2-Phase Adiabatic Logic For Low-Energy and CPA-Resistant Implantable Medical Devices

Amit Degada, Himanshu Thapliyal, *Senior Member, IEEE*

Abstract*—Designing a low-energy and secure lightweight cryptographic coprocessor is the primary design constraint for modern wireless Implantable Medical Devices (IMDs). The lightweight cryptographic ciphers are the preferred cryptographic solution for low-energy encryption. This article proposes 2-SPGAL, the 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL) for IMDs. The proposed 2-SPGAL is energy-efficient and secure against the Correlation Power Analysis (CPA) attack. The proposed 2-SPGAL was evaluated with the integration of synchronous resonant Power Clock Generators (PCGs): (i) 2N2P-PCG, and (ii) 2N-PCG. The case study implementation of one round of PRESENT-80 encryption using 2-SPGAL, with 2N2P-PCG integrated into the design, shows an average of 47.50% of energy saving compared to its CMOS counterpart, over the frequency range of 50 kHz to 250 kHz. The same 2-SPGAL based case study, with 2N-PCG integrated into the design, shows 51.18% of an average energy saving compared to its CMOS counterpart, over 50 kHz to 250 kHz. Further, the 2-SPGAL based PRESENT-80 one round shows an average energy saving of 16.62% and 28.90% respectively for 2N2P-PCG and 2N-PCG integrated into the design compared to existing 2-phase adiabatic logic called 2-EE-SPFAL. We also subjected PRESENT-80 design of 2-SPGAL and CMOS against CPA attack. The 2-SPGAL, with 2N2P-PCG and 2N-PCG, integrated into one round of PRESENT-80 design protects the encryption key. However, the encryption key was successfully revealed in one round of PRESENT-80 design using CMOS logic. Therefore, the proposed 2-SPGAL logic can be useful to design energy-efficient and CPA resilient Implantable Medical Devices (IMDs).

***Index Terms*—Implantable medical device, hardware security, adiabatic logic, power clock generators, side-channel attacks, correlation power analysis attack, cryptographic circuits.**

I. Introduction

The Implantable Medical Devices (IMDs) perform sensing of body signals, decision-making computation, and executing actuation tasks to assist chronic or long-term therapeutic procedures. Some examples of the IMD application include pace-makers, drug delivery systems, implantable cardiac defibrillators (ICDs), and neurotransmitters. The IMDs help to improve physiological functions, therefore, they are included in many new therapies to improve the quality of life. IMDs are often surgically placed inside the human body (Figure 1). Modern IMDs employ wireless technology that allows the patient to roam freely while receiving remote monitoring and treatments [1].

Amit Degada is currently PhD candidate in the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY 40506, USA.

Himanshu Thapliyal is currently with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA. (e-mail: hthapliyal@ieee.org).

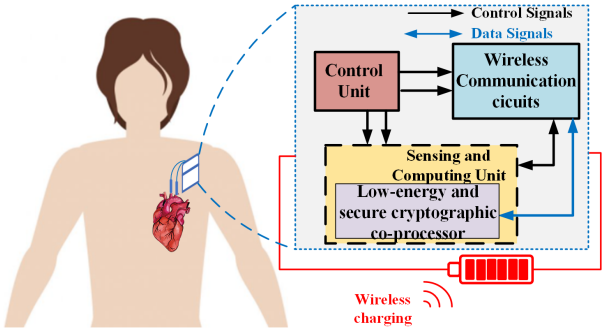


Fig. 1: Modern IMD requires low-energy consumption and secure communication.

However, the inclusion of wireless technology makes IMDs dissipating more energy. So, it becomes very important that modern IMDs should have low-energy consumption to extend the longevity of the battery. On the other hand, wireless access to IMDs has given rise to many cyber threats. In recent years, researchers have shown that compromised IMD can be exploited to send the unauthorized data and commands [2], unwarranted electric shock [3], [4] and deplete the battery [5]. Security compromise can be fatal and has become a primary design constraint for IMDs. To address the challenge to meet energy budget, security and privacy requirements for IMDs, many researchers have proposed the inclusion of low-energy encryption using Lightweight Cryptographic (LWC) ciphers [6], [7], [8]. These LWC ciphers could be vulnerable to Side-Channel Analysis (SCA) attacks, e.g. heat emission, electromagnetic radiation, power analysis [9], [10], and timing attacks [11]. The researchers in [12] have listed real and hypothetical SCA attacks possible over various IMD devices. Further, among different SCAs, the Correlation Power Analysis (CPA) attack is relatively simpler to implement and highly successful.

The adiabatic logic is a low-power circuit design technique that recovers the charge stored inside the load capacitors, and thus reduces the significant energy consumption compared to the conventional CMOS logic. The physiological signals of human bodies are typically low-frequency values [13], [14], [15]. Conventional ultra-low-power medical devices and operate over tens to a few hundred kilohertz of the frequency range. As adiabatic logic operates energy efficiently at low frequency, therefore in this work, we proposed to design low-energy and secure cryptographic co-processors based on adiabatic logic. Further, the adiabatic logic circuits have uniform power traces, thereby "hides" the information leakages. Therefore,

the proposed LWC circuit based on adiabatic logic will be resilient against the CPA attacks. To validate our hypothesis, we present a novel 2-phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) and use it to design a low-energy and CPA resistant design of LWC PRESENT. The energy and CPA resilient capability of the adiabatic logic circuit largely depends upon the design of the power clock generator (PCG) [16], [17], [18], [19]. The PCG consumes a large fraction of the energy consumption, and its poor design can also affect security resilience. In this work, we evaluate the energy and security metrics of the proposed 2-SPGAL with two different synchronous resonant sinusoidal PCGs: 2N2P-PCG and 2N-PCG (Refer Section IV).

A. Key Contributions from this work

The key contributions of this work are as follows:

- The article presents 2-SPGAL, a novel 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). The proposed 2-SPGAL can be a design choice for low-energy and CPA-resistant IMDs.
- The energy and security of the adiabatic logic largely depend upon the PCG integrated into the design. Therefore, we evaluated the energy efficiency and CPA-resistance of the proposed 2-SPGAL with two different types of synchronous resonant Power Clock Generators (PCGs). Two types of PCGs are 2N2P-PCG and 2N-PCGs.
- The logic gates, AND/NAND and XOR/XNOR gates of 2-SPGAL are evaluated in terms of energy and security metrics with 2N2P-PCG and 2N-PCG integrated into the design.
- The one round of PRESENT-80 designed using proposed 2-SPGAL with 2N-PCG integrated into the design, shows an average of 47.50% energy saving compared to its CMOS counterpart design for the frequency range of 50 kHz to 250 kHz. The same design implemented with 2N2P-PCG integrated into the design shows an average of 51.18% energy saving compared to its CMOS counterpart over the frequency range of 50 kHz to 250 kHz.
- The one round of PRESENT-80 designed using 2-SPGAL with 2N2P-PCG integrated into design shows an average of 16.62% energy-saving compared to existing 2-phase adiabatic logic 2-EE-SPFAL [20]. Similarly, 2N-PCG integrated into the design shows an average energy saving of approximately 29% compared to 2-EE-SPFAL [20].
- The output of the PRESENT-80 S-box is considered as the attack point in literature. Its CPA resilience capability is measured in Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) metrics. The 2-SPGAL based S-box with 2N-PCG integrated show an average improvement of 95.86% and 99.34% in NED and NSD values respectively, compared to its CMOS counterpart over the frequency range of 50 kHz to 250 kHz. Similarly, 2N2P-PCG integrated into 2-SPGAL based S-box shows an average improvement of 94.07% and 99.16% improvement in NED and NSD values compared to the CMOS S-box over the frequency range of 50 kHz to 250 kHz.
- We demonstrate that the PRESENT-80 using novel 2-SPGAL can successfully defend the encryption key against the CPA attack for both 2N2P-PCG and 2N-PCG integrated with the design. However, the encryption key is revealed in the same counterpart design using CMOS.

