2-SPGAL: 2-Phase Symmetric Pass Gate Adiabatic Logic for Energy-Efficient Secure Consumer IoT

Amit Degada 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*—The adaptation of the Internet-of-Things (IoT) for consumer electronics has enabled us to uplift everyday life. Low-power smart and secure computing devices are needed to sustain the expected growth of consumer IoT. Adiabatic switching is a modern approach that recycles the energy stored in load capacitance to save energy. Further, the cryptographic circuit designed using adiabatic switching is secure against the Correlation Power Analysis (CPA) attack in contrast to the same circuit designed using standard CMOS. In this paper, we propose 2-SPGAL, a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). As a case study, we simulated the design of PRESENT-80 (a lightweight cryptographic scheme) one round with an in-built Power Clock Generator (PCG) with 45nm technology. The 2-SPGAL shows on an average 82.76% and 67.35% better energy saving compared to standard CMOS, and 2-EE-SPFAL (another 2-phase adiabatic logic), respectively at a frequency range from 100 kHz to 25 MHz with a load of 1 fF. The 2-SPGAL has 16.78% savings of the number of transistors compared to 2-EE-SPFAL for implementation of one round PRESENT-80. Further, the CPA attacks reveal the key in standard CMOS, however, 2-SPGAL PRESENT-80 adiabatic logic design was successful to protect the key.**

***Index Terms*—Hardware security, adiabatic logic, side-channel attacks, correlation power analysis, cryptographic circuits.**

I. Introduction

The interest of the consumer in Internet-of-Things (IoT) based smart connected devices has gained momentum in recent years. Further, the recent development of cloud and edge computing, better internet connectivity, and smart hand-held devices has significantly sped up the adaptation of IoT in everyday life. The application domain of consumer IoT includes, but is not limited to, healthcare, wearable devices, smart-manufacturing, agriculture, and home-automation, etc [1]. However, there is a significant risk, and the threat is associated with collecting such huge user data generated by smart devices. The future growth of IoT significantly depends upon the device, which establishes the level of trust to consumers to share their data [2] [3]. One intriguing research direction is to design a low-powered embedded device that can prevent information leakage through Side-Channel Attack (SCA).

The SCA (see Figure 1) depends upon the observation of instantaneous power consumption [4], timing [5], electromagnetic (EM) radiation and few other observable criteria. If the devices have distinguishable power consumption for different operations then a successful Correlation Power Analysis (CPA), a type of SCA, can be carried out. The adiabatic logic circuit not only helps to reduce the energy consumption but "hides" the information leakage by avoiding instantaneous charging and discharging of the capacitor and balancing evaluation network [6] [7]. Over the years, researchers have proposed many adiabatic logic circuits working on a 4-phase clocking mechanism. Reduction in phases of operation can help to reduce the interconnection length, routing mechanism, and complexity of clock structure. In this work, we explore the 2-phase clocking scheme and evaluate its performance on the metrics of energy and secure design.

Our earlier work, Symmetric Pass Gate Adiabatic Logic (SPGAL) [8] is a 4-Phase clocking adiabatic logic circuit. SPGAL achieves a reduction in the adiabatic losses by ensuring zero potential difference between the source and drain of the transistor during the evaluation phase. Further, SPGAL has balanced supply peak current traces to achieve secure circuit design. However, SPGAL needs a 4-phase clocking mechanism and can result in higher interconnect lengths, thereby resulting in a higher post-layout area.

A. Key Contribution from this work

The key contribution of this work is as follow:

- We propose 2-SPGAL, a 2-phase clocking implementation of our earlier work on SPGAL [8]. The 2-phase clocking scheme could help to make the clock generator design simpler, reduction in the clocking complexity, and interconnect the area.
- As a case study, we implemented PRESENT-80 one round, a lightweight cryptographic scheme with an in-built power generator using 2-SPGAL. The simulation was carried out for a frequency range from 100 kHz to 25 MHz with a load of 1 fF. The 2-SPGAL shows an average 82.76% and 67.35% better energy saving compared to its counterpart standard CMOS and 2-EE-SPFAL [9], respectively.
- We demonstrate that the 2-SPGAL based PRESENT-80 one round encryption successfully protects the key against the CPA attack.
- Further, the 2-SPGAL based PRESENT-80 one round implementation requires 16.78% fewer transistors compare to 2-EE-SPFAL based design.

