2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic for CPA-Resistant IoT Devices

Zachary Kahleifeh and Himanshu Thapliyal
VLSI Emerging Design And Nano Things Security Lab (VEDANTS-Lab)
Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA
Email: hthapliyal@uky.edu

***Abstract*—Internet of Things (IoT) devices are mostly areas constrained and operate on a limited battery supply and therefore have tight energy budgets. Lightweight cryptography (LWC) such as PRESENT-80 allows for minimal area usage and low energy for secure operations. However, CMOS implemented LWCs are vulnerable to side-channel attacks such as Correlation Power Analysis (CPA). Adiabatic Logic is an emerging circuit design technique that can reduce energy consumption and be CPA resistant. Many existing adiabatic logic families use a 4-phase clocking scheme which pays a large area penalty. Thus, in this paper, we propose 2-EE-SPFAL, a 2-phase clocking scheme implementation of an existing adiabatic family known as EE-SPFAL. We explore 2-phase sinusoidal waves in terms of energy efficiency and security. To demonstrate energy savings and security against CPA attacks we construct one round of PRESENT-80 in both CMOS and 2-EE-SPFAL. Simulations were conducted using 45nm technology in Cadence Spectre. At 12.5MHz, our results show an average energy saving of 50% between CMOS and 2-EE-SPFAL. Furthermore, we performed a CPA attack on both the CMOS and 2-EE-SPFAL implementation and determined that the CMOS key could be retrieved while the adiabatic key was kept hidden.**

***Index Terms*—Energy recovery computing, Hardware Security, Side-Channel Attacks, Correlation Power Analysis**

I. Introduction

The arrival of the IoT age has led to an increase in the need for energy-efficient Integrated Circut (IC) design techniques with a parallel focus on the security of these devices. The Cisco Global Cloud Index estimates that close to 850ZB will be generated by IoT machines and people by 2021 [1]. Many of these devices, industrial and consumer alike, communicate and store information and thus are targets for side-channel attacks. Side-channel attacks come in many forms, they can exploit power consumption [2], timing [3], etc. Of the power analysis attacks, Correlation Power Analysis (CPA) attack is widely used because of its robustness towards both symmetric and non-symmetric cryptographic algorithms [4].

Novel computing paradigms such as adiabatic logic are promising to develop low energy and CPA resistant circuits [5]–[8]. Adiabatic logic recycles energy to reduce power [9], [10]. Further, adiabatic circuits can be designed such that their evaluation networks are balanced and therefore having equal discharge to prevent information leakage. Many adiabatic families operate on a 4-phase clocking scheme which can lead to high amounts of area overhead from both interconnection routing and the clock structure. Thus, in this paper, we explore 2-phase clocking to reduce area while remaining energy-efficient and secure.

Previously, we proposed a CPA resistant adiabatic logic family known as Energy Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [7]. EE-SPFAL operates using a 4-phase trapezoidal clocking scheme. To remain CPA resistant, EE-SPFAL requires four separate clocks and four separate discharge signals. A large amount of interconnects can lead to large areas on post-layout chip designs. 4-phase clocking design can be more complex than their 2-phase counterpart. Thus, in this paper, we propose 2-EE-SPFAL, a 2-phase implementation of EE-SPFAL to reduce interconnect area and clock design complexity. In our 2-EE-SPFAL design, we implement the circuit using a sinusoidal wave. To demonstrate energy savings and security we have constructed one round of PRESENT-80 using both CMOS and 2-EE-SPFAL. At 12.5MHz, our results show an average energy saving of 50% between CMOS and 2-EE-SPFAL. To demonstrate secure operations we preformed a CPA attack on PRESENT-80. We were able to retrieve the key of the CMOS implementation of PRESENT using 5120 traces. However, we were not able to retrieve the key of the 2-EE-SPFAL sinusoidal wave implementation of PRESENT-80.

The paper structure is organized as follows: Section II discuses adiabatic logic. Section III discusses the proposed implementation of 2-phase adiabatic clocking within EE-SPFAL. Section IV discusses the simulation results of 2-EE-SPFAL implemented NAND and XOR gates. Section V discuses PRESENT-80, a lightweight cryptography standard, its vulnerability to CPA attacks, and its defense using 2-EE-SPFAL. Finally, Section VI concludes the paper and discuss potential future work.