B. Organization of the paper

The article is organized as follows: In Section II, the background of adiabatic logic and the security evaluation metrics are explained. Section III illustrates the proposed 2-phase implementation of SPGAL. The PCG design and its external control signals for synchronization are explained in Section IV. The energy and security performance of proposed 2-SPGAL logic gate is presented in Section V. The case-study design of one round of PRESENT-80 encryption, and its energy-efficiency comparison with CMOS and 2-EE-SPFAL based counterpart is discussed in Section VI. The energy performance and security evaluation of PRESENT-80 S-box is discussed in Section VII. Section VIII discusses the CPA attack on CMOS and proposed 2-SPGAL based PRESENT-80 encryption circuit. Section IX concludes the paper.

II. Background

The countermeasure against power analysis attacks (e.g. CPA attack) can be classified as masking [10], random instruction injection [21], non-deterministic processors [22], random register renaming [23], secure co-processors [24], and cell-level countermeasures [25]. In cell-level countermeasure, e.g. adiabatic logic, the focus is on designing logic gates with uniform power traces. Further, the charge recovery operation makes adiabatic logic an attractive design choice for energy-efficient and CPA-resistant IMDs. The objective of this section is to give the background adiabatic logic. Additionally, the commonly used metrics in literature to evaluate the security of the cryptographic hardware are discussed.

A. Adiabatic logic

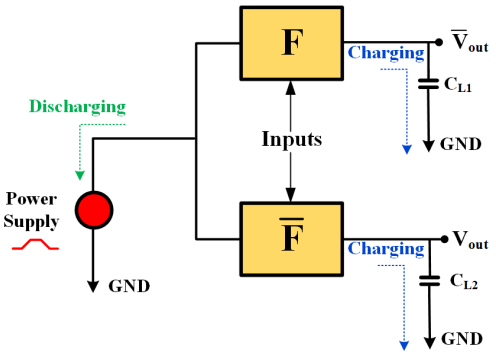


Fig. 2: Charging and discharging in adiabatic circuits [26].

To reduce the energy consumption, the adiabatic logic design technique recycles the energy stored in capacitive load back to the power clock circuit. The capacitive load is charged using the constant current source, rather than the conventional approach to use the constant voltage [27]. The constant current

source is practically achieved by a ramp referred to as a power clock. The generalized switching model, charging and the discharging path of the adiabatic logic is shown in Figure 2.

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

Equation 1 shows the energy consumption in adiabatic logic circuits. In equation 1, T is charging or discharging time-period, load capacitor C, adiabatic logic-based circuit resistance R, and V_{dd} is the full-swing voltage of power clocking signal. Equation 1 helps to understand that adiabatic circuitry has significantly low energy consumption for low-frequency operations compared to standard CMOS.

B. Evaluation metrics for CPA-Resistance

The CPA has proven its success, and its widely used by malicious cyber attackers against, both asymmetric and symmetric cryptographic algorithms [28]. The adiabatic logic maintains the uniform current traces. The benefit of the adiabatic logic should be evaluated by its ability to withstand the CPA. The common metric used to check the robustness of the hardware against CPA are Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) [26] [29] [30] [31] [32] [33].

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

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

The NED value is the difference between the maximum and minimum energy consumption for all possible input combinations. NSD is the deviation of the instantaneous energy to the average energy consumption. Lower NED and NSD value shows that the hardware is less exploitable to the CPA. For the success of the CPA attack, the hypothetical power model (calculated based on hamming weight) should be linearly proportional to actual side-channel leakages. Thus, less deviation in power traces makes it difficult to reveal the encryption keys.

III. Proposed 2-Phase Adiabatic Logic Design

The Symmetric Pass Gate Adiabatic Logic (SPGAL) logic gate structure (Figure 3) consists of three blocks: a sense amplifier, a discharge circuitry, and logic evaluation blocks. The PMOS transistors M1, and M2 construct the sense amplifier/latch. The discharge signal turns the nmos transistor M3, and M4 to ON, and provides a discharge patch for residue charge stored in the load capacitor. The evaluation block transistors produce correct logic gate output based on input logic signals. The SPGAL was originally proposed on a 4-Phase trapezoidal clocking scheme [26].

In this work, we hypothesize that the slow varying sinusoidal signal (Figure 4) can be a potential replacement for the trapezoidal clock. To check our hypothesis, the discharge

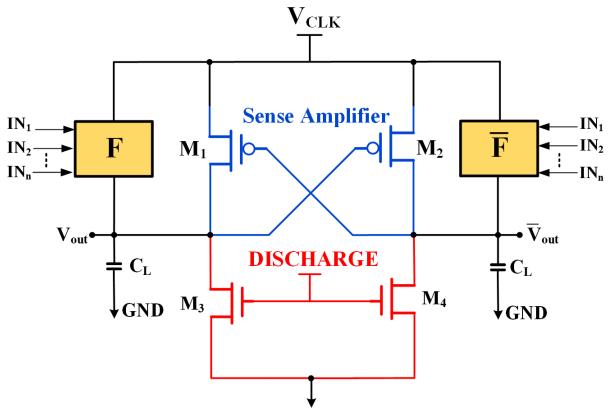


Fig. 3: General SPGAL logic gate structure [26].

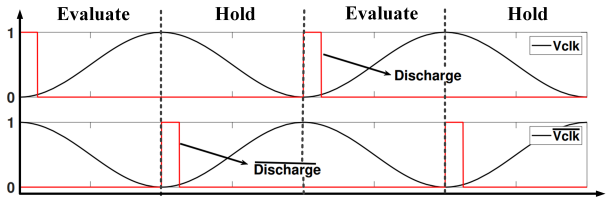


Fig. 4: Sinusoidal clocking idea [20], [34].

signal is adjusted to the negative peak of the sinusoidal signal. The rising part of the sinusoidal signal is referred to as evaluate and the falling part is referred to as the recovery phase of the adiabatic operations. The two discharge signals are synchronous to the negative pick of the respective phase. The above 2-phase sinusoidal clocking implementation of SPGAL is referred to as 2-SPGAL. The adiabatic logic circuits operate in pipelined fashions. It was found (Figure 5) that the 2-phase sinusoidal clocking allows using two out-of-phase power clocks and discharge signals to operate a 4-cascaded 2-SPGAL buffer logic gate.