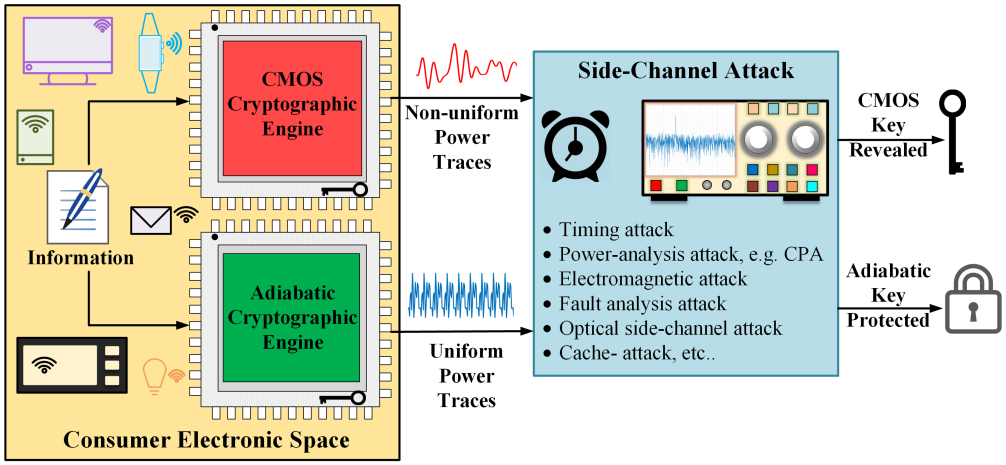

Fig. 1: Adiabatic logic as potential solution for low-power secure computing platform for consumer electronics.

B. Organization of the paper

This paper is organized as follows: Section II explains the background of adiabatic logic and evaluation metrics for secure adiabatic logic design. In Section III, an approach to the clocking scheme for 2-SPGAL based adiabatic logic is presented. Section IV presents the information to design an in-built power clock generator for the adiabatic logic-based system. Section V presents the design of PRESENT-80 one round implementation as a case-study of CPA-resistant circuit design. Section V is the conclusion of the paper.

II. Background

In this section, we discuss the background of adiabatic logic and how it can help to save energy. Further, we explain the key metrics indicating the ability of adiabatic logic to withstand CPA.

A. Adiabatic logic

Adiabatic logic is based on charging capacitive load using constant current rather than usual constant voltage [6]. However, designing the constant current source is a challenging task, thus in practice, a ramp voltage source is preferred as a replacement for constant current voltage. The ramp signal is usually referred to as Power Clock (PC) which serves as a power and clock source in an adiabatic circuit. As shown in Figure 2, the reduction in energy consumption in adiabatic logic is achieved. This is because as the energy stored in the capacitor after the end of each clock cycle is utilized in a successive clock cycle. The amount of energy consumed in adiabatic is given by equation 1.

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

In equation 1, T is the charging or discharging period of the load capacitor C, R is resistance due to transistor, and V_{dd} is the full-swing voltage in PC. We can see that if T is maintained greater than RC then, the energy consumption turns out to be less than standard CMOS.

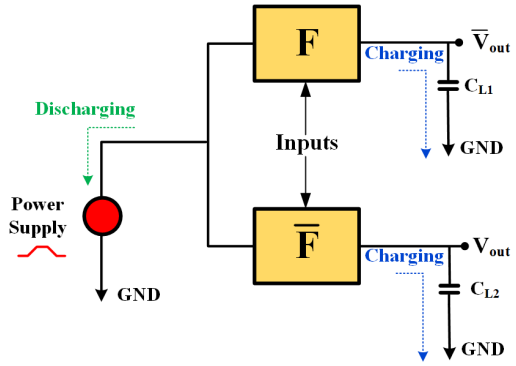

Fig. 2: Charging and discharging in adiabatic circuits.

