Energy-Efficient Power Analysis Attack Resilient Adiabatic MTJ-based Nonvolatile CLB

Milad Tanavardi Nasab
Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville
Knoxville, USA
mtanavar@vols.utk.edu

Wu Yang
Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville
Knoxville, USA
wyang19@vols.utk.edu

Himanshu Thapliyal
Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville
Knoxville, USA
hthapliyal@utk.edu

***Abstract*— Energy efficiency and security against side-channel attacks (like power analysis attacks) in modern and battery-operated applications like IoT and medical applications are vital. On the other hand, FPGAs are widely used as a hardware platform for these applications. Accordingly, energy-efficient and power analysis attack-resilient design for FPGA is required. This paper proposes an energy-efficient power analysis attack-resilient adiabatic nonvolatile hybrid MTJ/CMOS LiM-based CLB. The simulation results show that the proposed design has 98.72%, 98.72%, 98.69%, 98.61%, 98.43%, and 98.11% (at least 84.69%, 84.74%, 84.28%, 83.19%, 80.70%, and 77%) lower energy consumption compared to its CMOS counterpart (adiabatic counterparts) for frequencies of 1, 2.5, 5, 10, 20, and 40 MHz, respectively. Also, the proposed design keeps its energy consumption superiority for different TMR and power supply voltages, compared to its counterparts. The NED and NSD values of different designs have been calculated and used as power analysis attack-resiliency metrics. The results show that the proposed design has 1053x and 1628x (at least 23x and 14x) lower NED and NSD values compared to its CMOS counterpart (adiabatic counterparts). Furthermore, the NED and NSD values of the proposed design stay in the same range (10^{-4}) for different frequencies, power supply voltages, and TMR.**

Keywords—— Configurable Logic Block, Adiabatic Secure FPGA, Magnetic Tunnel Junction, Power Analysis Attack, Spintronic.

I. INTRODUCTION

Although application-specific integrated circuits (ASIC) provide lower delay and energy consumption compared to general-purpose CPUs, the high design-to-market time and design-and-manufacturing costs make ASIC designs inefficient for many applications. On the other hand, FPGAs provide lower energy consumption and delay compared to general-purpose CPUs (but not as good as ASIC designs) alongside fast design-to-market and low implementation costs. Furthermore, the infinite reconfigurability of FPGAs makes them the best option for hardware implementation in many applications [1-3].

Many modern applications like IoT, medical devices, and other battery-operated devices have limited power resources. Also, the security of these devices is of great importance. Accordingly, secure and low-energy hardware designs for these applications have attracted much attention in recent years. Although FPGAs have lower energy consumption compared to general-purpose CPUs, the power resources of modern devices may not be able to supply the energy demand of FPGAs. Using separate volatile SRAM cells alongside CMOS-based LUTs leads to high energy consumption [4-7]. In addition, SRAM-based FPGAs are vulnerable to side-channel attacks like power analysis attacks (the most common side-channel attack). Accordingly, designers must use different techniques to securely implement their design on the FPGAs. In addition to the complexity of implementing these techniques, using these techniques significantly increases the area overhead and energy consumption. Accordingly, designing low-energy and power attack-resilience-in-nature FPGAs is of great importance [8-10].

Non-volatile devices like magnetic tunnel junctions (MTJ) can be used to design non-volatile FPGAs. By utilizing MTJ devices in designing non-volatile FPGAs, unlike SRAM-based FPGAs, the configuration of the FPGA will be stored permanently, and it will not be lost after each power down. In addition to eliminating the need for external memory, permanently storing the configuration will lead to lower energy consumption, since reconfiguring the FPGA after each power down is energy-consuming. Furthermore, using MTJ devices paves the road to using novel architecture like logic-in-memory (LiM). The memory cells and look-up tables (LUTs) can be combined using LiM architecture, significantly reducing the area and energy overhead. It is noteworthy that although the SRAM cells are distributed throughout the SRAM-based FPGAs, they are used as separate circuits from the LUT circuits which leads to higher area and energy overhead [1, 3, 5, 7].

Another technique that can be utilized to reduce energy consumption is using the adiabatic-based design. Adiabatic-based circuits reduce energy consumption by recovering the stored charge in the capacitive load into the power supply using gradual charging and discharging. Adiabatic-based designs achieve optimal energy consumption in relatively lower frequencies, which makes them a promising candidate for energy-efficient hardware implementation in modern applications like IoT devices since the target applications usually work in low frequencies [11, 12].