II. Background on Adiabatic Logic

Adiabatic logic is one of the low-power design techniques for designing ultra-low-energy circuits [9]. Adiabatic logic reduces the overall energy consumed by the circuit by efficiently recycling the energy stored in the load capacitor after each clock cycle. The recovered energy is then reused in the next cycle. The energy dissipated in an adiabatic circuit is given by:

$$E_{diss} = \frac{RC}{T} C V_{dd}^2 \tag{1}$$

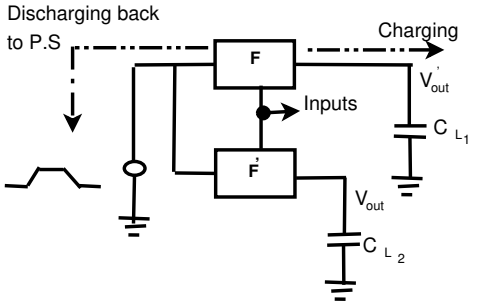


Fig. 1: Adiabatic charging and recovery principle

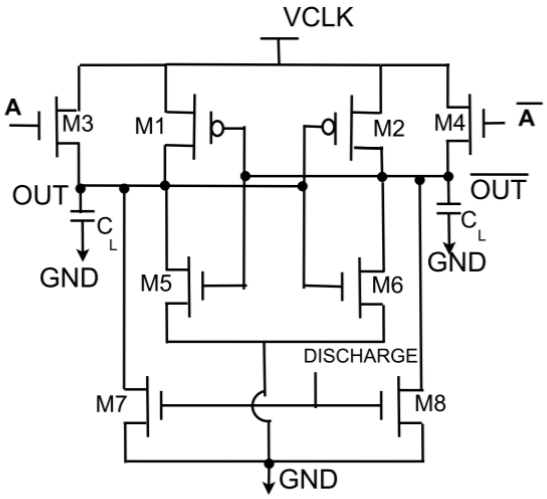


Fig. 2: Buffer design using Energy-Efficient Secure Positive Feedback Logic (EE-SPFAL) [7]

Where T is the charging period of the capacitor, C is the output load capacitor, V_{dd} is the full swing of the 2-phase power clock (e.g the max of the sinusoidal waveform to the ground). If the charging time $T > 2RC$, then the energy dissipated by an adiabatic circuit is less than a conventional CMOS circuit. Figure 1 illustrates the principle of charging and discharging (Recovery) within an adiabatic system.

III. Proposed 2-Phase Energy-Efficient Secure Positive Feedback Logic (2-EE-SPFAL)

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is a recently proposed low energy and CPA resistant logic family [7]. Figure 2 shows the schematic of the EE-SPFAL buffer. Transistors M1 and M2 are used to recover charge stored within the output load capacitors as the power clock is approaching ground. Transistors M3 and M4 are used to evaluate the logic. The evaluation transistors are designed such that the charge on out and $\overline{out}$ is balanced. Transistors M5 and M6 are used to avoid logic degradation. Finally, transistors M7 and M8 are used to reset the outputs before the next operation occurs. EE-SPFAL was originally constructed with a 4-phase trapezoidal clocking scheme. In this paper, we present the 2-phase design of EE-SPFAL using sinusoidal power clocks. For 2-phase EE-SPFAL to work properly and be CPA resistant, adjustments are made to the clocking scheme and discharge signals.

Figure 3 shows the proposed sinusoidal clocking scheme. It consists of two sinusoidal waves $180°$ out of phase. The clocking scheme consists of an "evaluate" phase in which the power clock is rising and a "recover" phase in which the power clock is falling. There are two discharge signals, one for each clock. The period and delay of the discharge signals are equal to their respective clocks.

Using two clocks rather than four results in multiple benefits. Namely, two clocks reduces the amount of area and complexity required to generate the power clock. Take the 4-phase clock generator in [11] and the 2-phase clock generator in [12] as a case study. The 4-phase design consumes a substantial area and requires a more complex design than in the 2-phase design.

The 4-phase clocking scheme also leads to a more complicated routing scheme. Using 4-phases requires four separate interconnects when four or more gates are cascaded. Take the four buffers seen in Figure 4 as a case study, in the 4-phase case, eight separate interconnects are required for the circuit to operate correctly while in the two phase case only four interconnects are needed.