B. Evaluation metrics for adiabatic logic

The dual-rail structure of the adiabatic logic system helps to maintain a uniform current profile makes. The CPA exploits the power consumption traces and is widely used for its proven success against both symmetric and non-symmetric cryptographic algorithms [10]. The metrics, Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) are useful metrics to understand the efficacy of the circuit to withstand the CPA attack.

$$NED = \frac{(E_{\max} - E_{\min})}{E_{\max}} \tag{2}$$

$$NSD = \frac{\sigma}{E_{avg}} = \frac{1}{E_{avg}} \sqrt{\sum_{k=1}^{N} \frac{(E_i - E_{avg})^2}{N}} \tag{3}$$

NED (equation 2), is the normalized energy difference between the minimum and maximum energy consumption among a set of values. Similarly, NSD (equation 3) is the normalized deviation of input energy value to average energy consumption, calculated upon a set of energy values.

III. Proposed Design

Symmetric Pass Gate Adiabatic Logic (SPGAL) is a CPA-resistant adiabatic logic style [8]. The SPGAL structure, as shown in Figure 3, can be categorized into three blocks, two balanced evaluation blocks: a sense amplifier, and a discharge circuit. SPGAL was originally proposed on a 4-phase clocking scheme [8]. Two pmos transistors M1 and M2, are connected in a back-to-back fashion to construct a sense amplifier/latch. The evaluation network produces the output bit set as per input signal condition at evaluation blocks. The discharge transistor M3 and M4 help to reset the output to maintain uniform power consumption.

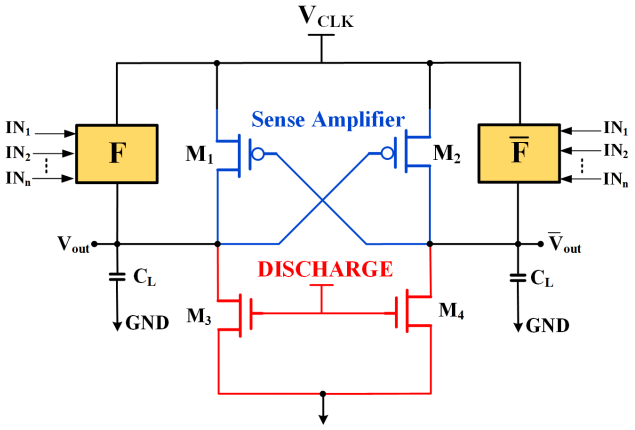

Fig. 3: General SPGAL gate structure [8].

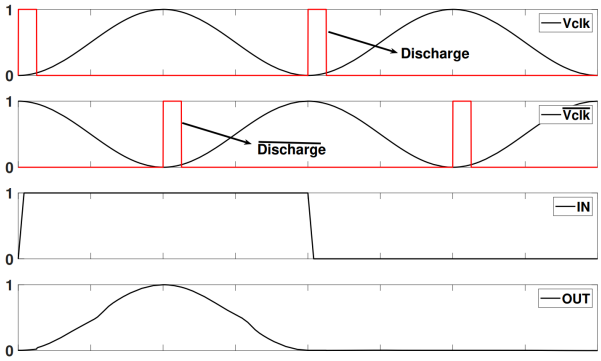

Fig. 4: 2-phase sinusoidal clocking scheme [9].

In this paper, we propose 2-SPGAL that is a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). We used two out-of-phase sinusoidal waves (Figure 4) [9]. The rising sinusoidal signal is the "evaluate" phase and the falling sinusoidal works as the "recover" phase. Further, there are two discharge signals, in "synchronization" with their respective clock signal. By the word "synchronization", we mean that the time-period and delay of the discharge signals should match with their respective sinusoidal clock signal. The reduced number of the clocks, e.g. 2-phase [11] vs. 4-phase [12] can result in a less complex clock generator design and fewer area requirements.