IV. Sinusoidal Power Clock Generator for 2-Phase Adiabatic Circuits

The objective of this section is to discuss the design of the energy-efficient Power Clock Generator (PCG) for 2-SPGAL operation. The adiabatic system usually consists of PCG and logic circuitry. The PCG supplies the power clock for adiabatic circuit operation, and the stored charge is recovered back to PCG. The poor design of the PCG can result in non-efficient adiabatic operation and less energy saving. Therefore, the

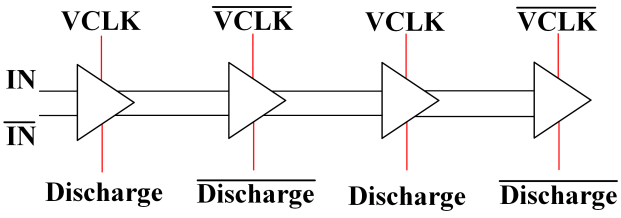
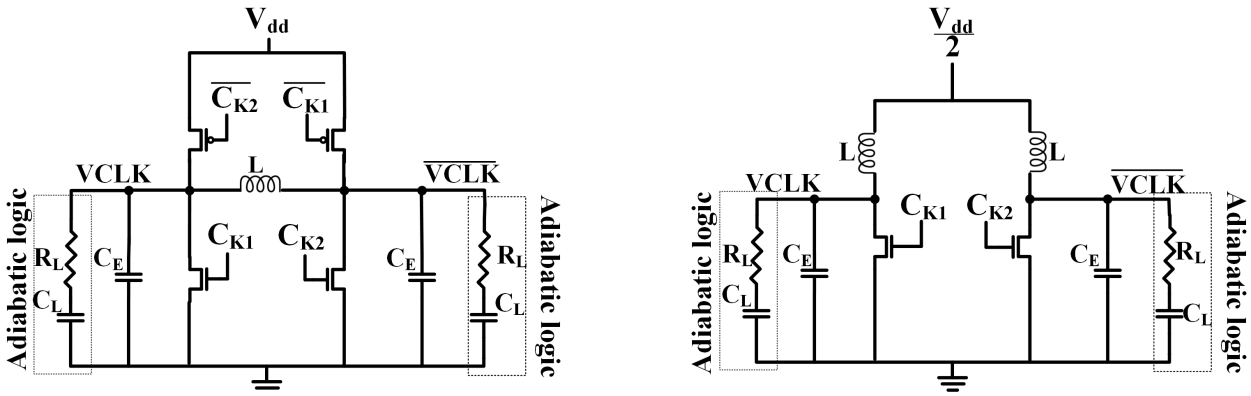


Fig. 5: Four cascaded adiabatic buffers implemented in cascade using 2-phase clocking scheme [20], [34].



(a) 2N2P-PCG. (b) 2N-PCG

Fig. 6: Synchronous PCG circuits [35].

energy and CPA resilient capability of the adiabatic system needs to be evaluated with PCGs integrated in design.

The PCGs are broadly classified in step-wise charging PCG and resonant clock generators. The oscillator-based resonant generator can recover the charge stored in the load capacitor back to the inductor. Further, the higher power conversion efficiency makes it more suitable for the adiabatic logic operation. The synchronous resonant are found to be more energy-efficient, and its example includes 2N-PCG and 2N2P-PCG [35]. The circuit diagram for 2N-PCG and 2N2P-PCG is shown in Figure 6. The 2N-PCG has two NMOS transistors, hence, referred to as 2N-PCG. The two inductors of the same value are interfaced with dc voltage equal to half of the full-swing voltage required. Similarly, 2N2P-PCG has two PMOS and two NMOS transistors. 2N2P-PCG requires only one inductor, and dc supply equal to full-swing voltage.

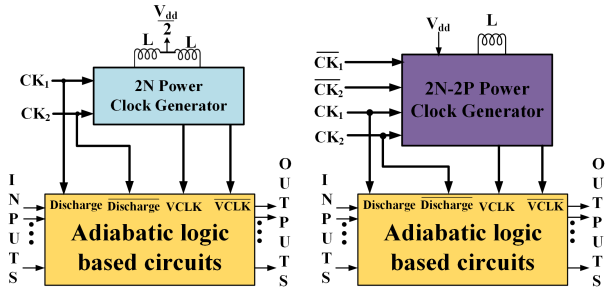


Fig. 7: PCG interfacing with 2-SPGAL based circuits.

The schematic to interface the proposed 2-SPGAL logic-based circuitry with synchronous PCGs is shown in Figure 7. The synchronous resonant PCG uses an external time-base signal. The external time-base signal allows adiabatic circuitry to synchronous with other non-adiabatic circuits in a larger system. The differential operation of the adiabatic logic makes the lumped capacitance value independent of the frequency of the operation. Thus, the change of frequency operation can be achieved by varying the external inductor value.

The timing diagram of the external control signal is shown in Figure 8. The two external control signals CK_1 and CK_2 are out-of-phase with each other. On the other hand, the

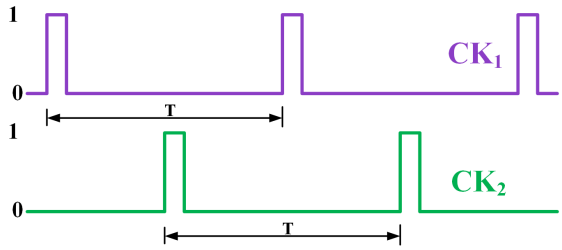


Fig. 8: Control signals in 2-Phase PCG design [35].

$Discharge$ and $\overline{Discharge}$ signals are out-of-phase. From Figure 8, we propose a novel way to use external time-base signals as control signals for PCG, and discharge signals for the adiabatic logic circuit. The proposed methodology helps to reduce the number of control signals for the adiabatic system.

V. Energy and Security Evaluation of 2-SPGAL Logic Gates

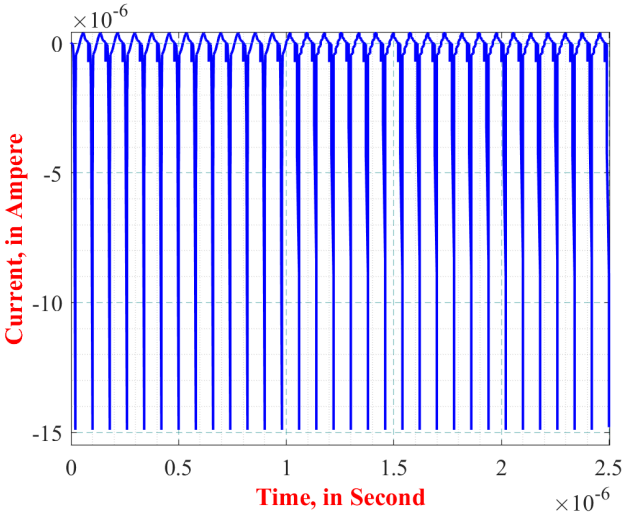


Fig. 9: Uniform current in 2-SPGAL Ex-OR logic gate.

The next step is to check the energy and security evaluation of 2-SPGAL gates at different frequencies with PCG integrated

into the design. For an ideal secure circuit, the variation in energy consumption should be zero for all possible input variations. In a practical scenario, the lower variation in energy consumption comes from a smaller variation in current traces. Further, the CPA estimates the correlation between the leakage power and mathematical hypothetical power models. Hence, the success of CPA depends upon the linear dependency between the hypothetical power traces and collected power traces. The above linear dependency can be disguised if we have uniform current traces. Figure 9 shows the current traces for XOR gates as an example. It can be observed that current traces 2-SPGAL based logic gates are uniform.