An adiabatic- CMOS-based LUT and three different adiabatic memories have been previously proposed by the authors in [13] to implement a configurable logic block (CLB). Although the proposed designs show significant energy savings compared to their CMOS counterparts, using separate circuits for memory and LUT, and volatile memories keeps the energy consumption relatively high. In addition, the resistance against the power analysis attack of the proposed design in [13] has not been explored.

This work was supported in part by the National Science Foundation CAREER Award under Grant 2232235.

(Corresponding Author: Himanshu Thapliyal)

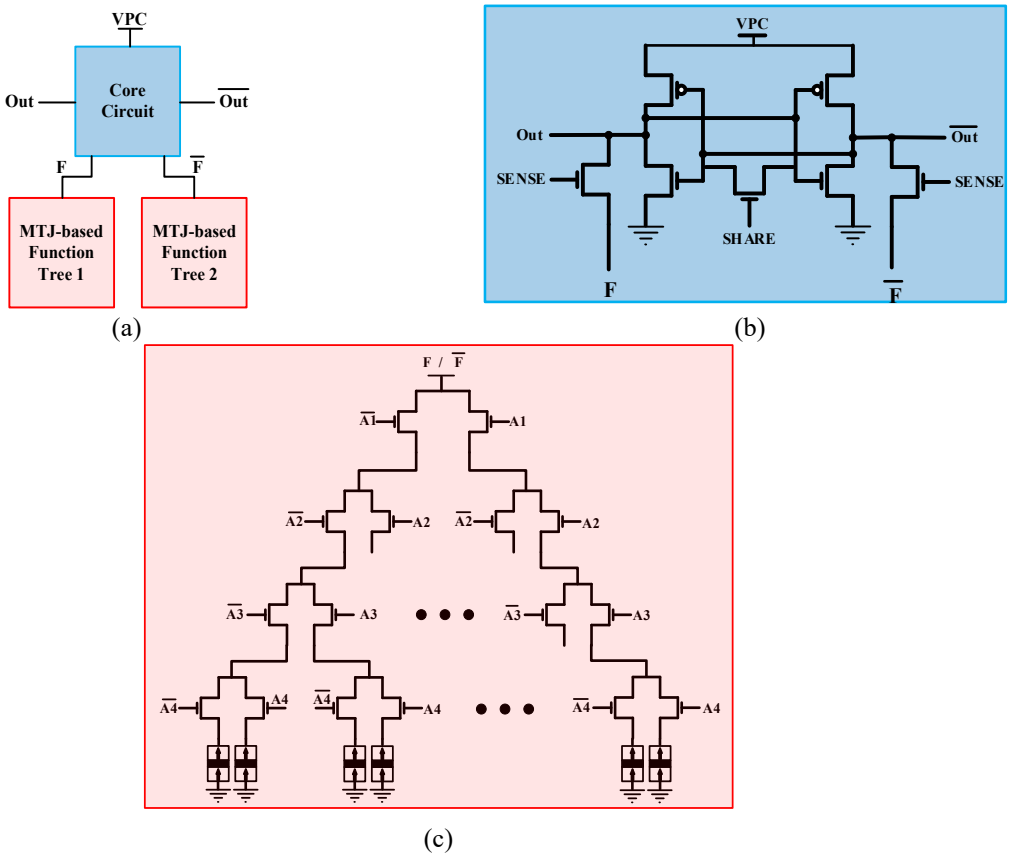

Fig. 1. Proposed design a) Block diagram b) Core circuit schematic c) MTJ-based function tree schematic.

In this paper, an energy-efficient power analysis attack-resilient adiabatic MTJ-based nonvolatile CLB has been proposed. The proposed design utilized the MTJ in a LiM architecture to combine the memory cells and LUTs, in order to reduce the area and energy overhead and eliminate the need for external memory. Also, the dynamic energy consumption of the proposed design is reduced by using adiabatic logic. Furthermore, the proposed design is secure against power analysis attacks. Accordingly, the proposed design can be utilized to design a power analysis attack-resilient non-volatile FPGA, which can provide a secure platform for secure hardware implementation of modern applications like IoT and medical devices.

The rest of the paper is organized as follows: a brief background for MTJ devices and adiabatic logic is presented in Section II. The proposed design is described in Section III. Performance parameters and simulation results of the proposed design and its counterparts are presented in Section IV. In Section V the resiliency of the proposed design and its counterparts against power analysis attacks has been investigated. Finally, Section VI concludes the paper.

