the respective tests [20]. So the test results prove Initially, WDDL is applied over the gate level Circuit Under Test (CUT). WDDL is a technique of replacement of the gate functionality with additional gates. The input logic and the logic switching relates to the static and dynamic power dissipation. With the replacement of one gate with additional gates, the power consumption will be different. This technique hides the actual power consumption of the circuit and restricts the attacker to analyze the power leakage from that the sequences generated by the proposed TRNG is completely random.

Total power consumption and area are compared for 8, 16 and 32 bit conventional and PUF based TRNG as shown in Fig. 4. It is observed that the TRNG module is efficient in terms of power, since the power consumption is found to be very nominal when compared with a conventional TRNG. It is observed from Fig. 4 that the difference shows, the increase in total power consumption is not increasing exponentially with increase in number of bits and hence it is much suitable in terms of power consumption.

This is achieved without using power reduction techniques like TBHEX Architecture or gating. The area occupied by the TRNGs appears to be ineffective but the variation trend shows The WDDL technique is applied to both combination and sequential benchmark circuits (ISCAS '85 and ISCAS '89).The main aim of implementing the WDDL logic is to restrict the power leakage of the circuit and restrict the attacker to analyze the functionality of the circuit through DPA attacks that this TRNG is suitable for larger subsystems as the area occupied is less.

A. Uniqueness validation

The uniqueness is calculated over boards and compared using the response generated in nominal environmental condition. It is formulated with average inter-chip Hamming Distance distribution, which provides the idea of how unique response bits are generated on different FPGA chips. As stated response bits generated from same FPGA are compared to each other to state how unique they are from each other. It states that responses generated from same FPGA are not monotonous if so they are prone to ML attacks.

With the maximum likelihood, uniqueness in the range 45-50 percent happens, which is very near to the ideal PUF behavior. Furthermore, the average uniqueness value achieved is 49.99 percent, with a standard deviation of 13.27, which is close to the desired uniqueness value of 50%.

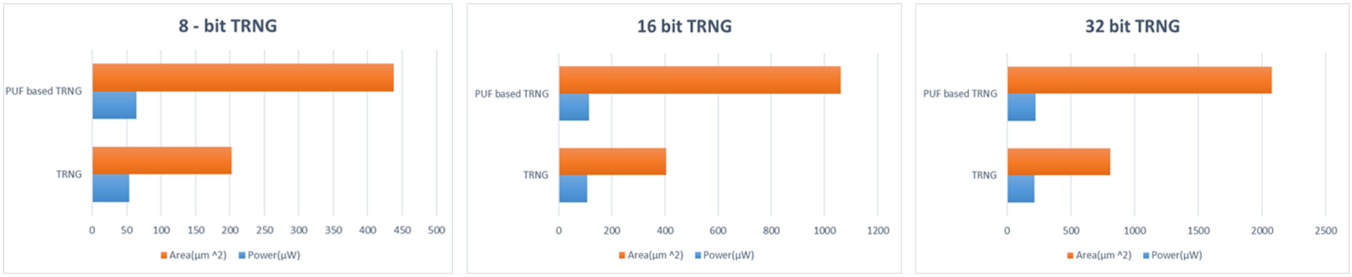

Fig. 5. Power and Area comparison between conventional and PUF based TRNG

TABLE I
POWER AND AREA COMPARISON OF ISCAS 85 AND WDDL CIRCUIT

CUT	Normal Circuit		WDDL Circuit		% decrease in power leakage	% increase in area
	Leakage Power (nW)	Area (mm^2)	Leakage Power (nW)	Area (mm^2)		
c17	3.115	27.69	2.92	50.15	6.6	44.8
c432	0.883	819.71	0.754	1382.3	17	40.7
c499	2.61	1868.2	2.42	2153.2	7.85	13.2
c880	1.92	1538.2	1.75	1823.1	9.71	15.6
c1355	2.9	2195.4	2.62	3296.3	12.1	33.4
c1908	2.54	3265.2	2.5	4596.4	1.66	29.0
c2670	3.65	4853.4	3.5	5239.2	4.2	7.4
c3540	4.98	5961.2	4.8	6752.4	3.7	11.7
c5315	6.15	7236.2	5.92	8632.1	3.88	16.2
c7552	9.32	9156.3	9.12	10258	2.1	10.7