We performed the SPICE simulation to collect the energy consumption value for all possible input bit variations. For example, an n-bit circuit will have a total 2^{2n} possible cyclic variations. The NED and NSD metrics at different frequencies can give an idea about the security resilience of the 2-SPGAL gates against CPA attack. The smaller the NED and NSD values imply the more robustness against the CPA attack. They are calculated based on energy consumption in circuit for different input bit combinations. On the other hand, the energy and security evaluation of the adiabatic logic circuit largely depends upon the types of PCG integrated. Thereby, the energy and security metric of the logic gates should be compared with PCG integrated into the design.

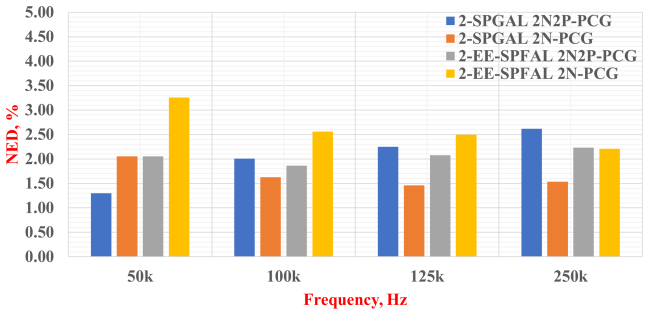


Fig. 10: NED value comparison for AND logic gate.

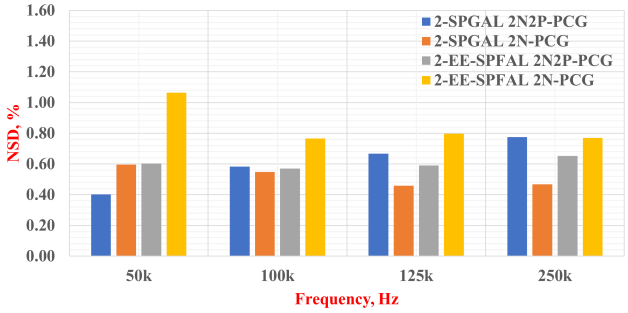


Fig. 11: NSD value comparison for AND logic gate.

Table I lists the simulation results for the proposed 2-SPGAL and the existing 2-EE-SPFAL [20] AND/NAND logic gate with 2N2P-PCG and 2N-PCG integrated into the design. Among the four different designed listed in Table I, 2-SPGAL AND/NAND logic gate with 2N-PCG integrated into the design has superior performance. It has an average NED and NSD value of 1.669 and 0.518 respectively over the frequency range of 50 kHz to 250 kHz. The 2-SPGAL AND/NAND logic gate with 2N2P-PCG integrated into the design, has an average NED and NSD metric value of 2.043 and 0.607. The average NED and NSD values for 2-EE-SPFAL [20] AND/NAND logic gate with 2N2P-PCG integrated into the design are 2.055 and 0.604 respectively, over the frequency range of 50 kHz to 250 kHz. The 2-SPGAL AND/NAND logic gate has identical CPA resilience capability with 2N2P-PCG integrated into the design compared to the 2-EE-SPFAL [20] counterpart. Further, the 2-SPGAL AND logic gate shows superior CPA resilience capability for 2N-PCG integrated into the design compared to 2-EE-SPFAL [20] AND/NAND logic gate counterpart.

TABLE I: Energy-efficiency and security evaluation of the 2-phase AND logic gate with 2N-PCG and 2N2P-PCG.

Proposed 2-SPGAL AND Logic Gate								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	9.18	11.25	11.15	9.00	11.11	9.00	11.16	8.97
$E_{max}(fJ)$	9.30	11.49	11.38	9.15	11.37	9.13	11.46	9.11
$E_{avg}(fJ)$	9.24	11.40	11.29	9.09	11.28	9.08	11.35	9.05
NED (%)	1.300	2.050	2.008	1.629	2.246	1.461	2.616	1.534
NSD (%)	0.402	0.596	0.583	0.548	0.667	0.459	0.776	0.467
2-EE-SPFAL AND Logic Gate [20]								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	11.86	7.40	11.75	5.18	11.70	5.40	11.76	6.28
$E_{max}(fJ)$	12.10	7.65	11.98	5.32	11.94	5.54	12.03	6.43
$E_{avg}(fJ)$	12.02	7.50	11.89	5.26	11.86	5.48	11.94	6.37
NED (%)	2.052	3.258	1.862	2.558	2.073	2.497	2.231	2.211
NSD (%)	0.603	1.064	0.571	0.766	0.589	0.798	0.652	0.769

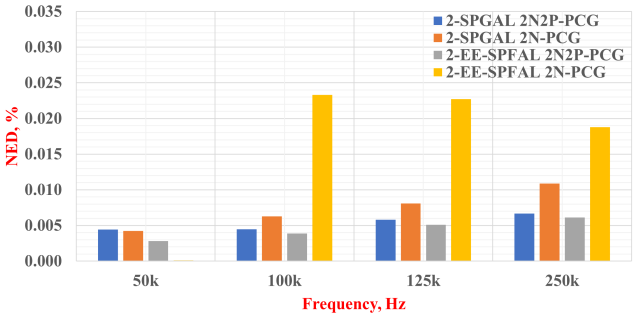


Fig. 12: NED value comparison for XOR logic gate.

Similar to AND/NAND logic gate, we performed the simulation to collect energy numbers for the proposed 2-SPGAL XOR logic gate and 2-EE-SPFAL [20] XOR/XNOR logic gate with 2N2P-PCG, and 2N-PCG integrated into the design. Table II shows energy and security metrics comparison for proposed 2-SPGAL XOR/XNOR gate with 2-EE-SPFAL XOR/XNOR logic gate [20]. The 2-SPGAL XOR/XNOR logic gate has an average NED and NSD values almost equal to zero like its 2-EE-SPFAL [20] counterpart with PCGs integrated into the design. This property is accounted for the balance of inputs on logic evaluation blocks. This results in a more symmetrically built load capacitance value. It results in equal switching activities of the XOR gate, thereby, more uniform power traces, therefore, almost ideal NED and NSD metric values.

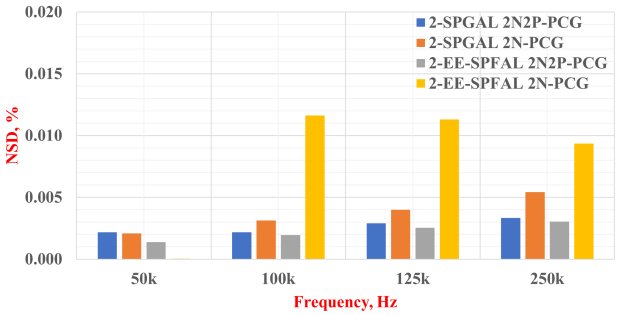


Fig. 13: NSD value comparison for XOR logic gate.

TABLE II: Energy-efficiency and security evaluation of 2-phase XOR logic gate with 2N-PCG and 2N2P-PCG.