II. Background

A. Magnetic Tunnel Junction

MTJ is a non-volatile spintronic device which has two states. The state of the MTJ is dependent on the magnetic direction of its two ferromagnetic layers which are separated by a thin oxide layer. If the magnetic direction of these two ferromagnetic layers is the same as each other, the MTJ is in a parallel state and shows relatively lower resistance (R_P) and if the magnetic directions of these two layers are opposite of each other, the MTJ is in an antiparallel state and shows relatively higher resistance (R_{AP}). It is noteworthy that the magnetic direction of one of these ferromagnetic layers is fixed (fixed layer) and the magnetic direction of the other layer is changeable (free layer). Higher differences between the resistance of MTJ devices in different states lead to higher reliability of MTJ-based circuits. Consequently, the tunnel magnetoresistance ratio (TMR) is used as a parameter showing this difference [14-19]. The TMR is calculated using Eq. 1.

$$TMR = \frac{R_{AP} - R_P}{R_P} \quad (1)$$

B. Adiabatic Logic

A gradually rising and falling signal is used as the power clock signal in designing adiabatic-based circuits, in order to minimize energy consumption. By using the power clock signal, the stored charge in the capacitive load will be recovered into the power supply and non-adiabatic energy dissipation will be minimized. For ideal adiabatic switching a constant current supply is needed [20-22]. In this case, energy dissipation is calculated using Eq. 2. Also, the energy dissipation of charging capacitance C to the voltage of V_{DD} is calculated using Eq. 3.

$$E_{Adiabatic} = \frac{RC}{T} CV_{DD}^2 \quad (2)$$

$$E_C = \frac{1}{2} CV_{DD}^2 \quad (3)$$

TABLE I. CRITICAL PARAMETERS OF CMOS TRANSISTORS AND MTJS

Description	Value
NMOS	
Gate length	60nm
Gate width	200nm
Number of fingers	1
PMOS	
Gate length	60nm
Gate width	400nm
Number of fingers	1
MTJ	
MTJ surface	60nm×60nm
Oxide barrier thickness	0.85nm
Free layer thickness	2nm
TMR	3
Resistance area product	10^{-11}

TABLE II. REFERRING TO THE NAMES OF THE COUNTERPARTS PROPOSED IN [13]

Referring name	Design
CMOS DESIGN	CMOS LUT with CMOS SRAM
CP1	Adiabatic LUT with 14T adiabatic memory
CP2	Adiabatic LUT with 16T adiabatic memory
CP3	Adiabatic LUT with 12T adiabatic memory

TABLE III. ENERGY CONSUMPTION (FJ/CYCLE) OF DIFFERENT CLBS

Frequency (MHz)	CMOS Design	CP1	CP2	CP3	Proposed Design
1	632.1	53.03	62.65	54.71	8.117
2.5	259.6	21.85	25.61	22.39	3.334
5	135.6	11.34	13.31	11.63	1.783
10	73.59	6.092	7.204	6.279	1.024
20	42.53	3.541	4.153	3.597	0.666
40	26.65	2.196	2.733	2.331	0.505

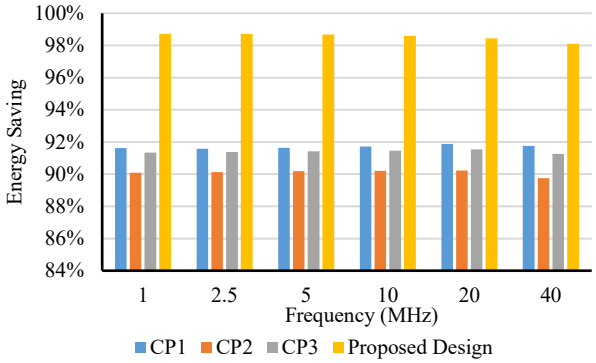

Fig. 2. Energy saving of the proposed design and its adiabatic counterparts compare to their CMOS counterpart for different frequencies.

Where R is resistance, C is the capacitance of the capacitive load, T is the charging/discharging time of the capacitive load, and V_{DD} is the full-swing voltage of the power clock or constant voltage power supply. By comparing Eq. 2. and Eq.3. in case that T is greater than $2RC$, the energy dissipation of the adiabatic-based circuits will be lower than CMOS circuits which makes the adiabatic-based circuits a promising energy-efficient candidate for low-frequency applications such as IoT devices.

III. PROPOSED DESIGN

Figure 1 shows the proposed two-phase energy-efficient power analysis attack-resilient adiabatic MTJ-based nonvolatile CLB. The proposed design consists of two parts: The Core Circuit (Fig. 1. b) and MTJ-based Function Trees (Fig. 1. c).

