Adiabatic Logic Based Energy-Efficient Security for Smart Consumer Electronics

Zachary Kahleifeh
University of Kentucky

Himanshu Thapliyal
University of Kentucky

Abstract— **Smart consumer electronic devices are mostly area 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 article, we introduce 2-EE-SPFAL, a 2-phase clocking scheme implementation of an existing adiabatic family known as EE-SPFAL. To show the applicability of 2-EE-SPFAL, we construct a 2-phase clock generator that remains energy efficient and secure. From 100 kHz to 25 MHz, our results show an average energy saving of 76.5% to 21.3% between CMOS and 2-EE-SPFAL. As a case study, we performed a CPA attack on both the CMOS and 2-EE-SPFAL implementation of PRESENT-80 and determined that the CMOS key could be retrieved while the adiabatic key was kept hidden.**

I. Introduction

The arrival of the smart consumer electronics age has led to an increase in the need for energy-efficient hardware design techniques with a parallel focus on the security of these devices [1], [2]. With the growth of smart consumer electronic devices, the potential threat vectors for malicious cyber-attacks are rapidly expanding [3]. Many of these devices communicate and store information and thus are targets for side-channel attacks. Side-channel attacks come in many forms, they can exploit power consumption [4], timing [5], etc. Side-channel attacks are a dangerous threat to consumers' personal information, device reliability, and general well-being. As the smart consumer electronics paradigm emerges, there are challenging requirements to design energy-efficient and secure systems.

Novel computing paradigms such as adiabatic logic are promising to develop low energy and CPA resistant circuits [6]. Adiabatic logic recycles energy to reduce power [7] (Figure 1). Figure 1 illustrates adiabatic logic as a solution to both energy constraints and security concerns. 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) [6]. 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 also 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. From 100 kHz to 25 MHz, our results show an average energy saving of 76.5% to 21.3% between CMOS and 2-EE-SPFAL with clock generator implemented. To demonstrate secure operations, we

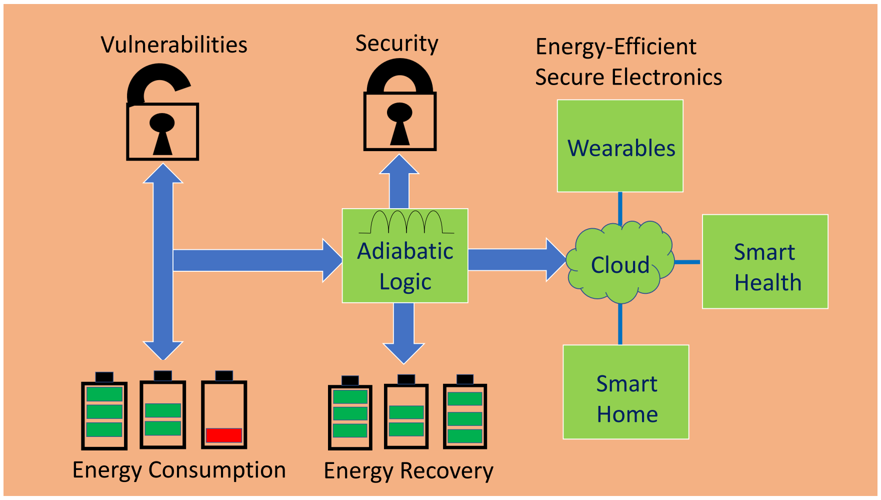


Fig. 1: Adiabatic logic is a potential solution to security and energy needs.

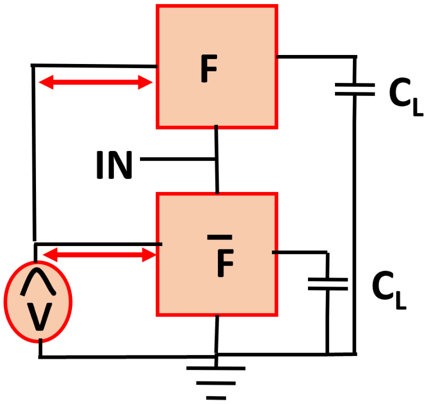


Fig. 2: General structure of adiabatic logic circuits.

also performed a CPA attack on PRESENT. We show that 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 to the 2-EE-SPFAL sinusoidal wave implementation of PRESENT-80.

II. Background on Adiabatic Logic and Correlation Power Analysis

Adiabatic logic is one of the low-power design techniques for designing ultra-low-energy circuits [8]. 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:

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

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 ground). If the charging time $T > 2RC$, then the energy dissipated by an adiabatic circuit is less than a conventional CMOS circuit. Figure 2 illustrates an adiabatic circuit structure and its discharge and recovery.