We evaluated the performance of the 2-SPGAL gates with 45nm technology. We can see in Figure 5 that the current in

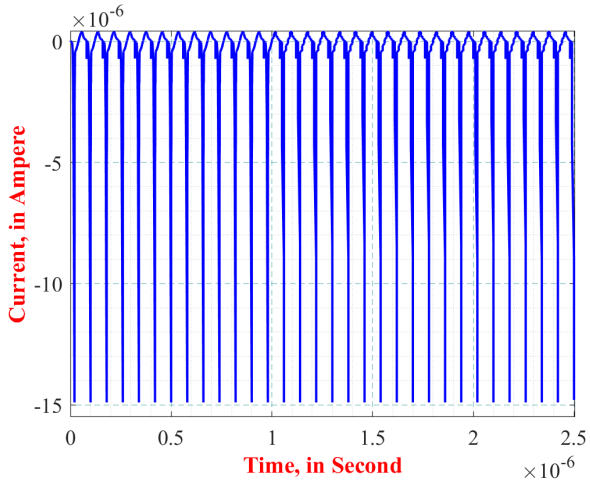

Fig. 5: Uniform current in 2-SPGAL XOR gate.

TABLE I: Simulation result for proposed 2-SPGAL and 2-EE-SPFAL [9] based logic gates at 12.5 MHz.

Parameter	AND Gate		XOR Gate	
	2-EE-SPFAL [9]	Proposed 2-SPGAL	2-EE-SPFAL [9]	Proposed 2-SPGAL
$E_{min}(fJ)$	1.87	1.82	1.87	1.83
$E_{max}(fJ)$	1.91	1.90	1.88	1.84
$E_{avg}(fJ)$	1.89	1.86	1.87	1.84
NED (%)	2.14	4.19	0.77	0.65
NSD (%)	0.70	1.32	0.30	0.25

the XOR gate is almost uniform. A small variation in current results in smaller NED and NSD. Table I list the value of E_{min}, E_{max}, E_{avg}, NED and NSD for AND and XOR gate at frequency 12.5 MHz. We can see that 2-SPGAL has better energy numbers than its counterpart 2-EE-SPFAL.

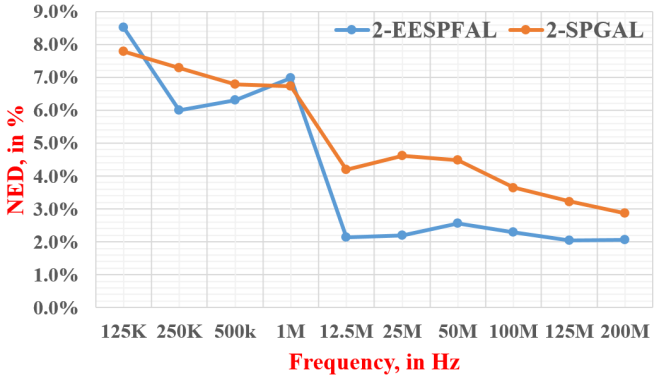

Fig. 6: NED Vs. Frequency comparison for proposed 2-SPGAL and 2-EE-SPFAL [9] AND Gate.

A lower value of NED and NSD reflects the capability of the adiabatic logic circuit to withstand CPA. The NED and NSD curve (with respect to frequency of operation) is useful to understand the relationship between information leakage and frequency. The NED and NSD value was calculated from frequency range 125 kHz to 200 MHz with load 10 fF, pmos width 120nm, and no in-built power clock generator.

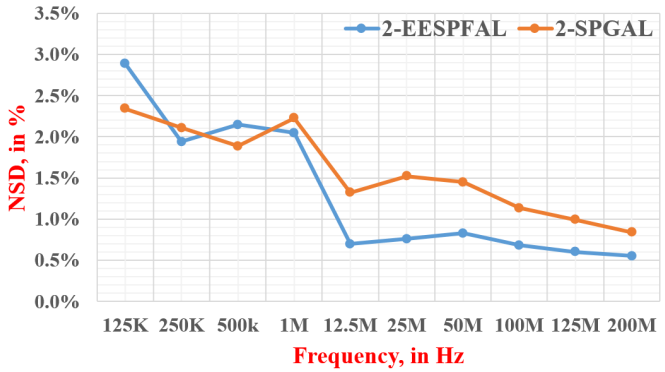

Fig. 7: NSD Vs. Frequency comparison for proposed 2-SPGAL and 2-EE-SPFAL [9] AND Gate.