In the Function Trees, two MTJ/CMOS-based networks are used. The selector signals are used to select the corresponding MTJs in Function Trees 1 and 2. Except for the state of the corresponding MTJs in Tree 1 and Tree 2, which are complementary to each other, these two Function Trees are similar. Therefore, two MTJs with complementary states are used for storing each bit of configuration. The difference between the states of the corresponding MTJs in Function Trees leads to a difference between the path resistance of the corresponding top node of the Function Trees to the ground. The difference between the path resistances is captured by the Core Circuit. The Core Circuit consists of two back-to-back inverters connecting to the ground and VPC, two NMOS transistors connecting nodes Out and $\overline{Out}$ to nodes F and $\bar{F}$ and controlled by the SENSE signal, and an NMOS transistor connecting the node Out to node $\overline{Out}$.

The proposed design works in two phases: the evaluation phase and the recovery phase. In the evaluation phase, the VPC rises from the ground toward full swing voltage (VDD). At the beginning of this phase, the SENSE signal is set to VDD. Consequently, the voltages of nodes Out and $\overline{Out}$ follow VPC, but since they have different path resistance to the ground (through the Function Trees) the voltage of one of these nodes will be slightly higher than the other node. When the difference between the voltages of nodes Out and $\overline{Out}$ reach a sufficient amount that can latch the output on the back-to-back inverter, the SENSE signal will be reset to '0', and consequently one of the output nodes will continue following VPC and the other one will have a logical value of '0'. In the recovery phase, VPC gradually falls from VDD to the ground and recovers the stored charge in the capacitive load. Before completely recovering the stored charge in the nodes Out or $\overline{Out}$ the PMOS transistors will be turned off and a residual charge will remain in one of the nodes Out or $\overline{Out}$. This residual charge can be used to leak information. To prevent information leakage, an NMOS transistor controlled by the SHARE signal is used to share the charge between the nodes Out and $\overline{Out}$ before the next evaluation phase starts, consequently, the power trace of the proposed design for different sequences of inputs becomes identical and independent of inputs or their sequences.

IV. SIMULATION RESULTS

Comprehensive performance investigation and comparison of the proposed two-phase energy-efficient power analysis attack-resilient adiabatic MTJ-based nonvolatile CLB and its state-of-the-art counterparts are presented in this section. Spice simulations have been performed in Cadence Spectre. Also, the TSMC 65nm CMOS PDK and MTJ model presented in [23-25] have been used to create schematic entries and Spice simulations. The values in Table I are used as the parameters in the simulations, unless for investigating the effects of the parameter in which case it is mentioned in related sections. Table II shows the names that are used to refer to counterparts.

A. Frequency Sweep

The performance and energy saving of adiabatic-based circuits depends on the frequency at which the circuit is operating. Accordingly, the energy consumption of the proposed design and its counterparts have been calculated and reported in Table III.

TABLE IV. ENERGY CONSUMPTION (FJ/CYCLE) OF THE PROPOSED 16:1 CLB AND ITS COUNTERPARTS FOR DIFFERENT SUPPLY VOLTAGES

Supply voltage	CMOS Design	CP1	CP2	CP3	Proposed Design
1.2	73.6	6.09	7.20	6.28	1.02
1.1	50.6	4.46	5.16	4.50	0.811
1	34.4	3.23	3.66	3.19	0.640
0.9	23.1	2.33	2.59	2.26	0.520

TABLE V. ENERGY CONSUMPTION (FJ/CYCLE) OF THE PROPOSED 16:1 CLB AT DIFFERENT FREQUENCIES USING DIFFERENT TMR VALUES

Frequency (MHz)	TMR= 1	TMR= 1.5	TMR= 2	TMR= 2.5	TMR= 3
1	8.179	8.165	8.134	8.118	8.117
2.5	3.383	3.366	3.358	3.345	3.334
5	1.834	1.817	1.806	1.793	1.783
10	1.071	1.058	1.043	1.034	1.024
20	0.7115	0.6940	0.6795	0.6705	0.666
40	0.5518	0.5293	0.5148	0.5135	0.5053

TABLE VI. TRANSISTOR COUNT OF 16:1 CLB

CLB	CMOS design	CP1	CP2	CP3	Proposed design
Transistor count	402	324	292	260	67

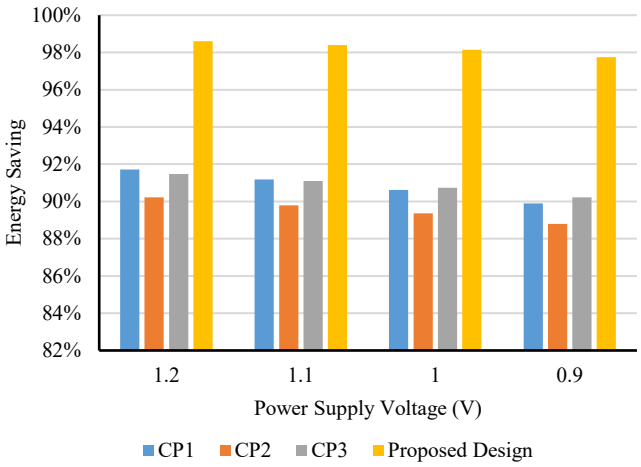

Fig. 3. Energy saving of the proposed design and its adiabatic counterparts compare to their CMOS counterpart for different supply voltages.