Side-channel attacks come in many forms, they can exploit power consumption [4], timing [5], etc. Of the power analysis attacks, the Correlation Power Analysis attack (CPA) is widely used because of its robustness towards both symmetric and non-symmetric cryptographic algorithms [9]. CPA attacks look to retrieve otherwise hidden keys by correlating the power of a circuit with a circuit's input.

CPA attacks can be conceptualized by examining Figure 4. Without examining the blocks, one can determine which weight is heavier by looking at the direction of the seesaw. This is similar to examining the power consumption to determine the inputs without actually looking at the inputs. If we instead balance the weights, the seesaw remains stable and thus we cannot determine anything about the blocks, the same can be said if a circuits power consumption is uniform. Similarly, depending on the input of the CMOS circuit a different amount

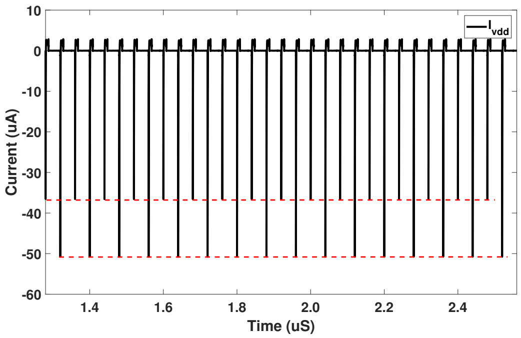


Fig. 3: Uniform current consumption of the 2-EE-SPFAL XOR gate.

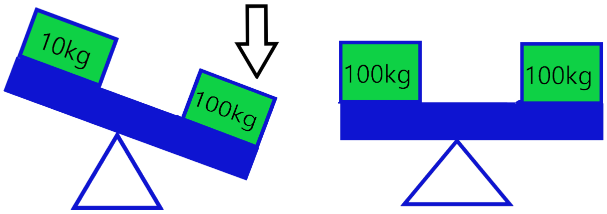


Fig. 4: Abstract illustration of Correlation Power Analysis.

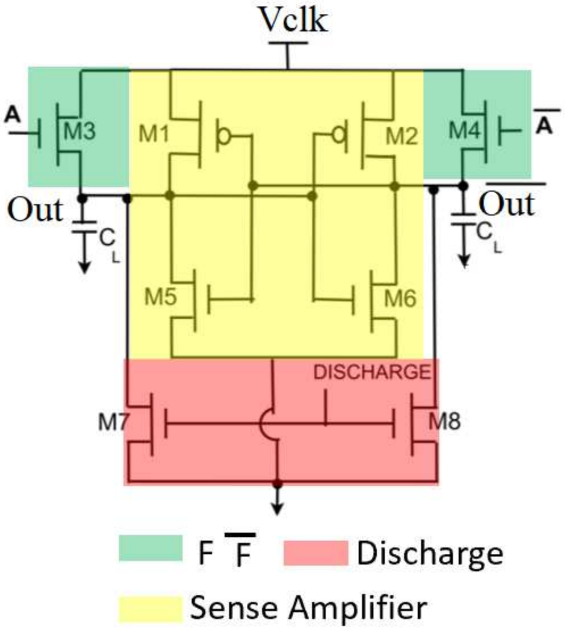


Fig. 5: General structure of 2-EE-SPFAL circuit.

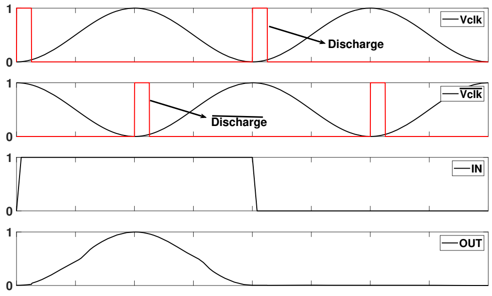


Fig. 6: Proposed 2-phase sinusoidal clocking scheme for 2-EE-SPFAL.