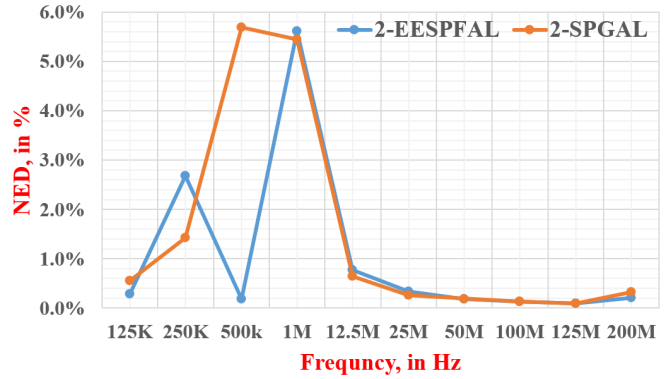

Fig. 8: NED Vs. Frequency comparison for proposed 2-SPGAL and 2-EE-SPFAL [9] XOR Gate.

Figure 6, and 7 show comparison of NED, and NSD metric performance for AND gate implemented using 2-SPGAL, and 2-EE-SPFAL. The 2-SPGAL based AND gate has an average NED value of 5.16% and NSD value of 1.58% while its counterpart 2-EE-SPFAL based AND gate has a NED value of 4.11% and NSD value of 1.32%, respectively. Similarly, in Figure 8, the NED value for 2-SPGAL based XOR gate is 1.48% while the NED value of the 2-EE-SPFAL XOR gate is 1.05%. Also, from Figure 9, the 2-SPGAL XOR gate has an average NSD value of 0.72% compared to 0.51% NSD value in the 2-EE-SPFAL XOR gate. 2-EE-SPFAL has a slightly better value of NED and NSD because of the pull-down configuration of the transistor in a sense-amplifier.

IV. 2-Phase Adiabatic Power Clock Generator

In conventional CMOS-based dynamic circuits, the clock and power lines are separate. However, in the adiabatic system, we have a single line to function as power and to maintain timing across the system. The Power Clock Generator (PCG) is a DC to AC voltage conversion using an external inductor and load of the circuit. It is important to note that the adiabatic circuit operates inherently pipelined-dynamic fashion, thus requiring multiple phase PCG designs.

The PCG consumes a large fraction of the overall adiabatic logic-based system. Inefficient PCG design could worsen the

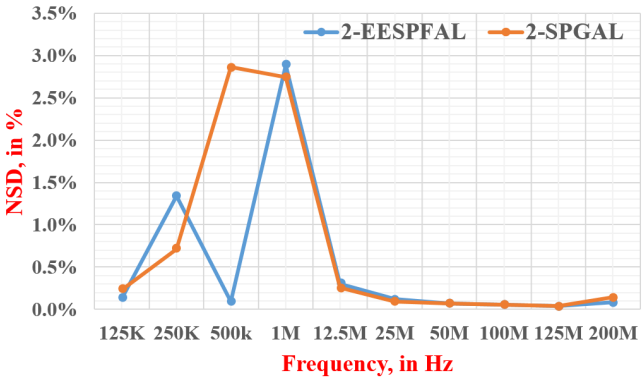

Fig. 9: NSD Vs. Frequency comparison for proposed 2-SPGAL and 2-EE-SPFAL [9] XOR Gate.

