University of Kentucky
UKnowledge

Electrical and Computer Engineering Graduate Research | Electrical and Computer Engineering

12-14-2021

Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices

Amit Degada
University of Kentucky

Himanshu Thapliyal
University of Tennessee, Knoxville

Follow this and additional works at: https://uknowledge.uky.edu/ece_gradpub

 Part of the Electrical and Computer Engineering Commons

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Repository Citation

Degada, Amit and Thapliyal, Himanshu, "Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices" (2021). *Electrical and Computer Engineering Graduate Research*. 1.
https://uknowledge.uky.edu/ece_gradpub/1

This Article is brought to you for free and open access by the Electrical and Computer Engineering at UKnowledge. It has been accepted for inclusion in Electrical and Computer Engineering Graduate Research by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices

Digital Object Identifier (DOI)
https://doi.org/10.1109/OJNANO.2021.3135364

Notes/Citation Information
Published in *IEEE Open Journal of Nanotechnology*, v. 3.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/.

This article is available at UKnowledge: https://uknowledge.uky.edu/ece_gradpub/1

IEEE Open Journal of Nanotechnology

Received 6 October 2021; revised 27 November 2021; accepted 9 December 2021. Date of publication 14 December 2021; date of current version 12 January 2022. The review of this article was arranged by Associate Editor Masashi Arita.

Digital Object Identifier 10.1109/OJNANO.2021.3135364

Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices

AMIT DEGADA [1] (Graduate Student Member, IEEE), AND HIMANSHU THAPLIYAL [2] (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY 40506 USA
[2]Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA

CORRESPONDING AUTHOR: HIMANSHU THAPLIYAL (e-mail: hthapliyal@ieee.org)

This work was supported in part by the National Science Foundation CAREER Award Number 1845448.

ABSTRACT Designing energy-efficient and secure cryptographic circuits in low-frequency medical devices are challenging due to low-energy requirements. Also, the conventional CMOS logic-based cryptographic circuits solutions in medical devices can be vulnerable to side-channel attacks (e.g. correlation power analysis (CPA)). In this article, we explored single-rail Clocked CMOS Adiabatic Logic (CCAL) to design an energy-efficient and secure cryptographic circuit for low-frequency medical devices. The performance of the CCAL logic-based circuits was checked with a power clock generator (2N2P-PCG) integrated into the design for the frequency range of 50 kHz to 250 kHz. The CCAL logic gates show an average of approximately 48% energy-saving and more than 95% improvement in security metrics performance compared to its CMOS logic gate counterparts. Further, the CCAL based circuits are also compared for energy-saving performance against dual-rail adiabatic logic, 2-EE-SPFAL, and 2-SPGAL. The adiabatic CCAL gates save on an average of 55% energy saving compared to 2-EE-SPFAL and 2-SPGAL over the frequency range of 50 kHz to 250 kHz. To check the efficacy of CCAL to design a larger cryptographic circuit, we implemented a case-study design of a Substitution-box (S-box) of popular lightweight PRESENT-80 encryption. The case-study implementation (2N2P-PCG integrated into the design) using CCAL shows more than 95% energy saving compared to CMOS for the frequency 50 kHz to 125 kHz and around 60% energy saving at frequency 250 kHz. At 250 kHz, compared to the dual-rail adiabatic designs of S-box based on 2-EE-SPFAL and 2-SPGAL, the CCAL based S-box shows 32.67% and 11.21% of energy savings, respectively. Additionally, the CCAL logic gate structure requires a lesser number of transistors compared to dual-rail adiabatic logic. The case-study implementation using CCAL saves 45.74% and 34.88% transistor counts compared to 2-EE-SPFAL and 2-SPGAL. The article also presents the effect of varying tank capacitance in 2N2P-PCG over energy efficiency and security performance. The CCAL based case-study was also subjected against CPA. The CCAL-based S-box case study successfully protects the revelation of the encryption key against the CPA attack, However, the key was revealed in CMOS-based case-study implementation.

INDEX TERMS Adiabatic logic, correlation power analysis attack, cryptographic circuits, healthcare, hardware security, medical device, power clock generators, side-channel attacks.

I. INTRODUCTION

According to the World Health Organization report, 1.9 billion adults were overweight, and out of which 35% were obese in 2017. Further, 340 million children and adolescents were obese or overweight in 2020. Higher body weight can lead to chronic diseases, such as cardiovascular diseases, hypertension, diabetes, degenerative to joints, musculoskeletal system disorders, and several cancers, e.g., liver, colon, ovarian, gallbladder, kidney, breast, and prostate [1]. The US Centers for Disease Control (CDC) classify obesity at epidemic proportions. The CDC reports say 6 in 10 adults in the US have a chronic disease and 4 in 10 adults suffers

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

TABLE 1. Frequency Range in Medical Applications

Reference	Medical Application	Frequency range of operation
[3]	Low frequency inductive implants (pacemakers, ICD etc.)	Less than 200 kHz
[4] [5]	Implant communication	9 - 315kHz
[6]	Bioelectrical impedance meter	50 kHz, 250 kHz
[7]	Electrical Impedance Myography (EIM)	50 kHz
[8] [9] [10]	Electrical Impedance Tomography (EIT)	50 kHz to 250 kHz
[11]	CMOS wearable non-invasive impedance meter	100 Hz to 1 MHz
[12]	Hearing Aid	32 khz to 8.00 Mhz
[13]	Magnetic Particle Imaging (MPI) systems	1 kHz to 100 kHz
[14] [15]	Low data-rate Body Couple communication (BCC)	10 kHz to 10 MHz
[16]	Home Health Hub	200 kHz to 1.0 MHz

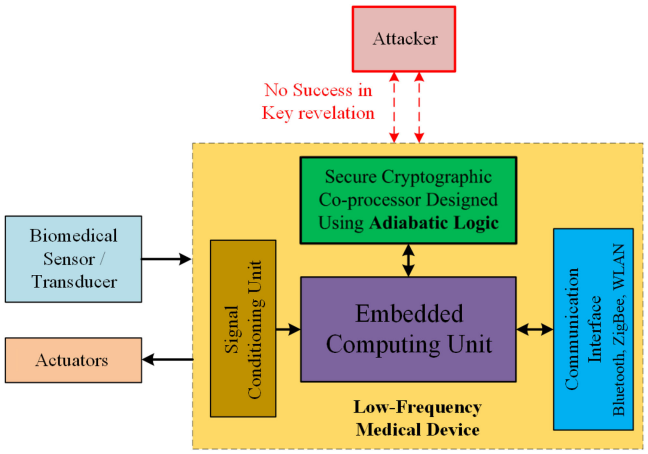

FIGURE 1. Adiabatic Logic as preferred choice to design energy-efficient and secure cryptographic coprocessor.

more than one chronic disease [2]. On the other end, the advancement in semiconductor technology has empowered the inclusion of medical devices in many chronic disease diagnostic, therapeutic processes, and patient monitoring. They are pervasive in medical labs, offices of physicians, and even implanted inside a patient's body, e.g. pacemaker, Implantable Cardiac Defibrillators (ICDs), and neurostimulators. Table 1 lists some of the medical devices and their frequency range of the operation.

Modern medical devices often aggregate physiological data, store the personal information of the patient and communicate to the cloud. Some of these devices, e.g. medical implants are battery-powered and their operational life is limited up to 10 years [17], [18]. Over the years, many researchers have raised concerns about compromising sensitive personal and physiological information. The compromised device can perform unauthorized command execution and data transmission [19], create electrical shocks [20], [21] and deplete battery [22]. It can compromise the secrecy and privacy of the patient information, however, in some cases it could be life-threatening. It becomes of utmost importance to protect user-information by including cryptographic coprocessors in device design. Security often comes with the cost of increment in the power consumption [23]–[26]. Therefore, designing energy-efficient and secure cryptographic coprocessor circuits in medical devices is an interesting research direction.

Lightweight Cryptographic (LWC) cipher is one of the preferred solution to provide encryption at low-energy budgets [27]–[29]. However, in recent years, the LWC ciphers have been found vulnerable against Side-Channel Analysis (SCA) attacks, e.g. heat emission, electromagnetic radiation, power analysis [30], [31], and timing attacks [32]. The work in [14], [30] lists several possible SCA over medical devices. Among different possible SCA, the Correlation Power Analysis (CPA) attack is easy to implement and found more lethal to reveal the encryption key.