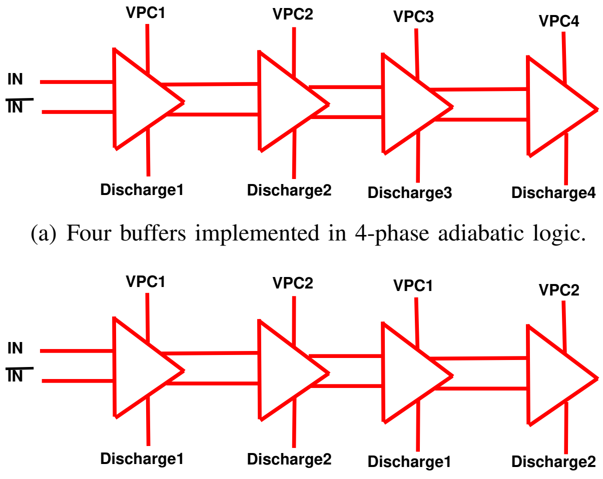
of power is consumed. With this information, an attacker can correlate the power of a cryptographic circuit with the input key. To combat this we look to design our circuits such that the outputs are balanced thus the power consumption is balanced. Uniform power consumption can be examined in Figure 3. Uniform power consumption prevents information leakage and thus keeps a cryptographic circuit secure.

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

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is a recently proposed low energy and CPA resistant logic family [6]. Figure 5 shows the general structure of a 2-EE-SPFAL adiabatic circuit. The structure consists of two balanced evaluation networks. The structure also consists of cross-coupled inverters acting as a sense amplifier. Finally, the discharge transistors are used to reset the output so that the power consumption remains uniform. 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 6 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



(a) Four buffers implemented in 4-phase adiabatic logic.

(b) Four buffers implemented in 2-phase adiabatic logic.

Fig. 7: Design of four buffers using 4-phase clocking and 2-phase clocking.

multiple benefits. Namely, two clocks reduce the amount of area and complexity required to generate the power clock. Take the 4-phase clock generator in [10] and the 2-phase clock generator in [11] 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 7(a) as a case study, in the 4-phase case, eight separate interconnects are required for the circuit to operate correctly while in the 2-phase case only four interconnects are needed.

IV. 2-Phase Adiabatic Power Clock Generator

This section discusses the energy-efficient adiabatic Power Clock Generator (PCG) which is used to operate 2-EE-SPFAL. The PCG uses an external inductor and the load of the adiabatic circuit to generate the waveforms. There are many existing clock generators, for this case study, we have used the 2N-2P synchronous clock generator discussed in [12]. The timing diagram of the controlling external signals is shown in Figure 8. From Figure 8, we developed the novel way for discharge and $\overline{discharge}$ signals to have dual-function: (i) control signals for the clock generator, and (ii) discharge control for the adiabatic logic circuit. The proposed dual-function reduces the number of external signals necessary for operation.

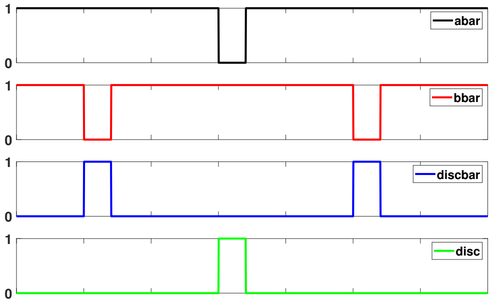


Fig. 8: Synchronous 2N-2P 2-phase clock supporting control signals.

V. Demonstration of 2-EE-SPFAL Security and Energy Efficiency

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.

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. NED and NSD values reported in this paper are calculated with the integration of the power clock generator.

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

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

Parameter	2-EE-SPFAL (NAND)	2-EE-SPFAL (XOR)
$E_{min}(fJ)$	2.94	2.86
$E_{max}(fJ)$	3.02	2.87
$E_{avg}(fJ)$	2.99	2.87
NED (%)	2.6	0.21
NSD (%)	0.75	0.08

lower values of NED and NSD compared to the NAND gate.

From Figure 3, we can observe 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.