IV. Simulation Results of 2-EE-SPFAL Logic Gates

Simulations are conducted using Cadence Spectre in 45nm CMOS technology. Each 2-EE-SPFAL gate results in a half-cycle delay thus additional buffers are inserted in 2-EE-SPFAL circuits to synchronize the outputs. The power numbers reported in this paper for the 2-EE-SPFAL based adiabatic circuits are calculated using the following formula:

$$P = \sum_{n=0}^{i} V_{Pi} \times I_{Pi} \tag{2}$$

Where V_{Pi} is the voltage of the i_{th} power clock and I_{Pi} is the current of the i_{th} power clock. While energy is defined as:

$$E = \int P\, dt = \int \sum_{n=0}^{i} V_{Pi} \times I_{Pi}\, dt \tag{3}$$

We evaluate two criteria to determine the energy efficiency and security of 2-EE-SPFAL. The criteria Normalized Energy Deviation (NED) is defined as (E_{max} - E_{min})/E_{max}. NED is used to indicate the percent difference between the minimum and maximum energy consumption of the possible input transitions. A second parameter, Normalized Standard Deviation (NSD), is defined as $\frac{\sigma_e}{\overline{E}}$ where σ_e is the standard deviation of the energy dissipated by the circuit per input transition and $\overline{E}$ is the average energy dissipation. Both NED and NSD are important parameters when determining circuit resilience to CPA attacks.

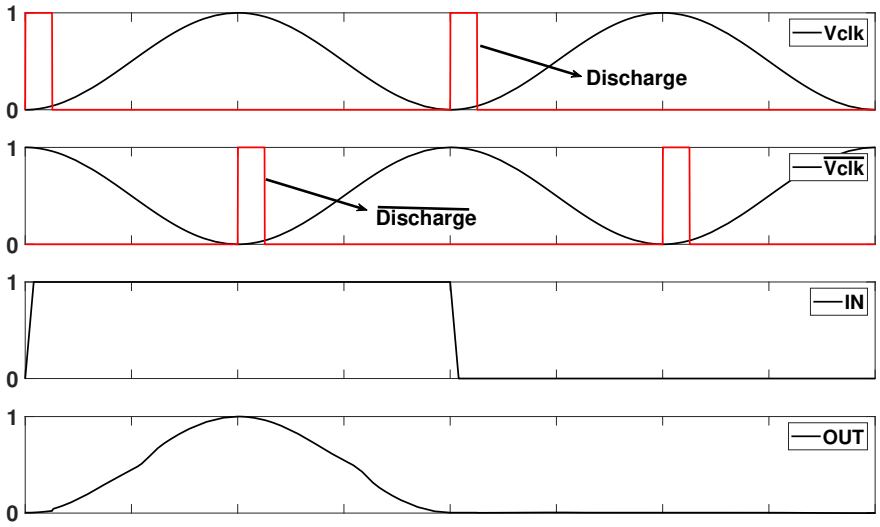


Fig. 3: Proposed 2-phase sinusoidal clocking scheme for EE-SPFAL

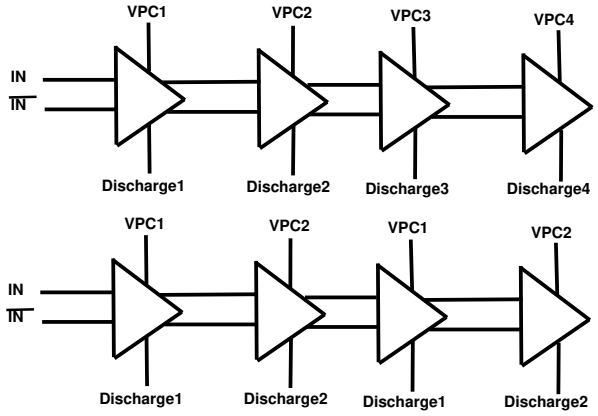


Fig. 4: Design of four buffers using 4-phase clocking and 2-phase clocking

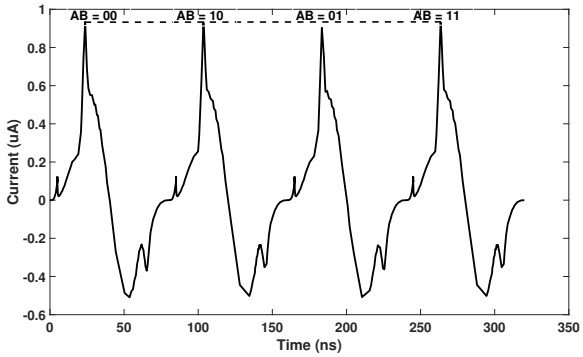


Fig. 5: Uniform current consumption of the 2-EE-SPFAL XOR gate

TABLE I: Simulation and calculation results for NAND and XOR gates

Parameter	2-EE-SPFAL (NAND)	2-EE-SPFAL (XOR)
$E_{min}(fJ)$	1.85	1.88
$E_{max}(fJ)$	1.96	1.90
$E_{avg}(fJ)$	1.91	1.89
NED	0.05	0.01
NSD	0.01	0.004