Currently, CMOS-based computing technology is reaching to its limit in energy efficiency with scaling down of the technology. There are two possible directions to reduce the energy consumption: (i) to reduce the energy required to distinct the logic '1' from logic '0' (ii) conserve the energy from one logical operation to the next [33], [34]. The adiabatic logic works on the energy recovery principle and is classified under the second approach mentioned above. Adiabatic logic in bulk MOSFET has emerged as an attractive choice for the designer compared to conventional CMOS due to its superior energy performance and CPA resilience. In this article, we use adiabatic logic to design energy-efficient and secure lightweight cryptographic coprocessors in medical devices (Fig. 1). The adiabatic logic circuits recover the energy stored inside the load capacitor (rather than dissipating as heat), thus, results in significantly low-power consumption. Further, the power traces of the adiabatic logic circuits are uniform in shape, unlike the conventional CMOS logic circuits. The uniform power traces is a very important property to disguise the processed information. The above property helps to combat the CPA. Earlier, we proposed two-phase sinusoidal clocking based adiabatic logic 2-phase Energy Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL) [35] and 2-phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) [36]. The above solution enables the design of the low-energy and CPA secure circuit. The 2-EE-SPFAL and 2-SPGAL are classified as dual-rail adiabatic logic as they produce two outputs at the logic gate, V_{out} and $\overline{V_{out}}$. The dual-rail adiabatic logic uses the two-transistor logic evaluation network to balance the switching activities, and therefore have uniform power traces. The above feature results in a larger transistor count overhead.

In this research, we address the above issue by exploring the single-rail adiabatic logic called Clocked CMOS Adiabatic Logic (CCAL). The CCAL was previously proposed in [37] with preliminary analysis limited to reduction in energy consumption for logic gates and a chain of inverters. It is interesting to see the security performance of the CCAL. Further, the energy and security performance of the adiabatic logic circuits largely depends upon the Power-Clock Generator (PCG) integrated with the logic circuit. The poor interfacing suffers a reduction in energy-saving and compromised security (explained in Section II). In this article, we evaluate the energy efficiency and security performance of the CCAL logic to

design a secure cryptographic circuit with PCG integrated into the design. Further, the physiological signals in human bodies are typically a few tens to hundreds of the frequency range. In the digital domain, after sampling the operational frequencies are mostly limited up to a few kHz (Table 1). The adiabatic logic saves significant energy consumption compared to its CMOS counterpart at low-frequency applications. Some example of the low-frequency medical device includes inductive implants, bioimpedance meter, Electrical Impedance Myography (EIM), hearing aids, Electrical Impedance Tomography (EIT), Magnetic Particle Imaging (MPI), and Body-Coupled Communication (BCC), etc. In this article, we evaluate the performance of the CCAL based cryptographic circuit for the frequency range of 50 kHz to 250 kHz.

A. KEY CONTRIBUTION

The key contributions of this work are as follows:

- The article explores CCAL, a novel single-rail Clocked CMOS Adiabatic Logic (CCAL) to design energy-efficient and secure cryptographic circuits. The CCAL can be an alternate choice for low-energy and CPA-resistant medical devices.
- The case-study implementation of PRESENT-80 S-Box circuitry saves more than 95% energy for frequency range 50 kHz to 125 kHz and approximately 60% more energy saving at 250 kHz compared to its CMOS counterpart. The above energy saving can be highly beneficial to design low-power cryptographic circuits.
- The case-study implementation shows saving of 45.74% and 34.88% of transistors compared to 2-EE-SPFAL [35] and 2-SPGAL [36]. At 250 kHz, compared to the dual-rail adiabatic designs of S-box based on 2-EE-SPFAL and 2-SPGAL, the CCAL based S-box shows 32.67% and 11.21% of energy savings, respectively. Thus, CCAL can be an alternate choice to design a secure and energy-efficient cryptographic circuit with lesser transistor overhead compared to its dual-rail adiabatic logic counterpart.
- We also presents the effect of varying tank capacitance in 2N2P-PCG over energy efficiency and security performance. We demonstrate that having 200 fF value of tank capacitor (C_E) in 2N2P-PCG can provide optimum energy and security features.
- The single-rail CCAL based circuitry removes the need for discharge circuitry required in its dual-rail counterpart. It helps to reduce the external need for the control signals for discharge circuitry.
- We demonstrate that the PRESENT-80 using CCAL can successfully defend the encryption key against the CPA attack for both 2N2P-PCG integrated into the design. However, the encryption key is revealed in the same counterpart design using CMOS.

B. ORGANIZATION OF THE PAPER

This article is organized as follows. The background information related to the research is briefly explained in Section II. In Section III, we present the CCAL logic gate structure, energy efficiency, and security metric performance. Section IV presents PRESENT-80 S-box design as a case-study implementation, compare the transistor count requirement in CCAL and other competitive logic design choice and provides energy and security performance analysis. Section V discusses the effect of varying tank capacitor values in PCG tank circuit over energy and security performance in case-study implementation. Section VI discusses the simulation of the CPA attack over the PRESENT-80 S-box. Section VII presents the discussion and conclusion.

II. BACKGROUND

In recent years, researchers have shown the effectiveness of power-analysis attacks to reveal the encryption key in cryptographic circuits. There have been many countermeasures are proposed, e.g., masking [31], random instruction injection [38], non-deterministic processors [39], random register renaming [40], secure co-processors [41], and cell-level countermeasures [42]. In this work, we employ the cell-level countermeasure, i.e. to build secure logic gates. Adiabatic logic design is one such approach, that can thwart the power-analysis attacks such as CPA.

In this section, we briefly discuss the adiabatic logic and the common metrics used to evaluate CPA resilience. Further, the energy and security performance of adiabatic logic circuits largely depend on the Power-Clock Generator (PCG) integrated into the design. We also provide a brief overview of the type of the PCG integrated with design.

A. ADIABATIC LOGIC

The adiabatic logic circuit techniques have emerged as an attractive choice to design cryptographic circuits in recent years. The adiabatic circuit recovers the stored charge in load capacitance of the logic gates to the power-clock circuits. Compared to the conventional CMOS circuit that uses the DC voltage to power up the circuits, the adiabatic logic circuits use a slow-varying voltage signal. This slow-varying voltage signal appears as a constant current source for a capacitive load [44]. The ramp signal (generated from PCG) is a practical way to achieve the constant current source. Fig. 2 illustrates the switching model, discharging and charging current path for the load capacitor current.

We can see in Fig. 2 that adiabatic logic circuit employs two logic evaluation blocks, F and $\overline{F}$, that outputs V_{out} and $\overline{V_{out}}$ respectively. The two complementary logical outputs (called dual-rail logic) are necessary to balance the switching activities., that balance the current passing into logic blocks. The above property is helpful to maintain nearly uniform current dissipation for all possible logic inputs. Therefore, dual-rail adiabatic logic circuits are the most commonly employed by researchers to design low-energy and CPA resilience circuits low-frequency devices.

Equation (1) mathematically describes the energy consumption in adiabatic logic circuits. The C is load capacitor, R is lumped resistance, V is the full-swing voltage of the

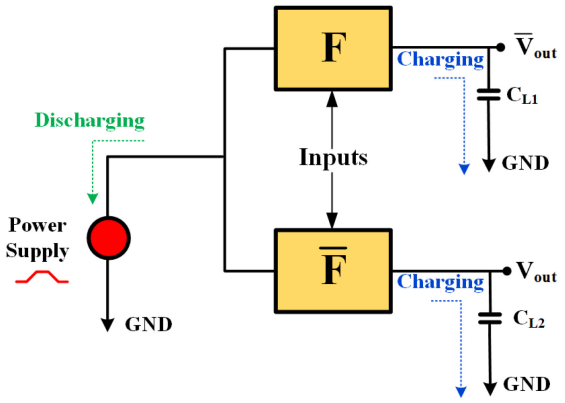

FIGURE 2. Charging and discharging in adiabatic circuits [43].