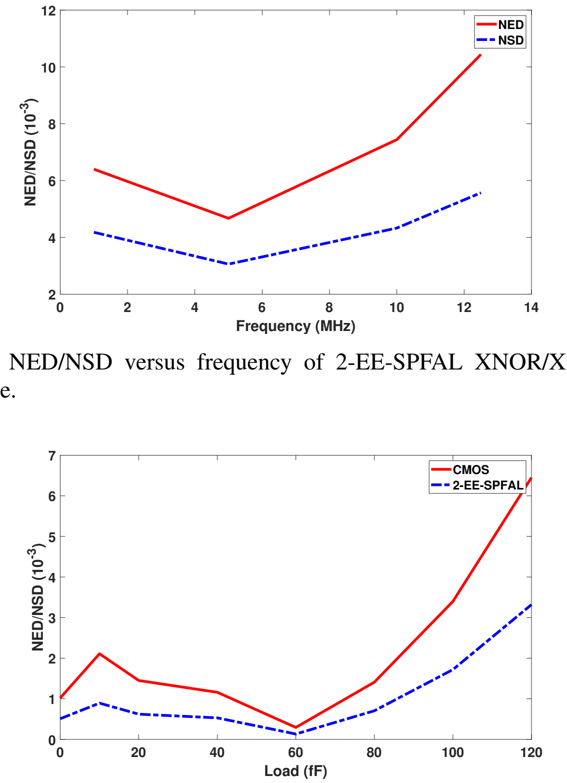
Furthermore, we examined the relationship between NED/NSD, frequency, and output load values. The relationships can be seen in Figures 9(a) and 9(b). We can observe that as frequency increases NED/NSD values also increase. The same relationship can be seen between NED/NSD and load. As the output load surpasses 60 fF the NED/NSD values begin to increase. When designing circuits one should take into consideration these relationships to prevent information leakage.

VI. A Specific Case Study on PRESENT-80

A. PRESENT: A lightweight encryption

PRESENT [13] is a lightweight cipher. PRESENT has low area overhead which makes it an ideal candidate for smart electronic 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 implemented in CMOS is susceptible to side-channel attacks such as Correlation Power Analysis (CPA). Many countermeasures against CPA attacks are not suitable for smart electronic devices as they consume large amounts of power thus we explore to design PRESENT-80 using 2-EE-SPFAL.



(a) NED/NSD versus frequency of 2-EE-SPFAL XNOR/XOR gate.

(b) NED/NSD versus load of 2-EE-SPFAL XNOR/XOR gate.

Fig. 9: Relationship between NED/NSD, frequency, and load for 2-EE-SPFAL XOR/XNOR gate.

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 smart electronic 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 10 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 and an integrated clock generator leads to more secure operation from uniform current consumption as seen in Figure 11. 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

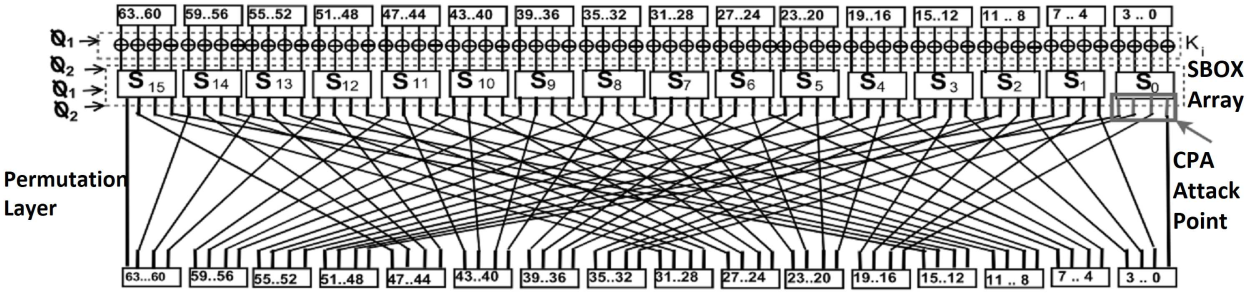


Fig. 10: One round of PRESENT-80 implemented in 2-EE-SPFAL.

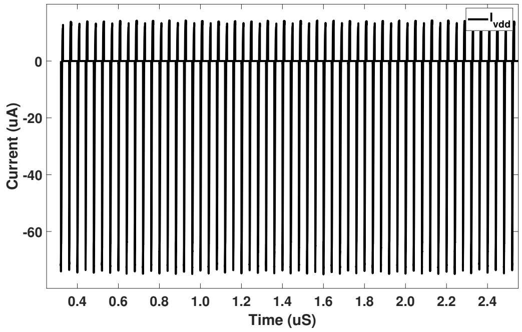


Fig. 11: Uniform current traces of PRESENT-80 implemented with 2-EE-SPFAL and clock generator.

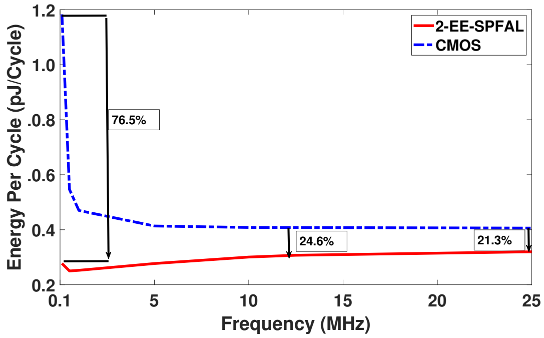


Fig. 12: Energy per cycle of PRESENT-80 implemented in CMOS and 2-EE-SPFAL.