Table I show the simulated and calculated parameters for the 2-EE-SPFAL sinusoidal based NAND and XOR implementation at 12.5 MHz. The low NED and NSD calculations show that 2-EE-SPFAL sinusoidal has minimal energy consumption changes between the input transitions. From the table, it can also be seen that the XOR gate of 2-EE-SPFAL sinusoidal has lower values of NED and NSD compared to NAND gate.

From Figure 5 we can see that regardless of input combination, the current consumption of the XOR gate is nearly constant. The small variations in current results in minimal NED and NSD values and thus are theoretically more resistant to Correlation Power Analysis (CPA) attacks.

V. Low Energy and CPA-Resistant PRESENT-80

A. *Present: A lightweight encryption*

PRESENT [13] is a lightweight cipher that is designed for low energy devices. PRESENT has obtained ISO/IEC standard (ISO/IEC 29192-2) for lightweight cryptography. PRESENT has low area overhead which makes it an ideal candidate for IoT circuits that look to balance area and security.

PRESENT supports key lengths of 80 or 128 bits. As the goal of this paper is low energy, we decided to use an 80-bit key. PRESENT-80 consists of 31 rounds, a round consists of the following operations:

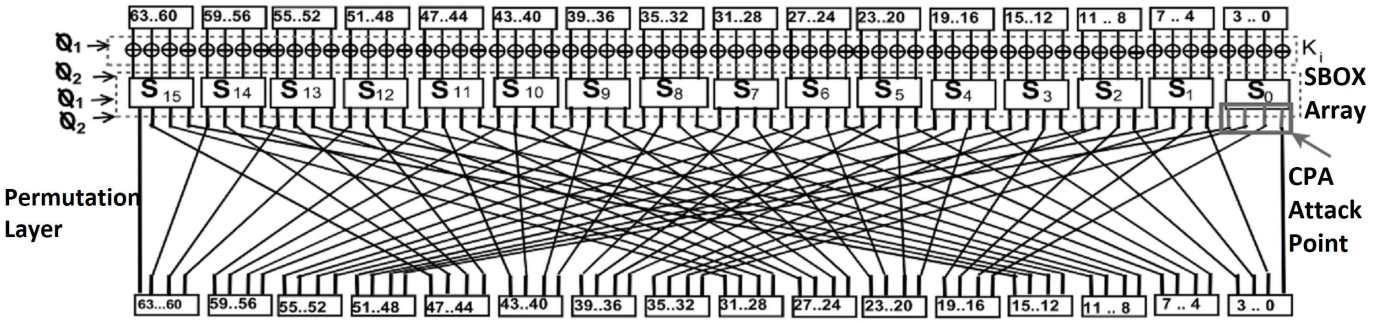


Fig. 6: One round of PRESENT-80 implemented in 2-EE-SPFAL

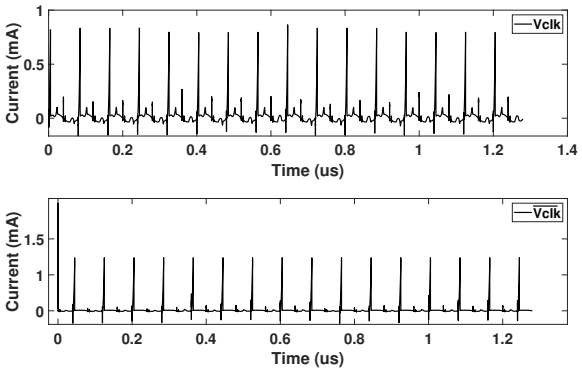


Fig. 7: Uniform current traces of PRESENT-80 implemented with 2-EE-SPFAL: Vclk and $\overline{Vclk}$ current traces

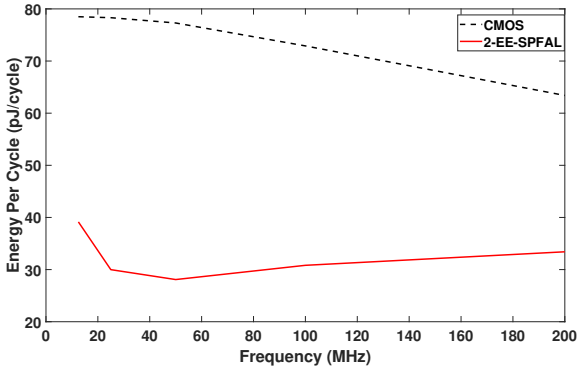


Fig. 8: Energy per cycle of PRESENT-80 implemented in CMOS and 2-EE-SPFAL

AddRoundKey: The 64-bit plain text is XORed with 64-bits of the key.