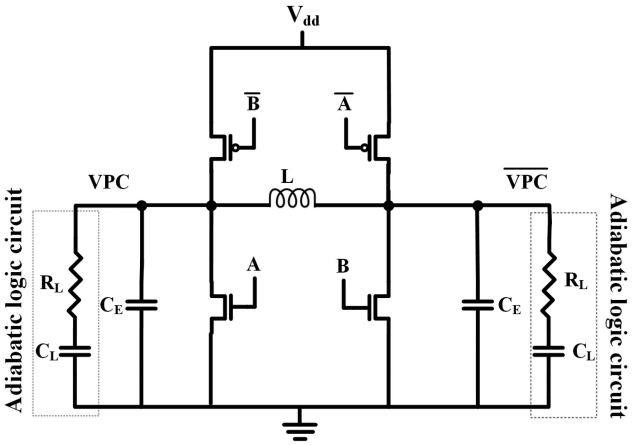

FIGURE 3. Synchronous 2N2P-PCG circuit [50].

power-clock circuit and T is the time period of charging and discharging operation. We can see that if the given frequency is lower (i.e. higher T) then it is possible to have the energy consumption significantly lower compared to the conventional energy dissipation in CMOS. The above property to thwart CPA attacks and lower energy consumption makes adiabatic logic, an ideal choice to design low-frequency cryptographic circuit in medical Devices. In this research, we explore one such technique called CCAL.

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

B. SECURITY PERFORMANCE METRICS FOR CPA-RESISTANCE

The Correlation Power Analysis (CPA) attack is one of the widely used power-analysis based side-channel attacks. Its relatively simple implementation and higher success rate have made it an attractive choice for attackers. Further, the CPA is equally effective to reveal the stored encryption key for both symmetric and asymmetric cryptographic algorithms. In the previous section, we have seen that adiabatic logic is an attractive design choice to design the CPA resilient circuit. Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) are commonly used metrics to compare the CPA resilience performance against CMOS circuits [43], [45]–[49].

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

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

The NED and NSD values are measured for all possible cyclic input permutations. The NED and NSD values are measured in terms of the percentage. The difference between the minimum and maximum energy consumption for all input combinations is referred to as NED (2). The NSD value (3) is the mean square difference between the instantaneous energy consumption of input to the average energy consumption for all possible outcomes. NSD gives more insight into how much inputs are deviated compared to average energy consumption in given adiabatic logic circuits. For an ideal adiabatic circuit, there will be equal energy distribution for all possible cyclic inputs, thus NED and NSD values are zero. For practical circuits, lower NED and NSD metrics values make it the better choice for CPA resilience performance.

C. INTEGRATED POWER-CLOCK GENERATOR

In this section, we explain the design of the Power Clock Generator (PCG) for adiabatic circuits. In the adiabatic circuit, unlike the conventional CMOS, the circuit operates on the slow-varying power-clock signal. The efficient design of the PCG is of utmost importance for adiabatic circuits. The PCG recovers the charge from the adiabatic logic core to the oscillator capacitor as well as inductor during charge-recovery operation. PCG usually consumes a large fraction of the power. Poor design and its inefficient integration with the design result in less energy-efficient and secure design. Therefore, it becomes necessary to evaluate the energy performance of the adiabatic circuit with PCG integrated into the design.

Over the years, many solutions PCG designs have been proposed to generate sinusoidal power clocking signals. The synchronous resonant PCGs have more energy conversion efficiency. In this work, we integrate 2N2P-PCG with adiabatic logic circuits and its schematic is shown in Fig. 3 [50]. The 2N2P-PCG uses an external inductor, two PMOS, two NMOS, and two external capacitor C_E.

In this article, we use the external inductor as on-chip inductors lead to a low Q value. The inherent structure and operation of the CCAL makes the lumped capacitance of the inductor independent of the input logic signal and remains constant. We use the external balancing capacitance C_E to adjust the capacitance value for better energy efficiency.

The 2N2P-PCG requires four external time-base signals. The external time-base signals can help to synchronize the adiabatic circuits in larger conventional non-adiabatic circuits.

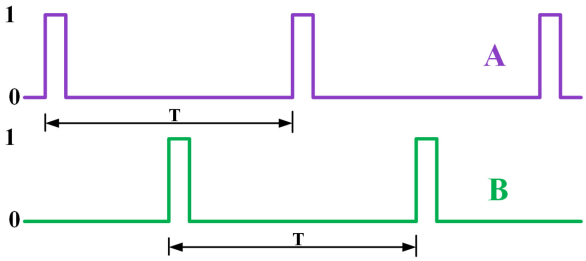

FIGURE 4. Control signals in 2-Phase PCG design [50].

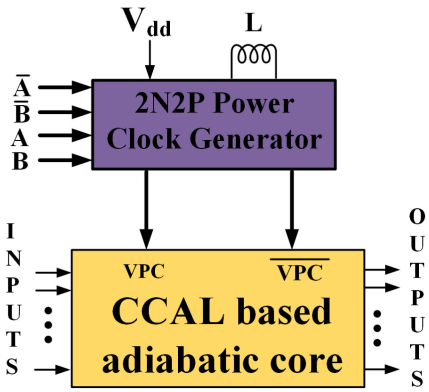

FIGURE 5. 2N2P-PCG interfacing with the CCAL based adiabatic logic circuits.

Fig. 4 shows the external time-base control signals used to operate 2N2P-PCG. The 2N2P-PCG generates two out-of-phase signals by two identical circuits operating in a lock-step manner. The operation frequency of the 2N2P-PCG is given by (4). CCAL logic requires two out-of-phase sinusoidal power-clock signals, VPC and $\overline{VPC}$. Fig. 5 shows the interfacing of 2N2P-PCG with the CCAL logic circuits.

$$f_0 = \frac{1}{2\pi\sqrt{L\left(\frac{C}{2}\right)}} \tag{4}$$

III. CLOCKED CMOS ADIABATIC LOGIC (CCAL) AND ITS EVALUATION IN ENERGY-EFFICIENCY AND SECURITY METRICS

In this section, we will first illustrate the background on the logic gate structure of CCAL. Then, we will present the energy efficiency and security performance evaluation of CCAL logic gates with 2N2P-PCG integrated into the design.

A. BACKGROUND ON CLOCKED CMOS ADIABATIC LOGIC (CCAL)

The Clocked CMOS Adiabatic Logic (CCAL) was previously proposed in [37] with preliminary analysis limited to reduction in energy consumption for logic gates and a chain of inverters. Fig. 6 shows the generalized gate structure of CCAL. It consists of two primary parts, (i) CMOS logic (ii) clock connection which connects CMOS logic to the sinusoidal clocking part. The signals VPC and $\overline{VPC}$ are two out-of-phase

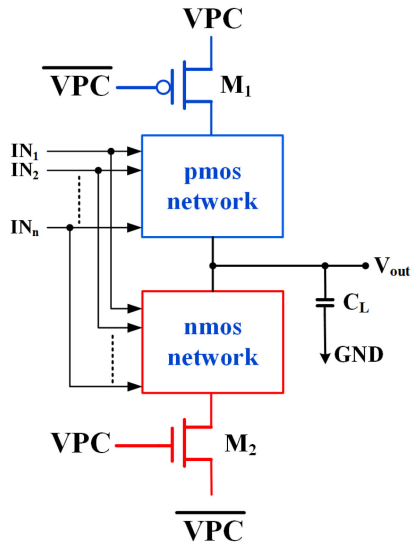

FIGURE 6. Clocked CMOS Adiabatic Logic (CCAL) gate schematic [37].

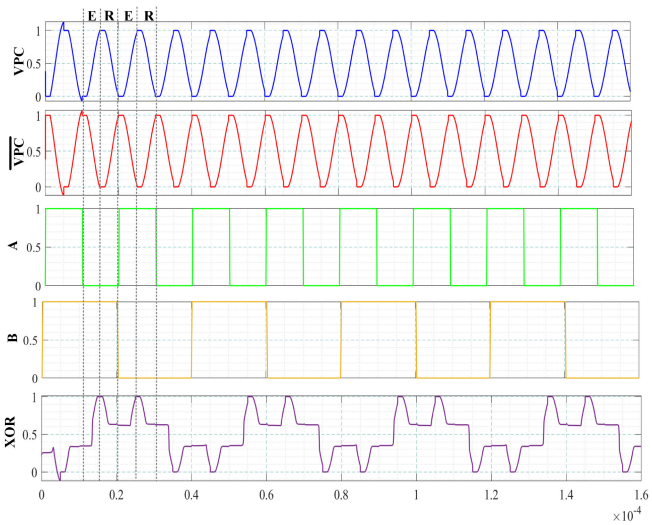

FIGURE 7. CCAL-based XOR logic gate waveform with 2N2P-PCG integrated into the design.

sinusoidal power clocks. The operation of CCAL (Fig. 7) can be explained in two stages: (i) Evaluation (E) (ii) Recovery (R). During the Evaluation stage, when the voltage at both clock signals is more than the threshold voltage (V_{th}) then it turns on both transistor M1 and M2 (clock connection network). Then the PMOS and NMOS blocks evaluate the output logic based on the input signal logic. During the Recovery (R) phase, the output voltage stored in load capacitance is held until the next evaluation phase.