2-SPGAL XOR Logic Gate								
	50 kHz		100 kHz		125 kHz		250 kHz	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	11.10	9.04	11.02	8.87	10.99	8.89	11.06	8.87
$E_{max}(fJ)$	11.11	9.04	11.02	8.87	10.99	8.89	11.06	8.87
$E_{avg}(fJ)$	11.10	9.04	11.02	8.87	10.99	8.89	11.06	8.87
NED (%)	0.0044	0.0042	0.004	0.006	0.006	0.008	0.007	0.011
NSD (%)	0.0022	0.0021	0.002	0.0036	0.003	0.004	0.004	0.005
2-EE-SPFAL XOR Logic Gate [20]								
	50 kHz		100 kHz		125 kHz		250 kHz	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	11.71	7.62	11.58	5.19	11.56	5.36	11.63	6.19
$E_{max}(fJ)$	11.71	7.62	11.58	5.19	11.57	5.37	11.63	6.19
$E_{avg}(fJ)$	11.71	7.62	11.58	5.19	11.56	5.36	11.63	6.19
NED (%)	0.0028	0.0001	0.004	0.023	0.005	0.023	0.006	0.019
NSD (%)	0.0014	0.0000	0.002	0.0012	0.003	0.011	0.003	0.009

VI. Case Study - PRESENT-80 One Round of Encryption Design Using 2-SPGAL

In this section, we illustrate the design of the PRESENT, a lightweight cryptographic cipher. The PRESENT is a simple, secure, and energy-efficient block cipher. The PRESENT block cipher is particularly suitable to the application which does not require large data to be encrypted, e.g. IMDs, RFID, IoT. The proposed 2-SPGAL can be a potential logic design option to design energy-efficient and secure IMDs.

A. PRESENT-80

The cryptographic circuits of the IMD should be low-energy as they operate in a limited battery budget. The PRESENT was originally proposed in [36] and recently received higher attention from the researchers due to its ability to meet low-energy encryption. Further, the counter mode operation of PRESENT enables its usage in challenge-response authentication protocols [37]. The PRESENT-80 comes up with two variants depending upon the size of the key, 80-bit, and 120-bit. The PRESENT-80 is 32-round of encryption, and out of which 31 rounds are identical. Therefore, we implemented one round of PRESENT-80 encryption using the proposed 2-SPGAL.

Figure 14 shows the schematic of the case-study design of PRESENT-80 one round of encryption. The PRESENT-80 design has three fundamental operations. During addRoundKey operation the XOR operation of the plain-text is done with the key. The Substitution-box (S-box) does the non-linear transformation in 4-bit chunks, with a total of 16 in parallel. The third operation is the permutation of the S-box output to add further randomization [36].

TABLE III: Number of Transistor Required to implement PRESENT-80 one round [34].

Adiabatic Logic	**2-EE-SPFAL [20]**	**Proposed 2-SPGAL**
Number of Transistor	9344	7776
2-SPGAL saves 16.78% transistor to its counterpart 2-EE-SPFAL [20]		

Table III lists the total number of transistors required to implement using proposed 2-SPGAL and 2-EE-SPFAL [20]. The SPGAL has two fewer transistors in its sense-amplifier structure of the gate. The 2-SPGAL based design requires 7776 transistors, while its counterpart designed using 2-EE-SPFAL needs 9344 transistors. This results in 16.78% fewer transistors in 2-SPGAL design compared to 2-EE-SPFAL [20]. The less number of transistors and simpler power clock routing can result meet the smaller layout and are the requirement for consumer IoT devices.

B. Energy-Efficiency comparison

$$E = \int_0^T V_P I_P dt \tag{4}$$

The energy consumption is the integration of the voltage and current product over the time period of the input signal. The $V_{\rm p}$ is voltage and $I_{\rm p}$ is the current from PCG or power supply [38]. We show the comparison of the average energy consumption for the one round of PRESENT-80 at 45nm technology with 10 fF load using (i) Proposed 2-SPGAL with 2N-PCG, and (ii) Proposed 2-SPGAL with 2N2P-PCG, (iii) 2-EE-SPFAL [20] with 2N-PCG, (iv) 2-EE-SPFAL [20] with 2N2P-PCG and (iv) conventional CMOS design. The cryptographic circuits are presented for low-frequency IMD devices, and therefore the frequency range of 50 kHz to 250 kHz is considered in this work.

The energy consumption is measured in terms of energy per cycle, i.e. average energy consumption value over all possible combinations of inputs [20]. Lower the energy per cycle value means better energy performance, and thus can be useful to design energy-saving IMDs. The energy per cycle for one round of PRESENT-80 designed using 2-SPGAL, 2-EE-SPFAL [20], and CMOS is shown in Table IV. The proposed 2-SPGAL logic base one round of PRESENT-80 shows overall superior performance compared to their CMOS and 2-EE-SPFAL counterparts for every frequency in the range of 50 kHz to 250 kHz. The average energy consumption (i.e. average energy for the frequency range 50 kHz to 250 kHz) for 2-SPGAL 0.727 pJ/Cycle and 0.785 pJ/Cycle respectively for 2N2P-PCG, and 2N-PCG integrated into the design. The same counterpart designed using 2-EE-SPFAL has an average energy consumption of 0.872 pJ/Cycle and 1.121 pJ/Cycle respectively with 2N2P-PCG, and 2N-PCG integrated into the design. Further, it can also be observed that for 2N-PCG integrated into the design, the 2-SPGAL based case

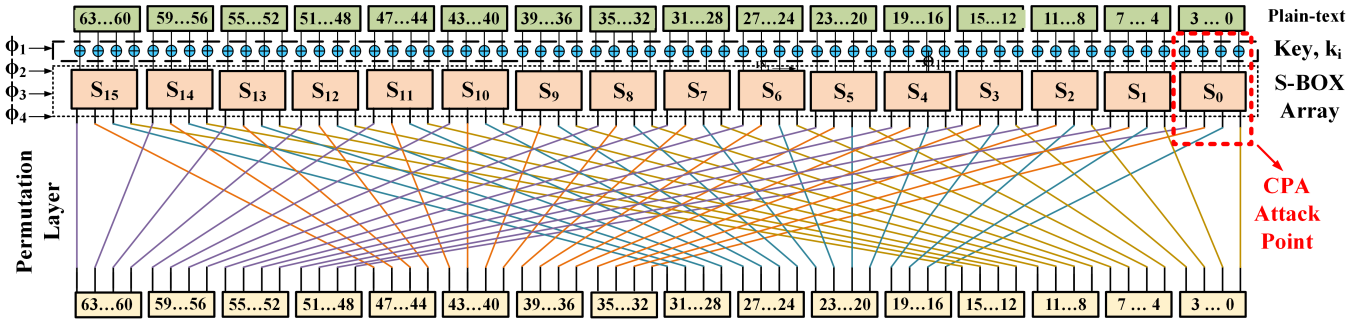


Fig. 14: one round of PRESENT-80 implementation using 2-phase adiabatic logic.

TABLE IV: Energy consumption (in pJ/cycle) in case study of one round of PRESENT-80 encryption.

Logic used to design case study	PCG integrated in design	50 kHz	100 kHz	125 kHz	250 kHz	Average
CMOS	–	2.376	1.569	1.409	1.092	**1.611**
2-EE-SPFAL [20]	2N-PCG	1.250	1.257	1.066	0.913	**1.121**
	2N2P-PCG	0.848	0.895	0.870	0.878	**0.872**
Proposed 2-SPGAL	2N-PCG	0.795	0.795	0.787	0.764	**0.785**
	2N2P-PCG	0.725	0.728	0728	0.728	**0.727**

TABLE V: Energy saving (in %) comparison in proposed 2-SPGAL based one round of PRESENT-80 encryption.