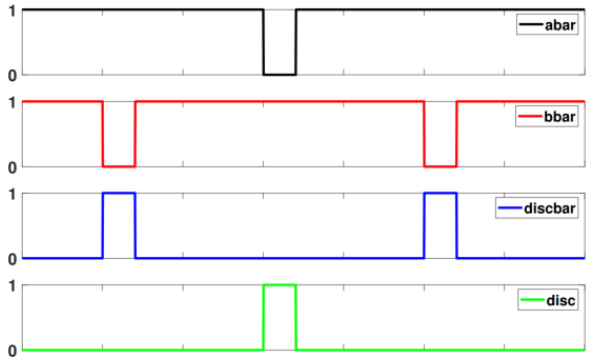

Fig. 10: Control signals in 2-Phase PCG design [9].

energy savings and hamper the energy recovery mechanism in the overall design. Thereby, the overall performance of the adiabatic circuit should be compared with the PCG design. In our work, we have used 2N-2P based synchronous PCG, originally proposed in [13]. Figure 10 shows the control signal given externally to the PCG circuit. We used a similar approach described in our earlier work [9], for $Discharge$ and $\overline{Discharge}$, serving not only as Discharge signal in the adiabatic logic circuit but also as an external control signal.

V. A case study: CPA-Resistant PRESENT-80

The objective of this section is to evaluate energy-saving and the security of 2-SPGAL based circuit design. We have implemented one round of encryption of lightweight cryptographic algorithm PRESENT-80 using the proposed 2-SPGAL. The simulation results show that 2-SPGAL based PRESENT-80 is energy efficient as compared to its implementation based on 2-EE-SPFAL and standard CMOS. We also found that the proposed 2-SPGAL based PRESENT-80 is resilient against side-channel attack CPA.

A. PRESENT-80

The embedded computing platform in consumer IoT puts a pressing demand in terms of low-power computation and lesser area. The researcher in [14] had proposed PRESENT, a lightweight cryptographic cipher. PRESENT has been a preferred choice in low-powered computing platform due to

its good balance between security and area requirements. It has two variants in terms of key size, 80 bit or 128 bit. The goal of the proposed work is for low-energy secure hardware. Therefore, we chose to simulate PRESENT-80 (80-bit variant) based on the proposed 2-SPGAL as a case study.

TABLE II: Number of Transistor Required to implement PRESENT-80 one round.

Adiabatic Logic	**2-EE-SPFAL [9]**	**Proposed 2-SPGAL**
Number of Transistor	9344	7776
2-SPGAL saves 16.78% transistor to its counterpart 2-EE-SPFAL		

Table II lists the number of transistors needed to implement the PRESENT-80 one round. We can see that 2-SPGAL based design of PRESENT-80 one round requires 7776 transistors, and 2-EE-SPFAL based implementation requires 9344 number of transistors. 2-SPGAL based implementation of PRESENT-80 one round has 16.78% less number of transistors compared to its 2-EE-SPFAL based implementation. Thus, 2-SPGAL would result in a compact layout, and smaller area designs compare to its counterpart 2-EE-SPFAL.

B. Energy value comparison

The objective of this simulation is to understand the amount of energy spent per cycle of one round of PRESENT-80 implementation. We implemented the PRESENT-80 using proposed 2-SPGAL logic and compared its energy values to existing work on 2-EE-SPFAL [9] and standard CMOS. The PRESENT-80 energy numbers for 2-SPGAL and 2-EE-SPFAL designed are obtained with an integrated clock generator. The integrated clock generator helps to maintain the uniform current traces, thereby preventing information losses to combat the CPA.

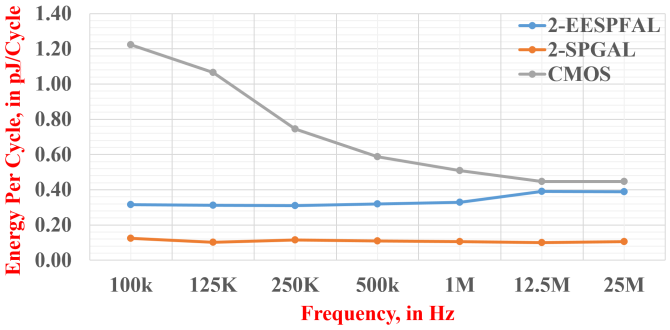

Fig. 11: Energy per cycle in PRESENT-80 one round implemented with proposed 2-SPGAL, 2-EE-SPFAL [9] and CMOS.