There have been many low-energy solutions in the research literature that works low-frequency operation. The adiabatic circuit-based cryptographic circuits are found to defend encryption keys against power-analysis attacks. Earlier, we proposed the two-phase sinusoidal clocking-based dual-rail adiabatic logic 2-SPGAL [36] and 2-EE-SPFAL [35]. The CCAL can be an alternate choice to design CPA secure and

energy-efficient cryptographic circuits. The single-rail adiabatic, e.g. CCAL has less logic overhead compared to its dual-rail adiabatic logic counterpart. The above properties can be highly beneficial for resource-constrained IMDs. Further, the dual-rail logic, 2-EE-SPFAL [35] and 2-SPGAL [36] requires the additional discharge circuitry and corresponding control signals. The CCAL network removes the need for discharge circuitry and the logic gate structure is very similar to the CMOS logic gate.

However, the performance of the adiabatic logic is largely affected by the integration of the PCG. It is important to investigate the performance of the CCAL based cryptographic circuits energy efficiency and security performance with the integration of PCG in design. Therefore, we evaluated the performance of the CCAL based circuits with 2N2P-PCG integrated into the design.

B. ENERGY-EFFICIENCY AND SECURITY EVALUATION OF CCAL LOGIC GATES

Logic gates are the primary constituent of a larger circuit. It becomes important to check the energy and security metrics performance to build low-energy and secure cryptographic circuits. In this section, we explain the energy-efficiency and security performance of the CCAL logic gates. We have compared the simulation results of the CCAL logic gate with CMOS, 2-EE-SPFAL [35], and 2-SPGAL [36] logic gates.

The energy consumption in medical devices should be as minimal as possible. Further, to build a secure circuit the variation in energy consumption for input combination variation should be ideally zero. The CPA calculates the correlation between hypothetical power traces of all possible keys and collected power traces from the circuit. Uniform power traces disguise the linear dependency. To look at this feature at the circuit level, we check the energy performance of the logic gate at all possible change in input values.

$$E = \int_0^T V_P I_P dt \tag{5}$$

The energy consumption is the integration of the product of voltage (V_p) and current (I_p), i.e. power consumption for input signal [51]. We built CCAL logic gates using 45 nm technology and considered the load of 10 fF. Further, the energy and security performance of adiabatic logic circuits largely depends upon the PCG integrated into the design. Therefore, the energy and security metric performance was evaluated for logic gates with 2N2P-PCG integrated into the design. We target particularly low-frequency medical device encryption, therefore, the frequency range of 50 kHz to 250 kHz is considered.

The variation in energy consumption value provides more insight than observing the current traces. We used SPICE simulation to collect energy consumption value for a total of 2^{2n} possible cyclic variations in the n-bit circuit. The energy consumption values can be used in (2) and 3 equation to calculated NED and NSD value. For ideal conditions, equal energy consumption results in zero NED and NSD values. However, for practical scenarios, the NED and NSD value should be as low as possible. Having lower NED and NSD value results in less correlation between hypothetical and actual power traces. Thus, the circuit can protect the stored encryption key.

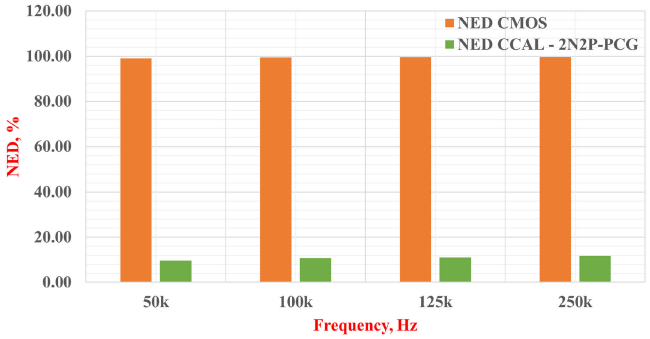

FIGURE 8. NED value comparison for AND logic gate.

It is very important to observe the energy saving in CCAL compared to other logic gates. For equal comparision, the dual rail logic circuits 2-EE-SPFAL [35] and 2-SPGAL [36] are designed with 2N2P-PCG integrated into the design, similar to the CCAL counterpart. For the energy performance metric, we have listed E_{min}, E_{max} and E_{avg}. A smaller difference between E_{min}, and E_{max} indicates the energy consumption across all possible input combinations is smaller and results in a better secure circuit. Further, the $_{avg}$ for each logic gate should be as low as possible for better energy efficiency.

Table 2 shows the comparison of CCAL AND logic gate with its counterpart in CMOS, 2-EE-SPFAL [35], and 2-SPGAL [36]. The CCAL AND logic gate has the lowest E_{avg} value for the frequency range of 50 kHz to 250 kHz. The CCAL AND logic gate has on an average of 4.7248 fJ E_{avg} for the frequency range of 50 kHz to 250 kHz. While in its CMOS, 2-EE-SPFAL [35], and 2-SPGAL [36] counterpart the average of E_{avg} is 7.7681 fJ, 11.9258 fJ, and 10.7920 fJ. Therefore, we can conclude that the sinusoidal clocking circuits on top of the PMOS and NMOS network help to reduce significant energy consumption compared to conventional CMOS logic and also to its dual-rail adiabatic logic counterpart. Table 3 summarizes the average energy saving (in %) in CCAL-based AND logic gate compared to its CMOS, 2-EE-SPFAL [35], and 2-SPGAL [36] counterpart.

For the secure encryption circuit design, it becomes important to check the NED and NSD performance of the logic gate before building the larger circuits. In this work, we primarily compared the NED and NSD value of CCAL logic gates with their CMOS counterpart. The CMOS circuit is considered the benchmark because has been shown to be vulnerable to CPA attacks. Figs. 8 and 9 shows the comparison of NED and NSD security performance metrics for CCAL and CMOS AND logic gate. We can see that CCAL AND logic gate

TABLE 2. Energy-Efficiency and Security Performance Comparison for and Logic Gate

	50 kHz				100 kHz			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	0.3745	11.8596	9.1762	4.8398	0.1873	11.7577	11.1575	4.5769
$E_{max}(fJ)$	38.0678	12.1081	9.2971	5.3530	29.8538	11.9808	11.3861	5.1297
$E_{avg}(fJ)$	9.8487	12.0227	9.2425	4.9780	7.6402	11.8864	11.2964	4.7216
NED (%)	99.02	2.05	1.30	9.59	99.37	1.86	2.01	10.78
NSD (%)	117.08	0.60	0.40	3.55	118.71	0.57	0.58	4.24
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	0.1498	11.7009	11.1185	4.5224	0.0749	11.7677	11.1600	4.3702
$E_{max}(fJ)$	28.2615	11.9486	11.3740	5.0853	25.1593	12.0363	11.4598	4.9547
$E_{avg}(fJ)$	7.2078	11.8591	11.2804	4.6682	6.3756	11.9351	11.3488	4.5316
NED (%)	99.47	2.07	2.25	11.07	99.70	2.23	2.62	11.80
NSD (%)	119.18	0.59	0.67	4.42	120.26	0.65	0.78	4.66

TABLE 3. E_{avg} - Energy Saving (In %) in CCAL and Logic Gate

Type of the logic	Baseline Logic to compare	50 kHz	100 kHz	125 kHz	250 kHz
Dual-Rail Adiabatic	2-EE-SPFAL [35]	58.60	60.28	60.64	62.03
	2-SPGAL [36]	46.14	58.20	58.62	60.07
Single-Rail	Conventional CMOS	49.46	38.20	35.23	28.92

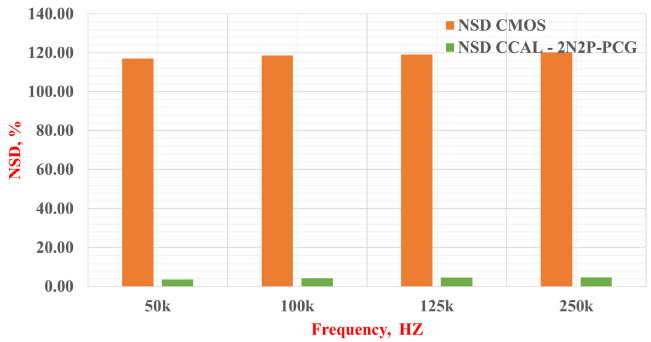

FIGURE 9. NSD value comparison for AND logic gate.