S-Box Layer: 16 4x4 identical S-Boxes are computed in parallel as a non-linear substitution layer.

P-Layer: Finally, the output of the S-Box circuits are permutated to allow for diffusion.

PRESENT-80 implemented in CMOS is susceptible to side-channel attacks such as Correlation Power Analysis (CPA). Many countermeasures against CPA attacks are not suitable for IoT devices as they consume large amounts of power [5] thus we explore to design PRESENT-80 using 2-EE-SPFAL.

B. 2-EE-SPFAL Implementation of PRESENT-80

CMOS implementation of PRESENT-80 is susceptible to Correlation Power Analysis (CPA) attacks and consumes large amounts of energy and thus is not suitable for low power IoT devices. In this section, we discuss the implementation of one round of PRESENT-80 with 2-EE-SPFAL. 2-EE-SPFAL requires two sinusoidal clocks $180°$ out of phase. Figure 6 shows the implementation of 1-round of PRESENT 80. The AddRoundKey stage is operated by ϕ_1, the S-Box stage consists of both ϕ_1 and ϕ_2 where ϕ_1 and ϕ_2 are the two respective power clocks.

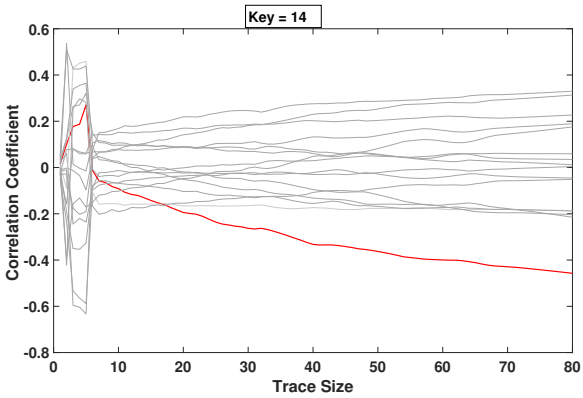
PRESENT-80 implemented with 2-EE-SPFAL from both Vclk and $\overline{Vclk}$. The uniform current traces during the operation of PRESENT-80 will prevent information leakage as we will see when a Correlation Power Analysis is performed. Figure 8 shows the energy per cycle of both the CMOS and 2-EE-SPFAL implementation of PRESENT-80 as a function of frequency. From Figure 8 we can see that when using a sinusoidal power clocks, 2-EE-SPFAL consumes less energy than its CMOS counterpart through 200MHz. Table II also shows the energy per cycle difference between the CMOS and 2-EE-SPFAL sinusoidal implementation of PRESENT-80. From Table II we can see that at 12.5MHz, there is an average energy saving of 50% between CMOS and 2-EE-SPFAL based designs.

TABLE II: Energy per cycle of one round of Present-80 implemented with CMOS and 2-EE-SPFAL

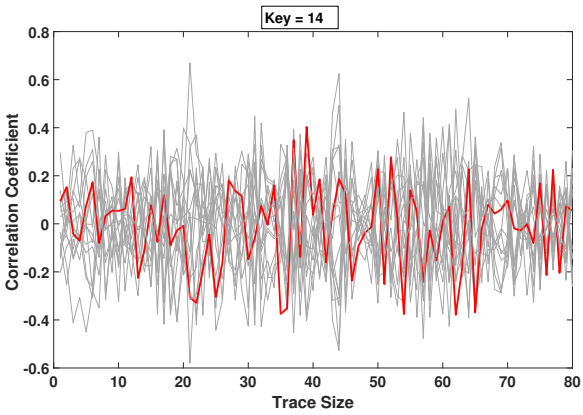
Energy Per Cycle (pJ/Cycle)	12.5MHz	25MHz	50MHz	100MHz	200MHz
CMOS	0.78	0.78	0.77	0.72	0.63
2-EE-SPFAL (sinusoidal)	0.39	0.29	0.28	0.31	0.38