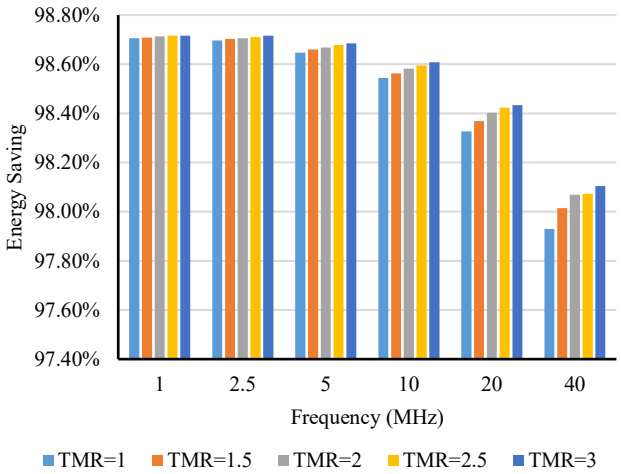

Fig. 4. Energy saving of the proposed design compared to its CMOS counterpart for different TMRs.

The results in Table III show that the proposed design not only has significantly lower energy consumption compared to its CMOS counterpart but also has significant energy savings compared to its adiabatic-based counterparts, which is mainly due to combining memory cells and LUTs in the proposed design and using LiM architecture. The results show the proposed design has 98.72%, 98.72%, 98.69%, 98.61%, 98.43%, and 98.11% lower energy consumption compared to its CMOS counterpart for frequencies of 1, 2.5, 5, 10, 20, and 40 MHz, respectively. Also, for these frequencies, the proposed design has at least 84.69%, 84.74%, 84.28%, 83.19%, 80.70%, and 77% lower energy consumption. Figure 2 shows the energy savings of the proposed design and its adiabatic counterparts for different frequencies, compared to their CMOS counterpart.

B. Power Supply Voltage Sweep

In order to investigate the effects of power supply voltage on the energy consumption of the proposed design and its counterparts, they have been simulated using different power supply voltages, using TMR=3 and at the frequency of 10 MHz. The results are shown in Table IV. Also, the energy savings of the proposed design and its adiabatic counterparts compared to their CMOS counterpart are shown in Fig. 3. The energy savings of the proposed design compared to its CMOS counterpart for power supply voltages of 1.2, 1.1, 1, and 0.9 V are 98.61%, 98.40%, 98.14%, and 97.75. Also, for these power supply voltages, the proposed design has at least 83.24%, 81.84%, 79.94%, and 76.95% lower energy consumption compared to its adiabatic counterparts. It is noteworthy that small and almost negligible energy savings reductions of the proposed design compared to its CMOS counterpart are due to the reduction of the ratio of power supply voltage over the threshold voltage of PMOS transistors. Since PMOS transistors are turned off before all the stored charges at output nodes can be restored, by lowering the power supply voltage and for constant threshold voltage, less charge recovery is performed.

C. TMR Sweep

An important parameter that can affect the performance of MTJ-based circuits is TMR. In order to investigate the effects of different TMRs on the performance of the proposed design, different simulations with different TMRs at the frequency of 10 MHz and power supply voltage of 1.2 V have been carried out. The energy consumption results of these simulations are shown in Table V. Also, the energy savings of the proposed design with different TMR for different frequencies are shown in Fig. 3. Although the results show that by increasing TMR the energy consumption will decrease, the difference between the energy consumption of the proposed design for different TMR is negligible. Furthermore, the reduction in energy consumption by increasing the TMR is due to the fact that for the same size of MTJ, its resistance increases by increasing TMR.

D. Area Overhead

In the area- and energy-limited applications like IoT and medical devices, in addition to energy consumption, area overhead is also of great importance. Accordingly in this part, the transistor numbers of the proposed design and its counterparts are compared.