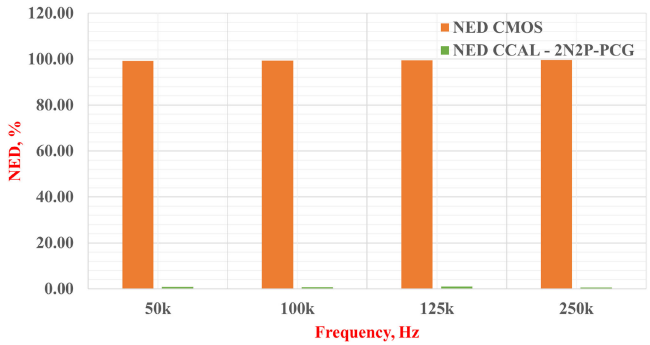

FIGURE 10. NED value comparison for XOR logic gate.

has a significantly smaller value of NED and NSD compared to CMOS AND logic. The average NED value for CCAL AND logic gate is 10.81% compared to 99.39% in its CMOS counterpart for the frequency range of 50 kHz to 250 kHz. This results in 89.13% better NED value in CCAL AND logic. Similarly, we can see an average of 96.45% better NSD value in CCAL AND logic gate compared to its CMOS counterpart in the same frequency range.

Similar to the AND logic gate, we repeated the simulation experiment for the XOR logic gates for all four logic designs in consideration. Table 4 lists the summary of simulation results for the XOR logic gate for the frequency range of 50 kHz to 250 kHz. We can see in Table 4 that the CCAL XOR logic gate has superior energy performance results. The average of $_{avg}$ value, for the frequency range of 50 kHz to 250 kHz, in the CCAL XOR logic gate is 5.40 fJ. However, in the same CMOS, 2-EE-SPFAL [35], and 2-SPGAL [36] counterparts have an average of $_{avg}$ values are 13.0968 fJ, 11.6237 fJ, and 11.0453 fJ. Table 5 saving lists the energy saving in CCAL XOR logic gate compared to single-rail counterpart, CMOS, and dual-rail adiabatic logic counterpart 22-EE-SPFAL [35], and 2-SPGAL [36]. The CCAL XOR logic gate saves on an average more than 58% energy compared to CMOS, and 53% and 51% more energy saving compared to 2-EE-SPFAL [35], and 2-SPGAL [36] based XOR gate respectively.

Figs. 10 and 11 graphically show the comparison of NED and NSD security metric performance for CCAL and CMOS XOR logic gate. Similar to the AND logic gate, the CCAL based XOR logic gate is superior in NED and NSD security metric performance. The CCAL XOR logic gate has an average of 99.23% better NED value compared to the CMOS XOR logic gate over the frequency range of 50 kHz and 250 kHz. Further, an average of 99.61% better NSD value is noted for the CCAL XOR logic gate compared to its CMOS counterpart in the same frequency range.

TABLE 4. Energy-Efficiency and Security Performance Comparison for XOR Logic Gate

	50 kHz				100 kHz			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	0.2459	11.7161	11.1072	5.5896	0.1529	11.5779	11.0179	5.3592
$E_{max}(fJ)$	32.5163	11.7165	11.1077	5.6366	25.9986	11.5783	11.0184	5.3926
$E_{avg}(fJ)$	16.3697	11.7163	11.1075	5.6114	13.0968	11.5781	11.0181	5.3775
NED (%)	99.244	0.003	0.004	0.833	99.412	0.004	0.004	0.619
NSD (%)	69.537	0.001	0.002	0.284	69.671	0.002	0.002	0.210
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	0.1250	11.5692	10.9915	5.3095	0.0919	11.6306	11.0635	5.2555
$E_{max}(fJ)$	22.8099	11.5698	10.9921	5.3643	22.7796	11.6313	11.0642	5.2870
$E_{avg}(fJ)$	11.4741	11.5695	10.9918	5.3405	11.4466	11.6309	11.0638	5.2711
NED (%)	99.452	0.005	0.006	1.1023	99.597	0.006	0.007	0.595
NSD (%)	69.752	0.003	0.003	0.389	69.906	0.003	0.003	0.206

TABLE 5. E_{avg} - Energy Saving (In %) in CCAL XOR Logic Gate

Type of the logic	Baseline Logic to compare	50 kHz	100 kHz	125 kHz	250 kHz
Dual-Rail Adiabatic	2-EE-SPFAL [35]	52.11	53.55	53.84	54.68
	2-SPGAL [36]	49.48	51.19	51.41	52.36
Single-Rail	Conventional CMOS	65.72	58.94	53.46	53.95

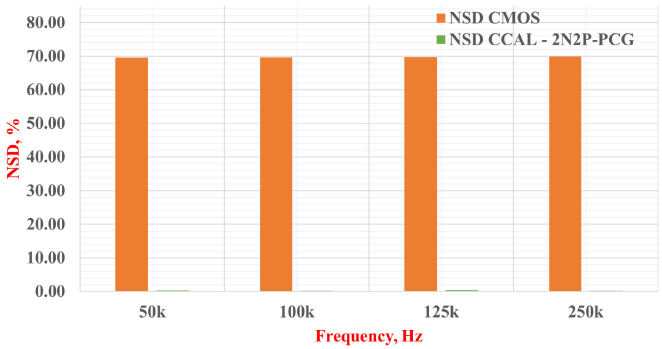

FIGURE 11. NSD value comparison for XOR logic gate.

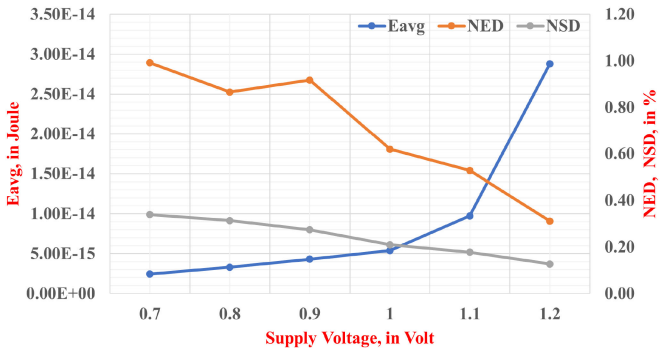

FIGURE 12. E_{avg}, NED and NSD metric in CCAL-based XOR logic gate as a function of the supply voltage.

Fig. 12 helps to understand the relation between the E_{avg} and supply voltage at frequency value 100 kHz, for CCAL-based XOR logic gate, with 2N2P-PCG integrated into the design. We also plotted the corresponding NED and NSD value along with E_{avg} on the same graph. We see that E_{avg} is decreasing with lowering the supply voltage. However, the security performance metric NED and NSD are higher with low supply voltage. The CCAL-based XOR logic gate shows better security performance as the supply voltage reaches a higher value. The better security performance is attributed to the minimum deviation in energy number.

It is important to note that NED and NSD values in dual-rail adiabatic logic (2-EE-SPFAL [35], and 2-SPGAL [36]) compared to single-rail adiabatic logic CCAL. This is expected behavior as dual-rail circuit uses two balanced switching logic evaluation networks F and $\overline{F}$. The switching in the evaluation block happens in a complementary fashion. Thus, the more uniformity in current results in logic gate output. However, for practical side-channel attacks (e.g. CPA in our case), it becomes important to check whether the CCAL based encryption circuit can prevent the revelation of the encryption key. The later part of the paper explains the CPA attack performance results over CCAL logic-based case-study implementation of the lightweight cryptographic cipher.

IV. A CRYPTOGRAPHIC CIRCUIT CASE-STUDY: PRESENT-80 S-BOX DESIGNED USING CCAL

In this section, first, we provide background information on lightweight cryptographic cipher PRESENT. The Substitution-box (S-box) is a vital component in the PRESENT cipher. We use the S-box as case-study implementation and show the comparison of transistor count implementation in adiabatic logic CCAL, 2-EESPFAL [35] and 2-SPGAL [36]. We also provide energy and security metric performance of the case-study design with 2N2P-PCG integrated into the design.