12 and Table II show the energy per cycle of both the CMOS and 2-EE-SPFAL implementation of PRESENT-80 as a function of frequency. From Figure 12 and Table II we can see that when using sinusoidal power clocks, 2-EE-SPFAL consumes less energy than its CMOS counterpart through 25MHz. We can see that at 12.5MHz, there is an average energy saving of 24.67% between CMOS and 2-EE-SPFAL based designs. From 100 kHz to 25 MHz, our results show an average energy saving of 76.5% to 21.3% between CMOS and 2-EE-SPFAL with clock generator implemented.

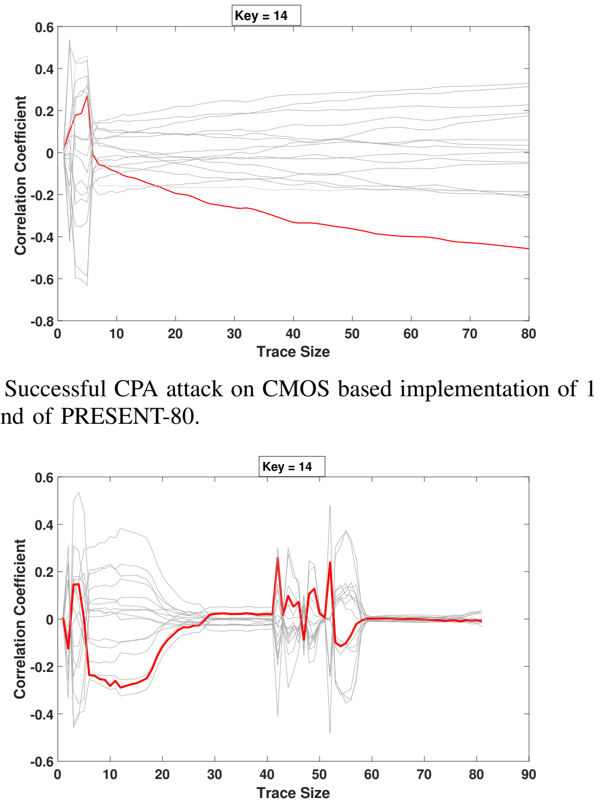
C. CPA Attack on PRESENT-80

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 10). The CPA attack is performed by following the steps described in [14]. The simulation was performed at 12.5MHz with a 100 fF 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 13(a) 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 13(b) 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 smart electronic devices.

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

Energy Per Cycle (pJ)	100kHz	500kHz	1MHz	5MHz	10MHz	12.5MHz	25MHz
CMOS	1.1	0.54	0.46	0.41	0.40	0.40	0.40
2-EE-SPFAL	0.27	0.25	0.25	0.27	0.30	0.30	0.31



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

VII. Conclusion

In this article, we have demonstrated the applicability of secure 2-phase adiabatic logic as a novel computing paradigm to design low energy and secure smart electronic 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.

Acknowledgment

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

References

[1] H. Thapliyal, “Internet of things-based consumer electronics: Reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 66–67, 2018.

[2] M. Alioto and M. Shahghasemi, “The internet of things on its edge: Trends toward its tipping point,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 77–87, 2018.

[3] J. Park and A. Tyagi, “Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly.” *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 92–102, 2017.

[4] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proc. 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 *Proc. International Conference on Smart Card Research and Advanced Applications*, 1998, pp. 167–182.

[6] 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.

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

[8] 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.

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

[10] J. Hu, W. Zhang, X. Ye, and Y. Xia, “Low power adiabatic logic circuits with feedback structure using three-phase power supply,” in *Proc. 2005 International Conference on Communications, Circuits and Systems, 2005.*, 2005.

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

[12] H. Mahmoodi-Meimand and A. Afzali-Kusha, "Efficient power clock generation for adiabatic logic," in *Proc. IEEE International Symposium on Circuits and Systems*, 2001, pp. 642–645.

[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 *Proc. International workshop on cryptographic hardware and embedded systems*, 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.

About the Authors

Zachary Kahleifeh is currently pursuing his PhD in Electrical and Computer Engineering at the University of Kentucky, Lexington, KY, USA. Contact him at zachary.kahleifeh@uky.edu.

Himanshu Thapliyal is an Associate Professor and Endowed Robley D. Evans Faculty Fellow with the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. Contact him at hthapliyal@uky.edu.