Figure 11 shows energy per cycle in one round PRESENT-80 implementation using standard CMOS, 2-EE-SPFAL, and 2-SPGAL design for the frequency range 100 kHz to 25 MHz with a load of 1 fF. We can see in Figure 11 that 2-SPGAL shows the overall least energy per cycle consumption across all frequencies of operation. The average energy in 2-SPGAL is 0.1090 pJ/cycle. compare to 0.3380 pJ/cycle in 2-EE-SPFAL and 0.7178 pJ/cycle in standard CMOS.

The energy-saving calculation in Table IV is calculated from the simulation result listed in Table III. The 2-SPGAL has an average of 67.35% and 82.76% better energy saving compare to 2-EE-SPFAL and standard CMOS respectively. Thus, the proposed 2-SPGAL has a significant reduction in energy dissipation.

C. CPA Attack on PRESENT-80 designed using 2-SPGAL

The objective of this section is to check the security of the 2-SPGAL based logic designed. We used the approach described in [15]. We performed a CPA attack on the S-Box layer designed using 2-SPGAL, and standard CMOS at 12.5 MHz frequency. We considered the ideal (without noise) environment to perform CPA for both designs, thus can require fewer traces. Practical CPA requires 100K traces, however, in an electrical-noise-free environment fewer (5120 in our case) would be sufficient to carry out a successful CPA attack. The S-Box of PRESENT-80, as shown in Figure 12 was chosen as an attack point.

The traces were collected in the Cadence Spectre platform. We can see in Figure 13 that the key=14 was revealed in standard CMOS design in 5120 traces. However, due to uniform current traces, the 2-SPGAL was able to preserve the key, hence validate that 2-SPGAL logic has not only to lower energy dissipation but also a CPA secure design.

VI. Conclusion

The paper presented 2-SPGAL, a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL), is a new logic style for low-power and secure computing using energy recovery circuits. 2-SPGAL requires few transistors compare to existing work on 2-phase secure adiabatic logic (2-EE-SPFAL). The 2-SPGAL shows significant energy saving at different frequencies compared to 2-EE-SPFAL and standard CMOS. Further, we demonstrated 2-SPGAL based PRESENT-80 is resistant against the CPA side-channel attack as a case study. In the future, post-layout area analysis and its effect on capacitance need to be evaluated. In conclusion, the proposed 2-SPGAL is a promising logic style to design secure and energy-efficient IoT edge computing nodes, Radio Frequency Identification (RFID), and Cyber-Physical System (CPS).

Acknowledgment

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

References

[1] C. Terrell and H. Thapliyal, "Approximate adder circuits using clocked cmos adiabatic logic (ccal) for iot applications," in *2020 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2020, pp. 1–4.

[2] I. J. Gedeon, P. Snively, C. Frey, W. Almuhtadi, and S. P. Mohanty, "Privacy and security by design," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 76–77, 2020.

[3] S. P. Mohanty, "Security and privacy by design is key in the internet of everything (ioe) era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, 2020.

TABLE III: Energy per cycle (in pJ/cycle) of one round PRESENT-80 implementation with load 1 fF.

Frequency	100 KHz	125 KHz	250 KHz	500 KHz	1 MHz	12.5 MHz	25 MHz
Proposed 2-SPGAL	0.1249	0.1024	0.1146	0.1095	0.1059	0.1008	0.1049
2-EE-SPFAL [9]	0.3164	0.3121	0.3107	0.3188	0.3284	0.3900	0.3896
CMOS	1.2238	1.0650	0.7456	0.5876	0.5096	0.4470	0.4463

TABLE IV: Energy saving comparison (in %) in proposed 2-SPGAL one round PRESENT-80 implementation.