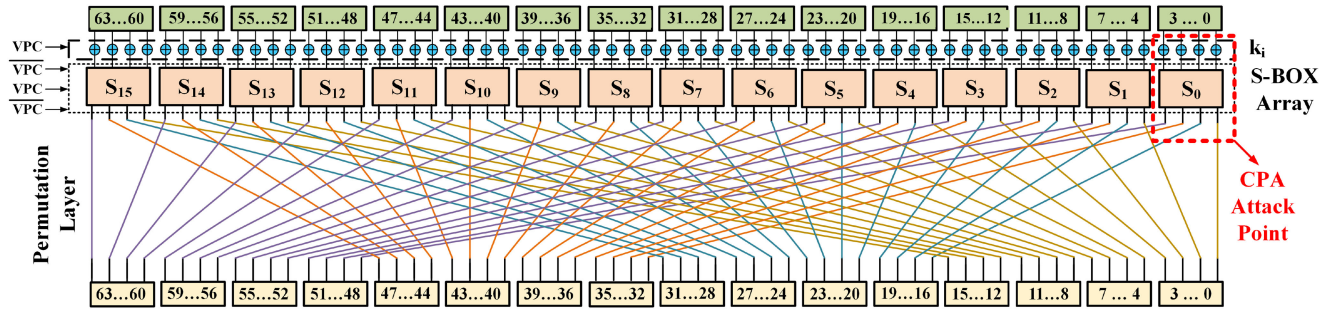

FIGURE 13. one round of PRESENT-80 implementation using 2-phase adiabatic logic [36].

TABLE 6. Transistor Count in PRESENT-80 S-Box Designed Using Dual-Rail Logic

Logic Gates	Number of Logic Gates	Total Transistor Counts 2-EE-SPFAL [35]	2-SPGAL [36]
Buffer	12	96	72
AND	16	224	192
OR	8	112	96
XOR	7	84	70

TABLE 7. Transistor Count in PRESENT-80 S-Box Designed Using Single-Rail Logic

Logic Gates	Number of Logic Gates	Total Transistor Counts CCAL	CMOS
AND	16	128	96
OR	8	64	48
XOR	4	40	32
XNOR	4	48	40

A. BACKGROUND ON PRESENT-80

The cryptographic cipher used in medical devices should be low-power and lightweight as they run on battery and have limited silicon space. PRESENT is one such popular lightweight cryptographic cipher [52]. Further, the counter mode operation in the PRESENT makes it suitable in challenge-response authentication [53]. The PRESENT comes in two variants based on the key size, 80-bit or 120-bit. The PRESENT-80, is an 80-bit key variant with a total of 32 rounds of encryption. In PRESENT-80, the first 31 rounds of encryption are identical and its schematic is shown in Fig. 13.

The PRESENT-80 has three fundamental operations. First, the plain text is XORed with 64 bits of the key. During the second operation, the Substitution-box (S-box) does a non-linear transformation of the 4-bit blocks, with a total of 16 such operations happening in parallel. The last operation is the permutation of S-box output to create further randomization. The S-box is the key constituent of PRESENT-80. Therefore, in this work, we have evaluated the transistor counts, energy efficiency, and security metrics performance comparison for S-box for 2-EE-SPFAL [35], 2-SPGAL [36], CCAL, and CMOS.

B. TRANSISTOR COUNT SAVING ANALYSIS IN CCAL-BASED CASE-STUDY IMPLEMENTATION OF PRESENT-80 S-BOX

We can see from Fig. 13 that S-box is a critical part of the PRESENT-80 implementation. In this section, we explain the S-box circuit implementation using four different logic circuits, i.e. 2-EE-SPFAL [35], 2-SPGAL [36], CCAL, and CMOS.

Table 6 illustrates the number of the transistors required to implement PRESENT-80 S-box using dual-rail adiabatic logic. The dual-rail adiabatic logic inherently works in pipeline fashion. In other words, the successive blocks of the circuits operate on different phases. In case of 2-phase clock, they are in-phase and out-of-phase [35], [36]. In order to make the output appear on the same clock phase, we need to put extra buffers for synchronization.

TABLE 8. Transistor Count Comparison for CCAL, 2-EE-SPFAL [35], 2-SPGAL [36] and Conventional CMOS for PRESENT-80 S-Box Design

Logic	Number of Transistors	Overhead compared to CMOS, in %	Transistor Saving in CCAL, in %
2-EE-SPFAL [35]	516	138.89	**45.74**
2-SPGAL [36]	430	99.07	**34.88**
CCAL	280	29.63	–
CMOS	216	–	–

Table 7 represents the number of logic gates and transistor count for PRESENT-80 S-box implemented using single-phase logic. The PRESENT-80 S-box implementation using CCAL is similar to CMOS-based implementation, except it requires two complementary sinusoidal power clocks and two extra transistors for clocking circuitry on top of the logic evaluation network. In the previous section, we have seen that the CCAL logic gates require significantly less energy consumption, as well as improve the resilience against the CPA attack.

Table 8 presents the comparison of the number of transistors required to implement PRESENT-80 S-box for different logic. The dual-rail adiabatic logic has more balanced switching activities, thus resulting in a more secure structure against CPA. However, the inherent structure of dual-rail logic results in more transistor counts. The transistor count overhead in 2-EE-SPFAL [35], and 2-SPGAL [36] compared to their CMOS-based S-box counterpart is approximately 139% and 99% respectively. On the other hand, the transistor overhead in CCAL based CMOS is 29.63%. Further, the CCAL based

TABLE 9. Energy-Efficiency and Security Performance Comparison for PRESENT-80 S-Box

	50 kHz				100 kHz			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	16.1017	111.8714	80.0749	72.1344	8.0508	106.7929	78.3831	68.4080
$E_{max}(fJ)$	24427.7700	120.2409	84.0927	82.1965	13822.5800	114.3578	84.5114	78.1032
$E_{avg}(fJ)$	3713.2974	116.3666	81.4804	78.5836	2251.8734	110.3418	80.0390	74.4624
NED (%)	99.93	6.96	4.78	12.24	99.94	6.62	7.25	12.41
NSD (%)	151.09	1.28	0.96	2.07	147.00	1.31	1.18	2.10
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**	**CMOS**	**2-EE-SPFAL** [35]	**2-SPGAL** [36]	**CCAL**
$E_{min}(fJ)$	6.4407	105.8047	78.1838	67.3192	3.2203	103.2192	77.6512	64.2043
$E_{max}(fJ)$	11375.7700	113.0351	83.0035	76.8905	709.6414	110.2786	82.4870	73.7168
$E_{avg}(fJ)$	1785.2113	109.0232	79.8261	73.3781	175.7356	106.2688	79.3894	70.4930
NED (%)	99.94	6.40	5.81	12.45	99.55	6.40	5.86	12.90
NSD (%)	151.00	1.30	1.19	2.11	88.77	1.30	1.20	2.19

TABLE 10. E_{avg} - Energy Saving (In %) in CCAL Based PRESENT-80 S-Box

Type of the logic	Baseline Logic to compare	50 kHz	100 kHz	125 kHz	250 kHz
Dual-Rail Adiabatic	2-EE-SPFAL [35]	32.47	32.52	32.70	32.67
	2-SPGAL [36]	3.56	6.97	8.08	11.21
Single-Rail	Conventional CMOS	97.88	96.69	95.89	59.89

S-box implementation saves 34.88% and 45.74% of transistor count compared to dual-rail logic 2-EE-SPFAL [35], and 2-SPGAL [36] respectively. For the space-limited IoT structure, the CCAL logic presents an alternative to design secure cryptographic circuits with less transistor overhead.

C. ENERGY AND SECURITY PERFORMANCE EVALUATION OF CASE-STUDY DESIGN PRESENT-80 S-BOX

The CCAL based logic gates shows 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 CCAL and CMOS logic gates. The S-Box implementation requires both VPC and $\overline{VPC}$ phases (Fig. 13) of power clock to operate. The S-box designs using adiabatic logic were tested with 2N2P-PCG.

Table 9 lists the energy-efficiency performance and calculated NED and NSD metrics. The energy consumption for adiabatic circuits was calculated for 2N2P-PCG integrated into the design. Similar to the logic gates, we collected the energy number in SPICE simulation for the frequency range 50 kHz to 250 kHz. The PRESENT-80 S-box circuit was designed at 45 nm technology and the load value was considered 10 fF. We can see in Table 10 that CCAL based S-box shows better energy performance than CMOS, 2-EE-SPFAL [35] and 2-SPGAL [36] over frequency range 50 kHz to 250 kHz. The average of E_{avg} for CCAL based S-box is 74.23 fJ for the frequency range 50 kHz to 250 kHz. For the same frequency range, the average of E_{avg} in CMOS, 2-EE-SPFAL [35] and 2-SPGAL [36] is approximately 1981 fJ, 110 fJ and 80 fJ respectively. Therefore, adding a clocking network on top of the pmos and nmos circuit helps to reduce the energy consumption value.