C. CPA Attack on PRESENT-80

2-EE-SPFAL based implementation of PRESENT-80 has been shown to reduce energy when compared to CMOS. However, it is important to validate the security of 2-EE-SPFAL. The S-Box layer of PRESENT-80 is chosen as the attack point (Figure 6). The CPA attack is performed by



(a) Successful CPA attack on CMOS based implementation of 1 round of PRESENT-80



(b) Unsuccessful CPA Attack on 2-EE-SPFAL based implementation of 1 round of PRESENT-80

Fig. 9: Correlation power analysis performed on both CMOS and 2-EE-SPFAL implementation of PRESENT-80

following the steps described in [14]. The simulation was performed at 12.5MHz with a 100fF load. The sinusoidal wave implementation of 2-EE-SPFAL was used as the test circuit. Practical CPA attacks usually require greater than 100,000 traces to be successful. However, we are performing a simulation which is absent from electrical noise and therefore we require much fewer traces. We have chosen 80 samples per clock period thus we will sample every 1ns assuming a clock period of 80ns. 5120 input traces were necessary to complete a successful CPA attack on the CMOS based design of PRESENT-80. Figure 9a shows a successful CPA attack on a CMOS implementation of PRESENT-80.

While the CMOS key was revealed in 5120 traces, the 2-EE-SPFAL implementation of PRESENT-80 did not reveal the key in greater than 12,000 traces. Figure 9b shows an unsuccessful CPA attack against the 2-EE-SPFAL implemented PRESENT-80. This case study shows 2-EE-SPFAL is a promising candidate for secure and low energy IoT devices.

VI. Conclusion and Future Work

In this paper, we have demonstrated the applicability of secure 2-phase adiabatic logic as a novel computing paradigm to design low energy and secure IoT devices. One round of PRESENT-80 is designed using both standard CMOS and adiabatic design principles as a case study. The circuits were analyzed and simulated using Cadence Spectre. The results show significant energy savings between the adiabatic design and the CMOS design. Along with energy savings, the adiabatic implementation of PRESENT-80 was able to keep the key secret when a Correlation Power Analysis attack was performed on the circuit. Post-layout area analysis of 2-EE-SPFAL needs to performed to understand the area savings of 2-phase implementation. Energy consumption of 2-EE-SPFAL must be evaluated with the integration of the power clock generator. Theoretical analysis of the 2-EE-SPFAL is needed to understand the reasons for high energy consumption at lower frequencies.

Acknowledgment

This work is partially supported by National Science Foundation CAREER Award No. 1845448.

References

[1] C. G. C. Index and C. C. V. N. Index, "Forecast and methodology, 2016–2021; white paper; cisco systems," *Inc.: San Jose, CA, USA*, 2017.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[3] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater, and J.-L. Willems, "A practical implementation of the timing attack," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 1998, pp. 167–182.

[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2004, pp. 16–29.

[5] A. Moradi and A. Poschmann, "Lightweight cryptography and dpa countermeasures: A survey," in *International Conference on Financial Cryptography and Data Security*. Springer, 2010, pp. 68–79.

[6] S. D. 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.

[7] S. D. Kumar, H. Thapliyal, and A. Mohammad, "Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 281–293, April 2019.

[8] S. D. Kumar and H. Thapliyal, "Exploration of non-volatile mtj/cmos circuits for dpa-resistant embedded hardware," *IEEE Transactions on Magnetics*, vol. 55, no. 12, pp. 1–8, Dec 2019.

[9] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Y.-C. Chou, "Low-power digital systems based on adiabatic-switching principles," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 2, no. 4, pp. 398–407, 1994.

[10] P. Teichmann, *Adiabatic logic: future trend and system level perspective*. Springer Science & Business Media, 2011, vol. 34.

[11] J. Hu, W. Zhang, X. Ye, and Y. Xia, "Low power adiabatic logic circuits with feedback structure using three-phase power supply," in *Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005.*, vol. 2. IEEE, 2005.

[12] W. C. Athas, L. Svensson, and N. Tzartzanis, "A resonant signal driver for two-phase, almost-non-overlapping clocks," in *1996 IEEE International Symposium on Circuits and Systems. Circuits and Systems Connecting the World. ISCAS 96*, vol. 4. IEEE, 1996, pp. 129–132.

[13] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 450–466.

[14] J. Wu, Y. Shi, and M. Choi, "Measurement and evaluation of power analysis attacks on asynchronous s-box," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 10, pp. 2765–2775, 2012.