TABLE VII. ENERGY PROFILE METRICS OF THE PROPOSED DESIGN AND ITS COUNTERPARTS AT THE FREQUENCY OF 10 MHZ

Design	CMOS design	CP1	CP2	CP3	Proposed design
E_{min} (fJ)	45.78	6.004	7.096	6.179	1.0446
E_{max} (fJ)	103.87	6.077	7.187	6.257	1.0451
E_{avg} (fJ)	73.201	6.039	7.138	6.220	1.0449
Standard deviation	2.60E-14	1.87E-17	2.36E-17	2.03E-17	2.2866E-19
NED	0.55926	0.01208	0.01265	0.01243	0.000531
NSD	0.35651	0.00311	0.00317	0.00327	0.0002188

TABLE VIII. ENERGY PROFILE METRICS OF THE PROPOSED DESIGN FOR DIFFERENT TMR AT THE FREQUENCY OF 10 MHZ

TMR	1	1.5	2	2.5	3
E_{min} (fJ)	1.1030	1.0777	1.0641	1.0528	1.0446
E_{max} (fJ)	1.1032	1.0789	1.0648	1.0540	1.0451
E_{avg} (fJ)	1.1031	1.0786	1.0644	1.0532	1.0449
Standard deviation	6.611E-19	1.795E-19	2.849E-19	4.022E-19	2.2866E-19
NED	0.000313	0.001091	0.000656	0.00117	0.000531
NSD	0.000599	0.000166	0.000267	0.0003819	0.0002188

TABLE IX. ENERGY PROFILE METRICS OF THE PROPOSED DESIGN FOR DIFFERENT SUPPLY VOLTAGES AT THE FREQUENCY OF 10 MHZ

Power supply voltage	0.9 V	1 V	1.1 V	1.2 V
E_{min} (fJ)	0.5620	0.68054	0.83509	1.0446
E_{max} (fJ)	0.5646	0.68060	0.83551	1.0451
E_{avg} (fJ)	0.5636	6.68058	0.83540	1.0449
Standard deviation	6.2142E-19	2.0360E-19	9.2747E-20	2.2866E-19
NED	0.0005180	0.000775	0.000497	0.000531
NSD	0.0001102	0.000299	0.000111	0.0002188

Table VI shows the transistor numbers of the proposed design and its counterparts. Since the MTJs are manufactured in a separate layer on the top of the transistors, they have not been taken into account for the comparison in this part. Table VI shows that the proposed design has 83% fewer transistors compared to its CMOS counterpart, and at least 74% fewer transistors compared to its adiabatic counterparts. This is due to the use of MTJs as memory cells and using LiM architecture in the design of the proposed CLB. Furthermore, it is noteworthy that the proposed design, unlike its counterparts, does not need external nonvolatile memory and interface circuits to connect the external memory to the CLBs. By taking into account these circuits, the proposed design will reach higher superiority in the case of transistor number and energy consumption.

V. Power Side-Channel Security

While the main channels of many cryptography algorithms are theoretically secure, attackers can use the side channels of the hardware implementation of these algorithms to steal information by observing the correlation between the processing data and side channels like power consumption. The most common side channel that is used to perform the attack is the power side channel. The techniques used by designers to encounter power analysis attacks can be categorized into two categories: concealing and hiding [8, 26-28]. In the concealing approach, designers try to randomize the power profile, while in the hiding approach, designers try to flatten the power consumption. Normalized energy deviation (NED) and normalized standard deviation (NSD) are good indicators of how flattened a power trace is. Lower values for NED and NSD show higher resistance against power analysis attacks. Accordingly, in this paper, NED and NSD values are used to compare the security of the proposed design and its counterparts. First, the NED and NSD values of the proposed design and its counterparts for different frequencies are compared, and next, the effect of using different TMR and power supply voltages are investigated. The NED and NSD values are calculated using Eq. 4. and Eq. 5.

$$NED = \frac{E_{max} - E_{min}}{E_{max}} \quad (4)$$

$$NSD = \frac{\sigma_E}{\mu_E} \quad (5)$$

Table VII shows the maximum, minimum, average, standard deviation, NED, and NSD of the energy of the proposed design and its counterparts at the frequency of 10 MHz and supply voltage of 1.2 V. The results show that the proposed design has a significantly more uniform energy profile (1053x and 1628x smaller NED and NSD compared to its CMOS counterpart). However, compared to the CMOS design, the adiabatic counterparts have relatively smaller NED and NSD values which is due to the use of dual-rail adiabatic circuits, but they still have higher NED and NSD values compared to the proposed design. This is mainly due to the unbalanced residual charge in the output nodes. Although the stored charges in the output nodes of the proposed design cannot be completely recovered to the power supply (like adiabatic counterparts), by sharing the residual charge between the output nodes and balancing their charge, the proposed design reaches lower NED and NSD values. In addition, calculating the NED and NSD values of the proposed design and its counterparts using different frequencies has led to similar results.