PCG integrated in 2-SPGAL design	Baseline Logic to compare case study implementation	50 kHz	100 kHz	125 kHz	250 kHz	Average
2N-PCG	2-EE-SPFAL [20]	36.40	36.76	26.13	16.32	**28.90**
	CMOS	66.54	49.32	44.10	30.05	**47.50**
2N2P-PCG	2-EE-SPFAL [20]	14.47	18.66	16.31	17.02	**16.62**
	CMOS	69.49	53.39	48.31	33.31	**51.18**

study implementation has approximately 30% less average energy consumption (in pJ/Cycle) compared to its 2-EE-SPFAL counterpart. Thus, for 2N-PCG integration into the design, the proposed 2-SPGAL can result in more energy saving compared to 2-EE-SPFAL. On the other hand, the CMOS-based one round of PRESENT-80 encryption design has an average energy consumption of 1.611 pJ/Cycle, the highest among five different circuits compared.

Table V lists the energy-saving (in%) value in 2-SPGAL based one round of PRESENT-80 implementation compared to its CMOS and 2-EE-SPFAL based counterpart designs. The energy-saving in 2-phase adiabatic logic are compared for the same type of PCG integrated into the design. on the other hand, the CMOS-based counterpart is implemented over DC voltage. The proposed 2-SPGAL based counterpart shows an average of 16.62% and 28.90% of energy-saving respectively with 2N2P-PCG and 2N-PCG integrated into the design, compared to its 2-EE-SPFAL counterpart. Therefore, the 2-SPGAL saves overall more energy compared to other 2-phase adiabatic logic 2-EE-SPFAL [20]. Similarly, we can see an average of 47.50% and 51.18% energy saving, with 2N-PCG and 2N2P-PCG integrated into 2-SPGAL design compared to CMOS based case-study implementation. Saving close to 50% of energy can help to increase IMD device lifetime substantially.

VII. Energy and Security Evaluation of PRESENT-80 S-box Design

In Section V, the 2-SPGAL based logic gates were shown promising results for the NED, and NSD metrics. The CPA attack collects the power traces at the output of the S-box, thereby it is a vital component of the PRESENT-80 design. We implemented the S-box design using the proposed 2-SPGAL, 2-EE-SPFAL [20], and CMOS logic gates. The S-box implementation requires both ϕ_1, and ϕ_2 phases (Figure 14) of power clock to operate. The S-box designs using adiabatic logic were tested for two PCGs: 2N-PCG and 2N2P-PCG.

Table VI shows the summary of energy consumption values and security metrics (NED and NSD) for the 2-SPGAL and 2-EE-SPFAL [20] based S-box with 2N2P-PCG and 2N-PCG integrated with the design. Similar to logic gates, we collected energy numbers for all possible input combinations for the frequency range 50 kHz to 250 kHz at 45nm technology with the load value of 10 fF. It can be observed, in Table VI that energy consumption in 2-SPGAL with 2N-PCG integrated design shows superior energy consumption value, with an average value of 48.49 fJ at all frequencies in consideration. The next better energy consumption for S-box is observed for 2-SPGAL with 2N2P-PCG integrated with design with an average value of 80.18 fJ.

Figure 15 and 16 shows the comparison of NED and NSD value for S-box designed using proposed 2-SPGAL, 2-EE-

TABLE VI: Energy-efficiency and security evaluation of PRESENT-80 S-box design using 2-phase adiabatic logic.

S-box design using 2-SPGAL logic gates								
	50 kHz		100 kHz		125 kHz		250 kHz	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	80.08	50.69	78.38	47.64	78.18	46.94	77.65	45.45
$E_{max}(fJ)$	84.09	52.57	84.51	49.67	83.00	49.04	82.49	47.64
$E_{avg}(fJ)$	81.48	51.38	80.04	48.42	79.82	47.78	79.39	46.41
NED (%)	4.78	3.59	7.25	4.08	5.81	4.27	5.86	4.60
NSD (%)	0.96	0.74	1.18	0.89	1.19	0.92	1.20	0.98
S-box design using 2-EE-SPFAL logic gates [20]								
	50 kHz		100 kHz		125 kHz		250 kHz	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{min}(fJ)$	111.87	3654.23	106.79	1050.03	105.81	750.94	103.21	247.59
$E_{max}(fJ)$	120.24	3971.60	114.36	1183.61	113.04	774.58	110.28	255.92
$E_{avg}(fJ)$	116.37	3898.30	110.34	1125.50	109.02	761.56	106.27	252.75
NED (%)	6.96	7.99	6.62	11.29	6.40	3.05	6.40	3.25
NSD (%)	1.28	1.45	1.31	1.83	1.30	0.82	1.30	0.82

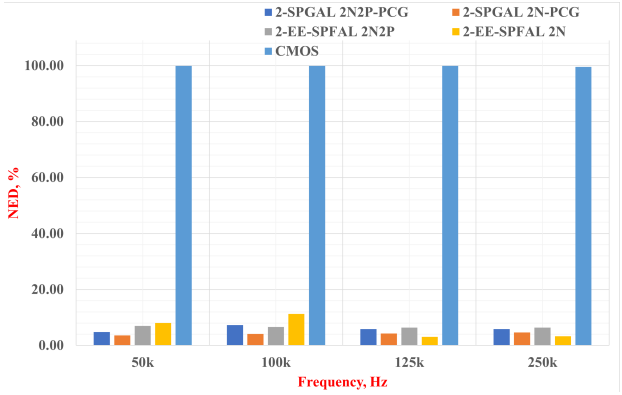


Fig. 15: NED value comparison for PRESENT-80 S-box.

SPFAL [20], and CMOS logic. We can see that adiabatic logic-based S-box has comparatively very low NED, and NSD value or better resilience against CPA compared to CMOS-based S-box. The S-box design using proposed 2-SPGAL, with 2N-PCG integrated into the design, shows an average of 95.86% and 99.34% better NED and NSD metric performance respectively compared its CMOS counterpart over the frequency range of 50 kHz to 250 kHz. Similarly, the 2-SPGAL S-box design with 2N2P-PCG integrated into the design shows an average of 94.07% and 99.16% better NED and NSD metric values respectively compared to CMOS counterpart over the frequency range of 50 kHz to 250 kHz. Further, the 2-SPGAL with 2N2P-PCG shows 10.15% and 12.98% better NED and NSD values respectively compared to the same counterpart implemented using 2-EE-SPFAL [20].

VIII. CPA Attack on one round of PRESENT-80 encryption design

The energy efficiency and security metrics comparison show the efficacy of the 2-SPGAL. It is also important to check the security resilience of the 2-SPGAL based design against power analysis attacks. The Correlation Power Analysis (CPA) is simpler to implement and has proven its success against symmetric and asymmetric encryption algorithms. The procedure to perform the CPA attack is explained in [39]. The one round of PRESENT-80 (Figure 14) is consist of 16 identical

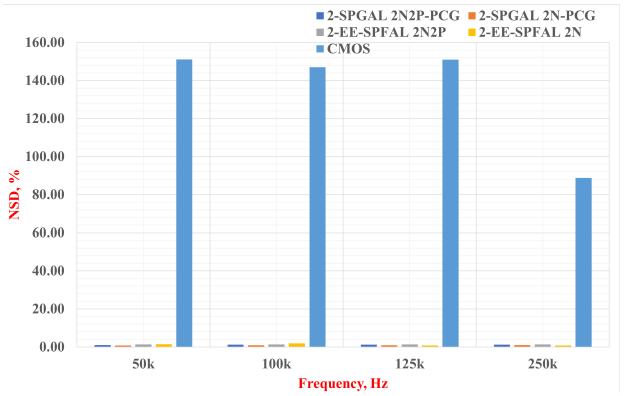


Fig. 16: NSD value comparison for PRESENT-80 S-box.

circuit blocks that includes four XOR gates and an S-box. Therefore, performing CPA attack on one such block would be similar to performing the CPA attack on entire circuit.