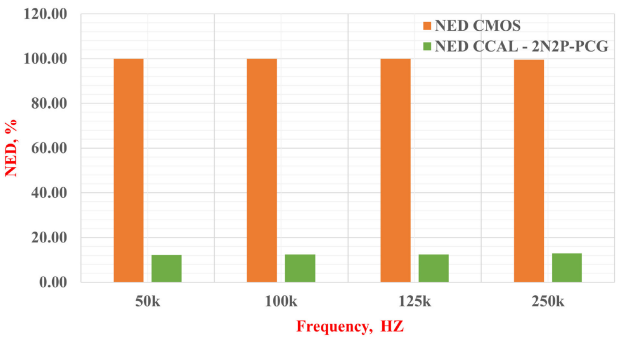

FIGURE 14. NED value comparison for PRESENT-80 S-box.

Similar to logic gate, it is interesting to see the NED and NSD performance between CCAL and CMOS. Figs. 14 and 15 shows graphical comparison for NED and NSD values in CCAL and CMOS for S-box circuit. The NED and NSD values in CCAL based PRESENT-80 S-box is overall lower for the frequency range 50 kHz to 250 kHz. The average NED value for the CCAL S-box is 12.50%, while in CMOS S-box it is 99.84% over frequency range 50 kHz to 250 kHz. The CCAL based S-box shows overall 97.48% improvement in NED security metric. Similarly, the NSD performance in CCAL-based S-box is average of 2.12% over frequency range 50 kHz to 250 kHz. For same frequency range, CMOS-based S-box have an average NSD value 134.46%. The CCAL-based S-box have overall 98.43% better NSD performance for frequency range 50 kHz to 250 kHz.

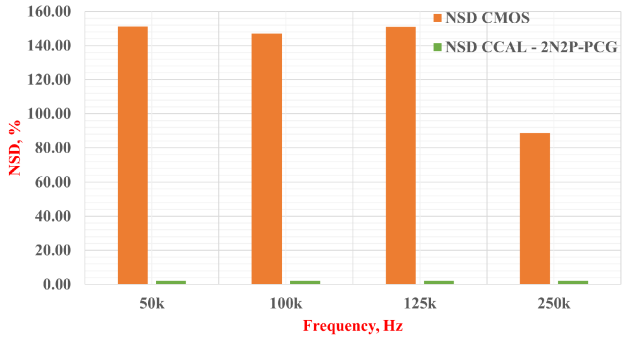

FIGURE 15. NSD value comparison for PRESENT-80 S-box.

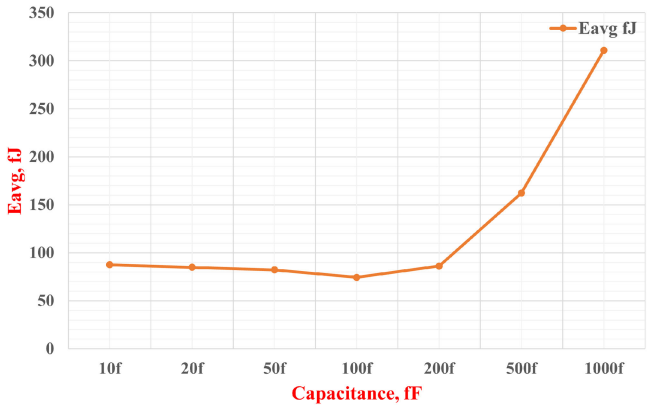

FIGURE 16. Effect of varying capacitor and inductor values over Average energy consumption in PRESENT-80 S-xox.

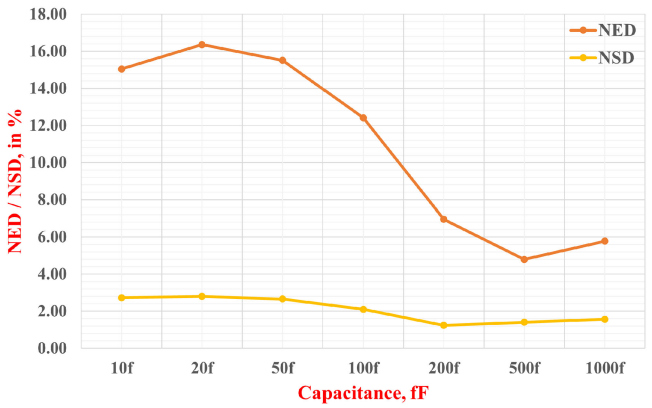

FIGURE 17. Effect of varying capacitor and inductor values over NED and NSD in PRESENT-80 S-box.

The CCAL-based S-box shows better security metric performance compared to its CMOS counterpart. We can see that CCAL-based S-box has better energy-efficiency performance compared to its dual-rail adiabatic counterpart. However, the dual-rail adiabatic logic, 2-EE-SPFAL [35] and 2-SPGAL [36] have better NED and NSD performance. The better security performance in dual-rail logic is an attribute of the balance switching activities in logic evaluation network. However, the CCAL has significant security performance improvement compared to CMOS. It will be interesting to see the performance of the CCAL based circuit against the CPA attack (explained in the next section).

V. EFFECT OF VARYING CAPACITOR AND INDUCTOR IN LC TANK IN 2N2P-PCG FOR ENERGY-EFFICIENCY AND SECURITY PERFORMANCE ANALYSIS IN CASE-STUDY

The Q factor is a key parameter in the power analysis of the RLC resonator circuit. When the adiabatic circuit is integrated with 2N2P-PCG (Fig. 3) then it can be modeled as an RLC circuit. (6) shows the relation between the Q factor and average power dissipation. We need a larger Q factor in order to have minimum power dissipation. However, in the RLC circuit, the Q factor of the LC tank circuit depends upon the Q factor of inductor and capacitor with their parasitic resistance respectively [54].

$$Q = 2\pi \frac{\text{Maximum Energy Stored}}{\text{Energy Dissipated per Cycle}} \tag{6}$$

Equation (7) shows the dependence of the Q factor of 2N2P-PCG tank circuit on Q factor of inductor ($Q_L = \frac{R_L}{\omega_0 L}$) and capacitor ($Q_C = \omega_0 C R_C$) respectively. In the above equations, R_L is the parasitic resistance of the inductor, and R_C is the parasitic resistance of the capacitor [54]. Therefore, we hypothesize that there will be a certain value of the inductor and capacitor for which the Q factor is maximum. Higher Q can result in lower energy dissipation. Further, it will also be interesting to see the effect on security performance metrics.

$$Q_{\text{tank}} = \omega_0 C \left(R_L \| R_C\right) = Q_L \| Q_C \tag{7}$$

To check our hypothesis, we fixed the frequency value to 100 kHz. We calculated the different combinations of L and C (4) for the frequency 100 kHz. Similar to the logic gate energy and security experiment, we collected energy consumption values for a total of 256 cyclic combinations of the inputs in CCAL-based S-box circuitry. Fig. 16 shows the E_{avg} at different capacitive value in LC tank circuit in 2N2P-PCG circuit. We can see that the lowest E_{avg} value of 74.46 fJ at capacitor value 100 fF.

Further, we can also observe the effect on security performance metrics NED and NSD. Fig. 17 shows the change in NED and NSD values at different values of the capacitors. The lowest NED and NSD values are observed are 4.79% and 1.40% at capacitor value 500 fF. The graph in Fig. 17 helps to understand the capability of the circuit to thwart the Correlation Power Analysis (CPA) attack. The lowest value of NED and NSD indicates that the circuit is more robust against CPA at 500 fF capacitance value in 2N2P-PCG.

We define the energy-security trade-off product as $Energy \times Security$ and measure in Joule. Previously, we have seen that the energy and security metrics performance shows the different trend for PCG tank capacitor C_E values. The case-study implementation shows optimum energy performance for C_E value of 100 fF and security performance at 500 fF. For optimum energy and security performance, the trade-off product $Energy \times Security$ should be minimum. Fig. 18

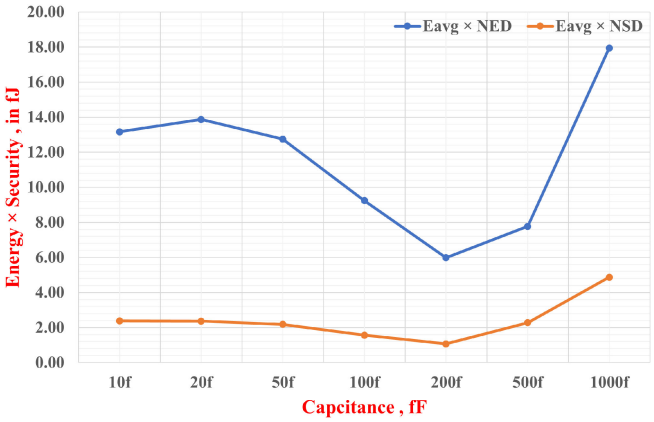

FIGURE 18. Energy-security trade-off in PRESENT-80 S-box designed using CCAL.