In order to investigate the effect of TMR on the resiliency of the proposed design against power analysis attacks, the NED and NSD values for different TMRs at the frequency of 10 MHz and supply voltage of 1.2 V have been calculated and shown in Table VIII. The results show that the proposed design keeps the NSD values in the range of 10^{-4} for different TMR ratios which is significantly smaller than its counterparts.

Also, the NED and NSD values of the proposed design for different supply voltages at the frequency of 10 MHz and TMR of 3 have been calculated to investigate the resiliency of the

proposed design against power analysis attacks using different power supply voltages. The results are shown in Table IX. The results show that the proposed design has small values of NED and NSD for the simulated power supply voltages. Accordingly, the proposed design keeps its resiliency against power analysis attacks for different power supply voltages.

VI. Conclusion

In this paper, a two-phase energy-efficient power analysis attack-resilient adiabatic MTJ-based nonvolatile CLB has been proposed. It is proven that the proposed design has lower energy consumption and area overhead compared to its state-of-the-art counterparts. Also, the energy performance of the proposed design for different frequencies, different power supply voltages, and different TMRs have been investigated. The results show that the proposed design keeps its energy superiority for different frequencies and power supply voltages. Also, it is shown that by increasing the TMR, the energy consumption of the proposed design will slightly decrease, but the amount of reduced energy consumption is small and negligible. The NED and NSD values of energy consumption have been calculated and used as power analysis attack-resiliency metrics. These values are used to show the degree of uniformity of the energy consumption. These values are calculated for different frequencies, power supply voltages, and TMRs to investigate the resiliency of the proposed design under different situations. The results show that the proposed design has significantly smaller values of NED and NSD compared to its counterparts and it keeps its superiority in power analysis attack-resiliency for different TMR and power supply voltages.

References

[1] H. L. Chee, "Non-volatile FPGA architecture based on Resistive Random-Access Memory," University of Nottingham, 2023.

[2] J. Echavarria, S. Wildermann, A. Becher, J. Teich, and D. Ziener, "FAU: Fast and error-optimized approximate adder units on LUT-Based FPGAs," presented at the 2016 International Conference on Field-Programmable Technology (FPT), 2016.

[3] R. Rajaei, "Radiation-Hardened Design of Nonvolatile MRAM-Based FPGA," *IEEE Transactions on Magnetics,* vol. 52, no. 10, pp. 1-10, 2016, doi: 10.1109/tmag.2016.2578278.

[4] J.-S. Ng, J. Chen, K.-S. Chong, J. S. Chang, and B.-H. Gwee, "A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 30, no. 9, pp. 1144-1157, 2022, doi: 10.1109/tvlsi.2022.3175180.

[5] A. Amirany, K. Jafari, and M. H. Moaiyeri, "A Task-Schedulable Nonvolatile Spintronic Field-Programmable Gate Array," *IEEE Magnetics Letters,* vol. 12, pp. 1-4, 2021, doi: 10.1109/lmag.2021.3092995.

[6] M. Morsali, R. Zhou, S. Tabrizchi, A. Roohi, and S. Angizi, "XOR-CiM: An Efficient Computing-in-SOT-MRAM Design for Binary Neural Network Acceleration," presented at the 2023 24th International Symposium on Quality Electronic Design (ISQED), 2023.

[7] J. Kim, Y. Song, K. Cho, H. Lee, H. Yoon, and E.-Y. Chung, "Stt-mram-based multicontext fpga for multithreading computing environment," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 41, no. 5, pp. 1330-1343, 2021.

[8] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008.

[9] D. Zooker, O. O. Shalom, Y. Weizman, A. Fish, and O. Keren, "Toward Secured FPGA: Silicon Proven CLB With Reduced Information Leakage," *IEEE Solid-State Circuits Letters,* vol. 3, pp. 146-149, 2020, doi: 10.1109/lssc.2020.3008704.

[10] V. Sureshkumar, P. Chinnaraj, P. Saravanan, R. Amin, and J. J. Rodrigues, "Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation," *IEEE Transactions on Vehicular Technology,* vol. 71, no. 4, pp. 3470-3479, 2022.

[11] W. Yang, A. Degada, and H. Thapliyal, "Adiabatic Logic-based STT-MRAM Design for IoT," presented at the 2022 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2022.