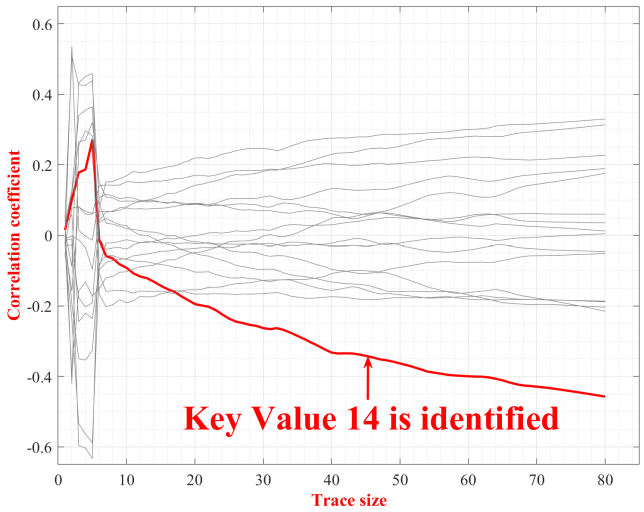


Fig. 17: Successful Revelation of Key=14 in on one round of PRESENT-80 encryption designed with CMOS.

The CPA attack requires the power traces collected from the attack point. The SPICE simulation was performed with a load value 10 fF to collect the power traces. The simulation environment is noise-free and requires fewer traces for successful CPA. More power traces are needed to minimize the noise effect. The simulation environment collects 80 traces in one clock period. For CMOS-based PRESENT-80 case-study design requires 5120 traces for successful CPA. Figure 17 shows that key-value 14 is revealed in PRESENT-80 designed using CMOS logic.

Similarly, we collected the 12,000 traces for PRESENT-80 implementation integrated with 2N-PCG and 2N-2P PCG. The larger number of traces can make the probability of CPA success higher. More traces results in a precise correlation between measured and hypothetical power traces used in the CPA attack. Figure 18 and 19 show that the correlation coefficient of actual key-value-14 is not standing out from other possible key values. The uniform current in the proposed 2-SPGAL at sinusoidal clocking helps to preserve the key. The

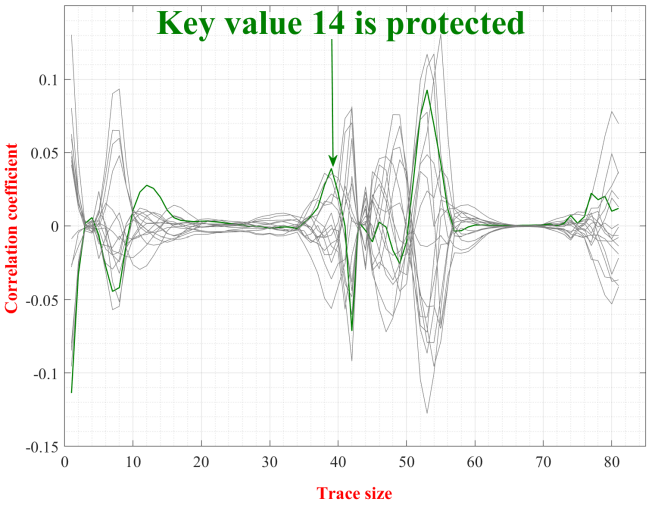


Fig. 18: Unsuccessful CPA attack on one round of PRESENT-80 encryption designed with proposed 2-SPGAL and 2N-PCG.

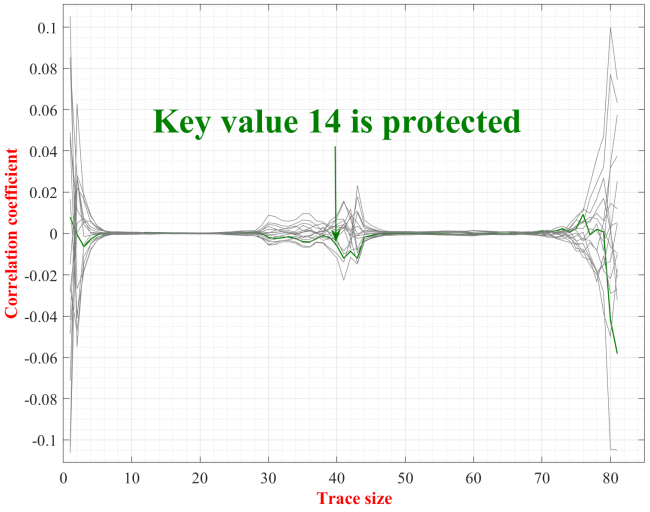


Fig. 19: Unsuccessful CPA attack on one round of PRESENT-80 encryption design with proposed 2-SPGAL and 2N2P-PCG.

CPA on case-study implementation shows that the proposed 2-SPGAL is energy efficient and secure against CPA attack.

IX. Conclusion

This article presented 2-SPGAL, the 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL) for Implantable Medical Devices (IMDs). The 2-SPGAL is energy-efficient and secure against the Correlation Power Analysis (CPA) attack. The proposed 2-SPGAL was evaluated in terms of energy, and security with two synchronous resonant Power Clock Generators (PCGs): 2N-PCG, and 2N2P-PCG. The case-study implementation of PRESENT-80 one round of encryption shows better energy saving compared to CMOS design for both 2N-PCG and 2N2P-PCG integrated with the design. The CPA attack point S-box shows better NED, and NSD as security metrics value in the proposed 2-SPGAL based design (with 2N-PCG and 2N2P PCG integrated) compared to CMOS based design. We also demonstrated that 2-SPGAL based design can protect the secret key against CPA, however, the key gets successfully revealed in CMOS based design. The proposed 2-SPGAL with its promising energy-efficient and CPA-resistant properties can be used to design energy-efficient and secure Implantable Medical Devices.

Acknowledgments

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

References

[1] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Design Automation Conf.*, 2012, pp. 12–17.

[2] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *IEEE 13th Int. Conf. on e-Health Networking, Applications and Services*, 2011, pp. 150–156.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symp. on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 129–142.

[4] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proc. of the ACM SIGCOMM 2011 Conf.*, 2011, pp. 2–13.

[5] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform," *J. of Netw. and Computer Appl.*, vol. 107, pp. 1–21, 2018.

[6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, 2008.

[7] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices," in *205th Int. Symp. on Medical Information and Communication Technology*, 2011, pp. 6–9.

[8] J. Fan, O. Reparaz, V. Rožić, and I. Verbauwhede, "Low-energy encryption for medical devices: Security adds an extra design dimension," ser. DAC '13. New York, NY, USA: Assoc. for Comput. Machinery, 2013.

[9] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *26th Int. Conf on VLSI design and 2013 12th Int. conf. on embedded systems*. IEEE, 2013, pp. 203–208.

[10] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annu. Int. cryptology Conf.* Springer, 1999, pp. 388–397.

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

[12] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *26th Int. Conf. on VLSI Design and 12th Int. Con. on Embedded Systems*, 2013, pp. 203–208.