TABLE II
POWER COMPARISON OF ISCAS 89 CIRCUITS AND WDDL CIRCUITS

CUT	Leakage Power (nW)		% decrease in leakage power
	Normal Circuit	WDDL Circuit	
s27	3.11	2.98	2.11
s298	5.23	5.02	4.23
s400	2.61	2.45	1.61
s420	2.9	2.72	1.9
s510	5.92	5.86	4.92

The responses from one FPGA are compared to other respective responses from different FPGA boards for uniqueness. Figure 6a shows the histogram comparing intra-chip uniqueness between three FPGA boards and figure 6b shows the plot comparing inter- chip uniqueness of APUF, ROPUF, and the proposed PUF. It can be seen that the distribution is close to 50% for the proposed PUF depicting unique CRPs. It is clear that when Butterfly PUF responses are passed through the proposed scheme there is a huge increase in the uniqueness of the response bits.

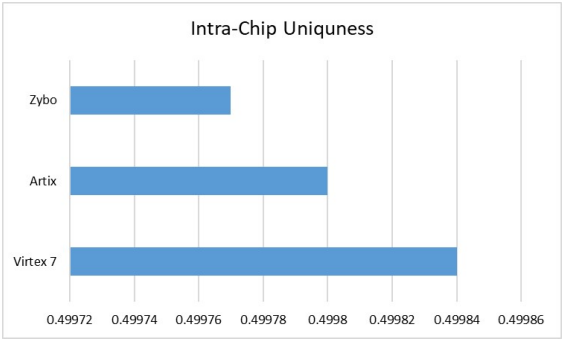

Fig. 6a. Intra chip uniqueness in different FPGAs

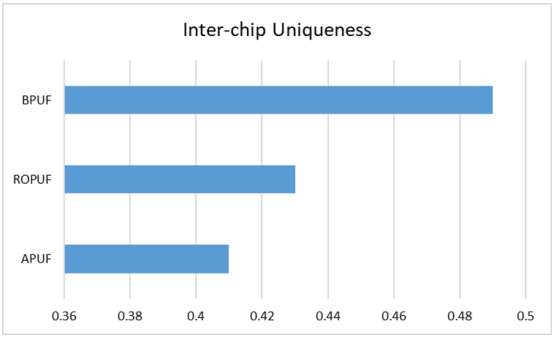

Fig. 6b. Inter-chip uniqueness of different PUFs

The responses from one FPGA are compared to other respective responses from different FPGA boards for uniqueness. Figure 7.1 shows the histogram comparing intra-chip uniqueness between three FPGA boards and figure 7.2 shows the plot comparing inter- chip uniqueness of APUF, ROPUF, and the proposed PUF. It can be seen that the distribution is close to 50% for the proposed PUF depicting unique CRPs. It is clear that when Butterfly PUF responses are passed through the proposed scheme there is a huge increase in the uniqueness of the response bits.

B. Uniformity validation

For the PUF's security, uniformity is an important quality metric. This measure determines how evenly the proportion of "0s" and "1s" in a PUF's response bits is distributed [22]. This percentage must be 50% for fully random PUF replies. By this equation, uniformity of an n-bit PUF identifier is defined as the percentage Hamming Weight (HW) of the n-bit identifier.

$$Uniformity = \frac{1}{n}\sum_{l=1}^{n} r_{i,l}\ X\ 100\%$$

Where r i, l is the l−th binary bit of an n−bit response from a chip i. Uniformity is 49.77 percent on average, with a low of 10.54 percent and a maximum of 90.17 percent, respectively.