Frequency	100 KHz	125 KHz	250 KHz	500 KHz	1 MHz	12.5 MHz	25 MHz
Compare to 2-EE-SPFAL [9]	60.53	67.20	63.11	65.65	67.76	74.17	73.07
Compare to CMOS	89.80	90.39	84.63	81.37	79.22	77.46	76.48

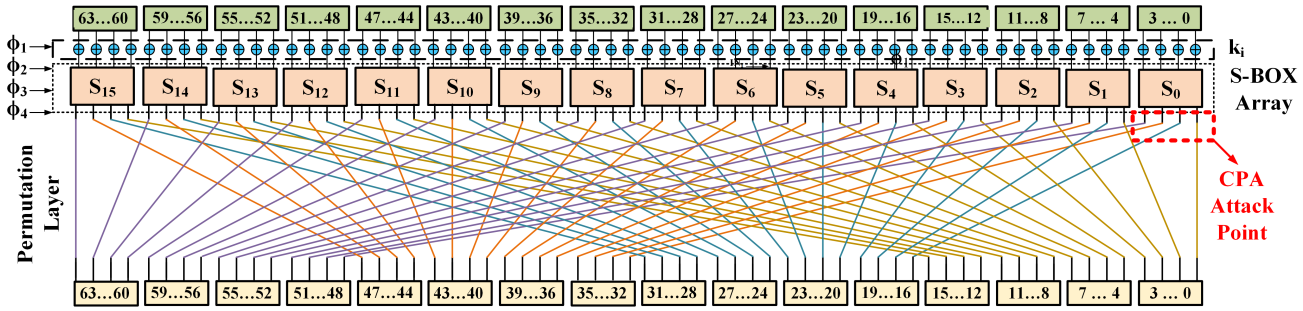

Fig. 12: PRESENT-80 one round implementation using 2-phase adiabatic logic.

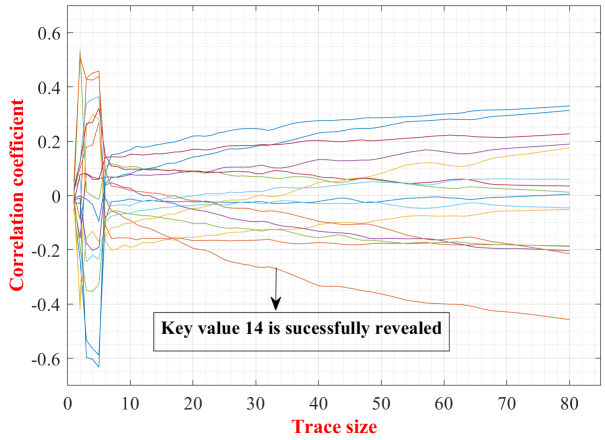

Fig. 13: Successful Revelation of Key=14 in PRESENT-80 designed with CMOS.

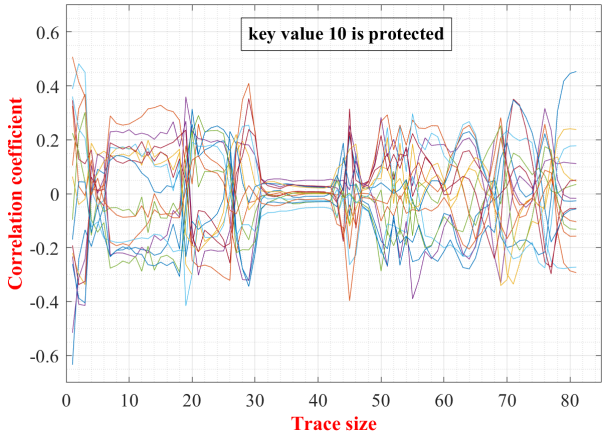

Fig. 14: Unsuccessful CPA attack on PRESENT-80 one round designed with proposed 2-SPGAL.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.

[5] 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.

[6] 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.

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

[8] 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.

[9] Z. Kahleifeh and H. Thapliyal, "2-phase energy-efficient secure positive feedback adiabatic logic for cpa-resistant iot devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–5.

[10] 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.

[11] 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.

[12] 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.

[13] H. Mahmoodi-Meimand and A. Afzali-Kusha, "Efficient power clock generation for adiabatic logic," in *ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No. 01CH37196)*, vol. 4. IEEE, 2001, pp. 642–645.

[14] 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.

[15] 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.