[13] S. Maji, U. Banerjee, S. H. Fuller, M. R. Abdelhamid, P. M. Nadeau, R. T. Yazicigil, and A. P. Chandrakasan, "A low-power dual-factor authentication unit for secure implantable devices," in *IEEE Custom Integrated Circuits Conf. (CICC)*, 2020, pp. 1–4.

[14] S. Yin, M. Kim, D. Kadetotad, Y. Liu, C. Bae, S. J. Kim, Y. Cao, and J.-S. Seo, "A 1.06- μ w smart ecg processor in 65-nm cmos for real-time biometric authentication and personal cardiac monitoring," *IEEE J. Solid-State Circuits*, vol. 54, no. 8, pp. 2316–2326, 2019.

[15] "Short Range Devices (SRD); Ultra Low Power Active Medical Implants (ULP-AMI) and accessories (ULP-AMI-P) operating in the frequency range 9 kHz to 315 kHz Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU ," ETSI (European Telecommunications Standards Institute), Sophia-Antipolis, France, Standard, Jun. 2016.

[16] A. G. Dickinson and J. S. Denker, "Adiabatic dynamic logic," *IEEE J. Solid-State Circuits*, vol. 30, no. 3, pp. 311–315, 1995.

[17] J. Lim, D.-G. Kim, and S.-I. Chae, "A 16-bit carry-lookahead adder using reversible energy recovery logic for ultra-low-energy systems," *IEEE J. Solid-State Circuits*, vol. 34, no. 6, pp. 898–903, 1999.
[18] S. G. Younis and T. F. Knight, "Non-dissipative rail drivers for adiabatic circuits," in *Proc. of Sixteenth IEEE Conf. on Advanced Research in VLSI*, 1995, pp. 404–414.
[19] S. Maheshwari and I. Kale, "Impact of adiabatic logic families on the power-clock generator energy efficiency," in *15th Conf. on Ph.D Research in Microelectronics and Electronics (PRIME)*, 2019, pp. 25–28.
[20] 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.
[21] J. A. Ambrose, R. G. Ragel, and S. Parameswaran, "Rijid: random code injection to mask power analysis based side channel attacks," in *Proc. of the 44th Annu. Design Automation Conf.*, 2007, pp. 489–492.
[22] D. May, H. L. Muller, and N. P. Smart, "Non-deterministic processors," in *Australasian Conf. on Information Security and Privacy*. Springer, 2001, pp. 115–129.
[23] D. May, H. Muller, and N. Smart, "Random register renaming to foil dpa," in *Int. Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2001, pp. 28–38.
[24] K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "A side-channel leakage free coprocessor ic in 0.18 μm cmos for embedded aes-based cryptographic and biometric processing," in *Proc. of the 42nd Annu. Design Automation conf.*, 2005, pp. 222–227.
[25] A. Moradi and A. Poschmann, "Lightweight cryptography and dpa countermeasures: A survey," in *Int. Conf. on Financial Cryptography and Data Security*. Springer, 2010, pp. 68–79.
[26] 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," *Integr. the VLSI J.*, vol. 58, pp. 369–377, 2017.
[27] 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 Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 2, no. 4, pp. 398–407, 1994.
[28] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Int. workshop on cryptographic hardware and embedded systems*. Springer, 2004, pp. 16–29.
[29] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 149–156, 2014.
[30] H. S. Raghav, V. A. Bartlett, and I. Kale, "Investigating the effectiveness of without charge-sharing quasi-adiabatic logic for energy efficient and secure cryptographic implementations," *Microelectronics J.*, vol. 76, pp. 8–21, 2018.
[31] H. S. Raghav and I. Kale, "A balanced power analysis attack resilient adiabatic logic using single charge sharing transistor," *Integr. the VLSI J.*, vol. 69, pp. 147–160, 2019.
[32] C. Monteiro, Y. Takahashi, and T. Sekine, "Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks," in *36th IEEE Int. Conf. on Telecommunications and Signal Processing (TSP)*, 2013, pp. 732–736.
[33] B. Fadaeinia and A. Moradi, "3-phase adiabatic logic and its sound sca evaluation," *IEEE Trans. on Emerging Topics in Computing*, 2020.
[34] A. Degada and H. Thapliyal, "2-spgal: 2-phase symmetric pass gate adiabatic logic for energy-efficient secure consumer iot," in *Presented at the 39th IEEE Int. Conf. on Consumer Electronics (ICCE)*, Jan. 10-12, 2021, pp. 1–6.
[35] H. Mahmoodi-Meimand and A. Afzali-Kusha, "Efficient power clock generation for adiabatic logic," in *The 2001 IEEE Int. Symp. on Circuits and Systems (ISCAS) (Cat. No. 01CH37196)*, vol. 4, 2001, pp. 642–645.
[36] 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 *Int. Workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 450–466.
[37] M. J. Dworkin, *Sp 800-38A. Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. National Institute of Standards & Technology, 2001, [Online; accessed 05-May-2021].
[38] Y. Takahashi, T. Sekine, and M. Yokoyama, "Two-phase clocked cmos adiabatic logic," *Far East J. Electronics and Communications*, vol. 3, no. 1, pp. 17–34, 2009.
[39] J. Wu, Y. Shi, and M. Choi, "Measurement and evaluation of power analysis attacks on asynchronous s-box," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 10, pp. 2765–2775, 2012.

ABOUT THE AUTHORS

Amit Degada is currently a PhD candidate in the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. He has completed his Masters of Technology from National Institute of Technology (NIT) Surat, India. His research interest is on the development of hardware assisted cybersecurity primitives for consumer IoT applications.

Himanshu Thapliyal (SM'16) is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, Tennessee, USA. He received a PhD degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2011 where he received the 'Distinguished Graduate Achievement Award'. From 2012-14, he worked as a designer of processor test solutions at Qualcomm, where he received the Qualcomm QualStar Award for contributions to memory built-in self-test. He joined as an Assistant Professor at the University of Kentucky, Lexington in 2014 where he got promoted to Associate Professor in 2020. He is the recipient of the NSF CAREER award, and IEEE-CS TCVLSI Mid-Career Research Achievement Award. He received the Provost's Wethington Award for contributions to the University of Kentucky Research Program. He has authored over 150 publications that have resulted in over 4700 citations with h-index=40 (Google Scholar). He has been ranked in the top 50 among scientists throughout the world in the field of Computer Hardware & Architecture for the calendar years 2019 and 2020. He has received Best Paper awards at the 2021 IEEE International Conference on Consumer Electronics, 2020 IEEE World Forum on Internet of Things (WF-IoT), 2017 Cyber and Information Security Research Conference (CISR), and 2012 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). He is the steering committee vice-chair of the IEEE Symposium on Smart Electronic Systems. He served as the General Chair of the 2020 IEEE Symposium on Smart Electronic Systems. He has served as the Program Chair of the 2020 IEEE International Conference on Consumer Electronics, 2019 IEEE Computer Society Annual Symposium on VLSI, and 2018 IEEE Symposium on Smart Electronic Systems. He is serving as the Section Editor of the Springer Nature Computer Science and is leading two sections: (i) Quantum Computing and Emerging Technologies, and (ii) Emerging Trends in Sensors, IoT and Smart Systems. He is also serving as the Senior Associate Editor of the IEEE Consumer Electronics Magazine, Associate Editor of the IEEE Internet of Things Journal, and the editorial board member of the Microelectronics Journal. His research interests hardware security of IoT and vehicles, quantum computing, and smart healthcare solutions for older adults and Alzheimer's Disease and Related Dementias (ADRD).