As mentioned by Krzysztof Szczypiorski, "Industry 4.0: age of human-machine barrier disappearance, cyberspace appears in the so-called age of computers, where mass production is supported by machines."[22]. Hence the cyber-physical-systems fabricated as ICs yielded through mass production are vulnerable to security threats, further when security is inbuilt through the design process enhances the reliability of the mass production.

V. CONCLUSION

This paper proposed a WDDL based gate replacement technique combined with PUF TRNG technique. The main objective of this design is to protect the circuit from side channel analyzes and data leakage as well. The strategy suggested to minimize the leakage of the data is PUF. The architecture of 8, 16 and 32-bit PUF based TRNG is compared to various parameters such as area and total power, which proves the proposed technique consumes less power. The increase in area occupied by the circuit is also of negligible quantity for larger circuits and hence suitable for securing the CUT. The architecture is also modest and incorporating them for the security of CUT is also simple. On an average the leakage power reduces by 6.88% in combinational benchmark and 3% in sequential benchmark circuits. The proposed structure consumes extremely low power and thus effective compared to other techniques which employ larger blocks to incorporate security feature into it. The proposed TRNG based on PUF produces a high periodicity random sequence output, which is validated by the eight standard NIST tests. . This PUF-based TRNG configuration is especially reasonable for cryptographic and security based hardware applications, because of its power efficiency.

REFERENCES

[1] Swarup Bhunia., Michael S. Hsiao., Mainak Banga., Seetharam Narasimhan. (2014.): Hardware Trojan Attacks: Threat Analysis and Countermeasures. In: Proceedings of IEEE, Vol.102, No.8. https://doi.org/10.1109/JPROC.2014.2334493

[2] Masoud Rostami., Farinaz Koushanfar., and Ramesh Karri.(2014.): A Primer on Hardware Security: Models,Methods, and Metrics. In: Proceedings of IEEE, Vol.102, No.8. https://doi.org/10.1109/JPROC.2014.2335155

[3] Seetharam Narasimhan., Rajat Subhra Chakraborty., Swarup Chakraborty.(2012) Hardware IP Protection During Evaluation Using Embedded Sequential Trojan. In: IEEE Design and Test of Computers, Vol.29, pp. 70-79. https://doi.org/10.1109/MDT.2012.2205997

[4] Yier Jin., Nathan Kupp., and Yiorgos Makris.(2009) Experiences in Hardware Trojan Design and Implementation. In: IEEE International Workshop On Hardware-Oriented Security and Trust, pp 50-57. https://doi.org/10.1109/HST.2009.5224971

[5] Yuyu Zhang., Guoxi Wang., Yufeng Ma., Jingwen Li. (2011) A Comprehensive Design Method Based on WDDL and Dynamic Cryptosystem to Resist DPA Attack. In: International Conference on Intelligence Science and Information Engineering, pg. 333-336. https://doi.org/10.1109/ISIE.2011.145

[6] Nianhao Zhu., Yujie Zhou., and Hongming Liu.(2015) A Novel Way to Implement WDDL Logic to Resist Power Analysis Attack in Algorithm Level. In: Applied Mathematics and Information Sciences, Vol.9, No. 1, pg. 269-280. https://doi.org/10.12785/amis/010133

[7] Zhimin Chen., Ambuj Sinha., and Patrick Schaumont.(2013) Using Virtual Secure Circuit to Protect Embedded Software from Side-Channel Attacks. In: IEEE Transactions on Computers, Vol. 62, No. 1. https://doi.org/10.1109/TC.2011.225

[8] Behnam Khaleghi., Ali Ahari., Hossein Asadi., and Siavash Bayat-Sarmadi.(2015) FPGA-Based Protection Scheme against Hardware Trojan Horse Insertion Using Dummy Logic. In: IEEE Embedded Systems Letters, Vol. 7, No. 2. https://doi.org/10.1109/LES.2015.2406791