[12] M. T. Nasab and H. Thapliyal, "Low-Power Adiabatic/MTJ LIM-Based XNOR/XOR Synapse and Neuron for Binarized Neural Networks," in *2023 IEEE 23rd International Conference on Nanotechnology (NANO)*, 2023: IEEE, pp. 649-654.

[13] W. Yang, M. Tanavardi Nasab, and H. Thapliyal, "Energy Efficient CLB Design Based on Adiabatic Logic for IoT Applications," *Electronics,* vol. 13, no. 7, p. 1309, 2024.

[14] P. Li *et al.*, "Spin-orbit torque-assisted switching in magnetic insulator thin films with perpendicular magnetic anisotropy," *Nat Commun,* vol. 7, p. 12688, Sep 1 2016, doi: 10.1038/ncomms12688.

[15] A. Amirany, K. Jafari, and M. H. Moaiyeri, "Highly reliable bio-inspired spintronic/CNTFET multi-bit per cell nonvolatile memory," *AEU - International Journal of Electronics and Communications,* vol. 158, 2023, doi: 10.1016/j.aeue.2022.154452.

[16] M. T. Nasab, A. Amirany, M. H. Moaiyeri, and K. Jafari, "Process-in-Memory realized by nonvolatile Task-Scheduling and Resource-Sharing XNOR-Net hardware Accelerator architectures," *AEU-International Journal of Electronics and Communications,* p. 155284, 2024.

[17] A. Amirany, K. Jafari, and M. H. Moaiyeri, "True Random Number Generator for Reliable Hardware Security Modules Based on a Neuromorphic Variation-Tolerant Spintronic Structure," *IEEE Transactions on Nanotechnology,* vol. 19, pp. 784-791, 2020, doi: 10.1109/tnano.2020.3034818.

[18] B. Jahannia, S. A. Ghasemi, and H. Farbeh, "An energy efficient multi-retention STT-MRAM memory architecture for IoT applications," *IEEE Transactions on Circuits and Systems II: Express Briefs,* 2023.

[19] B. Jahannia, S. A. Ghasemi, and H. Farbeh, "Multi-Retention STT-MRAM Architectures for IoT: Evaluating the Impact of Retention Levels and Memory Mapping Schemes," *IEEE Access,* vol. 12, pp. 26562-26580, 2024.

[20] S. Dinesh Kumar, H. Thapliyal, A. Mohammad, and K. S. Perumalla, "Design exploration of a Symmetric Pass Gate Adiabatic Logic for energy-efficient and secure hardware," *Integration,* vol. 58, pp. 369-377, 2017, doi: 10.1016/j.vlsi.2016.08.007.

[21] Z. Kahleifeh, H. Thapliyal, and S. M. Alam, "Adiabatic/MTJ-based physically unclonable function for consumer electronics security," *IEEE Transactions on Consumer Electronics,* vol. 69, no. 1, pp. 1-8, 2022.

[22] A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and cpa-resistant implantable medical devices," *IEEE Transactions on Consumer Electronics,* vol. 68, no. 1, pp. 47-56, 2022.

[23] Z. Yue *et al.*, "Compact Model of Subvolume MTJ and Its Design Application at Nanoscale Technology Nodes," *IEEE Transactions on Electron Devices,* vol. 62, no. 6, pp. 2048-2055, 2015, doi: 10.1109/ted.2015.2414721.

[24] Y. Wang *et al.*, "Compact Model of Dielectric Breakdown in Spin-Transfer Torque Magnetic Tunnel Junction," *IEEE Transactions on Electron Devices,* vol. 63, no. 4, pp. 1762-1767, 2016, doi: 10.1109/ted.2016.2533438.

[25] Y. Wang, Y. Zhang, E. Y. Deng, J. O. Klein, L. A. B. Naviner, and W. S. Zhao, "Compact model of magnetic tunnel junction with stochastic spin transfer torque switching for reliability analyses," *Microelectronics Reliability,* vol. 54, no. 9-10, pp. 1774-1778, 2014, doi: 10.1016/j.microrel.2014.07.019.

[26] M. Alioto, M. Poli, and S. Rocchi, "Power analysis attacks to cryptographic circuits: a comparative analysis of DPA and CPA," in *2008 international conference on microelectronics*, 2008: IEEE, pp. 333-336.

[27] M. Avital, H. Dagan, O. Keren, and A. Fish, "Randomized multitopology logic against differential power analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 23, no. 4, pp. 702-711, 2014.

[28] M. Avital, I. Levi, O. Keren, and A. Fish, "CMOS based gates for blurring power information," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 63, no. 7, pp. 1033-1042, 2016.