[9] Yier Jin., Xiaolong Guo., Raj Gautam Dutta., Mohammad-Mahdi Bidmeshki., Yiorgos Makris (2017) Data Secrecy Protection Through Information Flow Tracking in Proof-Carrying Hardware IP Part I: Framework Fundamentals. In: IEEE Transactions on Information Forensics and Security, Vol. 12, No. 10. https://doi.org/10.1109/TIFS.2017.2707323

[10] Tushar Singh Chouhan (2015) Implementation of PRESENT Cryptographical Algorithm for the Encryption of Messages in NETFPGA. In: International Conference on Computational Intelligence and Communication Networks, pg. 1115-1119. https://doi.org/10.1109/CICN.2015.219

[11] Massimo Alioto., Massimo Poli., and Santina Rocch (2010) A General Power Model of Differential Power Analysis Attacks to Static Logic Circuits. In: IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 18, No. 5. https://doi.org/10.1109/TVLSI.2009.2015327

[12] N. Avirneni., and A. Somani (2013) Countering Power Analysis Attacks using Reliable and Aggressive Designs. In: IEEE Transactions on Computers, pg. 1-10. https://doi.org/10.1109/TC.2013.9

[13] Xiaoming Chen., Qiaoyi Liu., Yu Wang., Qiang Xu., and Huazhong Yang (2017) Low-Overhead Implementation of Logic Encryption Using Gate Replacement Techniques. In: 18th International Symposium on Quality Electronic Design (ISQED), pg. 257-263. https://doi.org/10.1109/ISQED.2017.7918325

[14] Shiva Prasad R, Anirudh Siripagada., Santthosh Selvaraj., Mohankumar N(2018) “Random Seeding LFSR based TRNG for Hardware Security Applications” In: Second International Conference on Integrated Intelligent Computing, Communication and Security(ICIIC). https://doi.org/10.1007/978-981-10-8797-4-44

[15] Ali Sadr., Mostafa Zolfaghari-Nejad (2012) Physical Unclonable Function (PUF) Based Random Number Generator. In: Advanced Computing: An International Journal (ACIJ), Vol.3, No.2.

[16] Abhranil Maiti., Raghunandan Nagesh., Anand Reddy., Patrick Schaumont(2009) Physical Unclonable Function and True Random Number Generator: a Compact and Scalable implementation. In: the 19th ACM Great Lakes symposium on VLSI. https://doi.org/10.1145/1531542.1531639

[17] Kumar, A.V., Bharathi, S., Meghana, C., Anusha, K., & Priyatharishini, M. (2019). Toggle Count Based Logic Obfuscation. 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), 809-814. https://doi.org/10.1109/ICECA.2019.8821935

[18] V. A. Deepak, M. Priyatharishini, M. Nirmala Devi (2019)", Design Protection Using Logic Encryption and Scan-Chain Obfuscation Techniques", International Journal of Electronics and Telecommunications, Volume 65, Issue 3, Pages 389 – 396. https://doi.org/10.24425/ijet.2019.129790

[19] S. Sankaran, S. Shivshankar and K. Nimmy,(2018),"LHPUF: Lightweight Hybrid PUF for Enhanced Security in Internet of Things," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 275-278, https://doi.org/10.1109/iSES.2018.00066

[20] A. Cui, C. H. Chang, W. Zhou and Y. Zheng, (2021), "A New PUF Based Lock and Key Solution for Secure In-field Testing of Cryptographic Chips," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 2, pp. 1095-1105, https://doi.org/10.1109/TETC.2019.2903387

[21] U. Rührmair and M. van Dijk, (2013), "PUFs in Security Protocols: Attack Models and Security Evaluations," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, pp. 286-300, https://doi.org/10.1109/SP.2013.27

[22] Krzysztof Szczypiorski (2020) "Cyber(in)security", International Journal of Electronics and Telecommunications, Volume 66, Issue 1, Pages 243-248. https://doi.org/10.24425/ijet.2020.131870