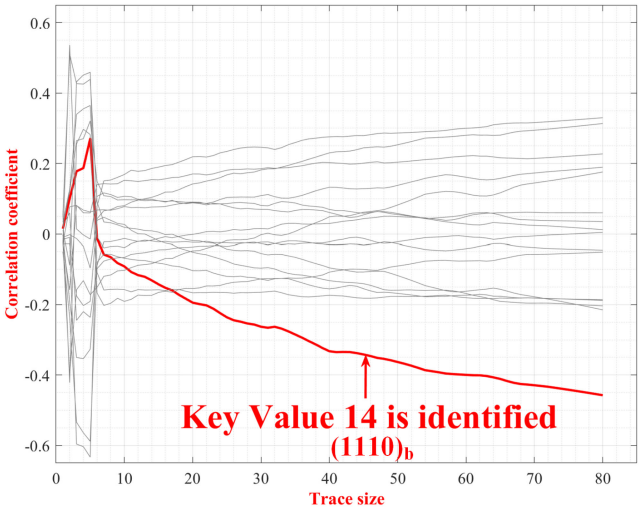

FIGURE 19. Successful Revelation of Key=14 in on one round of PRESENT-80 encryption designed with CMOS.

shows an insight for the energy and security performance metrics together at different tank capacitor values. We can see that for capacitor value 200 fF has the lowest $E_{avg} \times NED$ and $E_{avg} \times NSD$ equal to $5.98fJ$ and $1.07fJ$ respectively. Thus, we can say that having 200 fF value of tank capacitor (C_E) in 2N2P-PCG can provide optimum energy and security performance together.

VI. CPA ATTACK SIMULATION

In the previous section, we demonstrated the efficacy of the CCAL to design low-energy and CPA resilient cryptographic circuits. The CCAL based S-box was energy efficient, however, the NED and NSD performance were relatively higher compared to Dual-Rail adiabatic logics 2-EE-SPFAL [35] and 2-SPGAL [36]. In this section, we subject the CCAL based S-box design against the CPA. The article [55] illustrates the procedure to carry out the CPA in SPICE simulation. We can see in Fig. 13 that one round of PRESENT-80 encryption contains 16 identical blocks. Each block has four XOR logic gates and a non-linear transformation circuit, called S-box. Therefore, the output of S-box is considered as CPA attack point in the literature [35], [36], [43], [55]. The S-box takes the 4-bit input coming after XOR operation between the 4-bit key value and plain-text.

The CPA attack requires the power traces collected from the attack point. The SPICE simulation was performed with a load value of 10 fF to collect the power traces. The simulation environment is noise-free and requires fewer traces for successful CPA. If a CPA attack is carried out in a noisy environment then it requires a larger number of traces. We collected power traces for the CMOS-based PRESENT-80 S-Box. The CPA attacks reveal the correct encryption key after 5120 power traces. Fig. 19 shows the correlation coefficient starts appearing different after 40 power traces. The distinct power consumption, therefore, the current makes the CPA successful over the CMOS-based S-box of PRESENT-80 encryption.

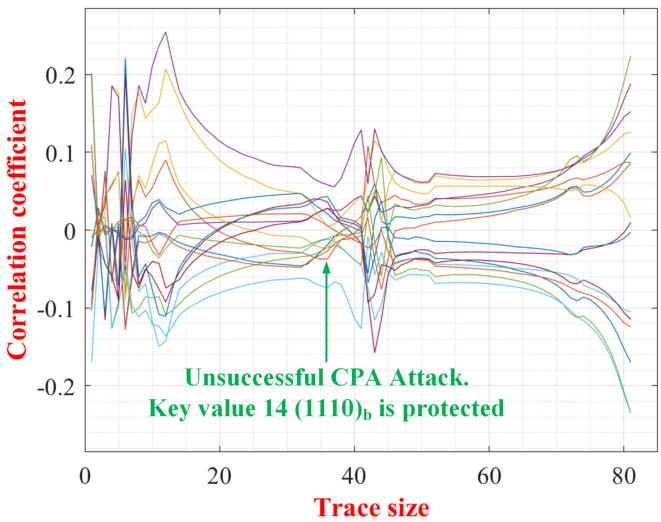

FIGURE 20. Unsuccessful CPA attack on one round of PRESENT-80 encryption designed with CCAL and 2N-PCG.

The CCAL based S-box has better NED and NSD performance compared to CMOS. However, dual-rail adiabatic logic, e.g. 2-EE-SPFAL [35], and 2-SPGAL [36] have better NED and NSD values. It becomes important to see if CCAL based PRESENT-80 S-box is safe against the CPA attack. Similar to CMOS, we collected 12,000 power traces for the CCAL based PRESENT-80 S-box with 2N2P-PCG integrated into the design. Similar to our previous work on dual-rail adiabatic logic, 2-EE-SPFAL [35] and 2-SPGAL [36], the CCAL based S-box circuit protects the revelation of the encryption key (Fig. 20). Therefore, higher NED and NSD value in CCAL compared to dual-rail logic does not affect the properties to protect the encryption key against the CPA attack.

VII. DISCUSSION AND CONCLUSION

The cost and the reliability of the medical devices are the important factors to consider while selecting a technology with adiabatic logic. Bulk MOSFET at 45 nm combined with adiabatic logic will provide a low-cost solution for medical devices that can also provide an energy-efficient and secure solution. Novel devices such as Junctionless MOSFET [56] and Tunnel FET [57] can also be explored with adiabatic logic for developing low-power and secure solutions. However, the designer should consider the cost and the reliability of the emerging devices when combined with adiabatic logic while making the design choice for medical devices. The low-frequency medical devices are vulnerable to side-channel attacks (e.g. Correlation Power Analysis (CPA) attack). The conventional approach to improve the CPA resistance results in an increase in power consumption. In this article, we used the single rail adiabatic circuit design technique called Clocked CMOS Adiabatic Logic (CCAL) to design cryptographic circuits in low-frequency medical devices. CCAL shows encouraging energy-saving and security performance compared to its dual-rail adiabatic logic and CMOS counterparts. Further, the CCAL enables the designer to reduce the transistor count in cryptographic hardware compared to existing solutions based on adiabatic logic proposed in the literature. We also demonstrated the capability of the CCAL based logic to thwart the CPA attack and protect the encryption key. Therefore, CCAL can be a promising design choice for the designer of medical devices to increase their battery longevity with improved CPA resistance while keeping the transistor overhead to minimal. While designing single rail adiabatic logic circuits, the stability in the outputs should be considered while cascading the designs. The stable outputs can be produced by inserting the flip-flop to sample the correct output at each stage [58]. Another alternative approach to provide stable outputs could be to use noise reduction circuitry that can be added to restore the signal degraded [59]. Some possible future research direction would be to check the performance of the CCAL-based circuit implementation with different types of Power Clock Generator, e.g., switch capacitor, stepwise charging, etc.

REFERENCES

[1] World Health Organization, "Obesity and overweight," World Health Organization, Accessed on: Oct. 2, 2021. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/obesity-and-overweight

[2] Center for disease control (CDC), "Chronic disease in america," Accessed on: Oct. 2, 2021. [Online]. Available: https://www.cdc.gov/chronicdisease/tools/infographics.htm

[3] T. G. Mahn, "Wireless medical technologies: Navigating government regulation in the new medical age," *Fishs Regulatory Government Affairs Group*, 2013. [Online]. Available: https://www.fr.com/wp-content/uploads/2017/09/2017.09.12-Wireless-Medical-Technologies-Navigating-Government-Regulation.pdf

[4] *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 Standard ETSI EN 302 195 V2.1.1, Jun. 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_en/302100_302199/302195/02.01.01_60/en_302195v020101p.pdf

[5] S. Hanna, "Regulations and standards for wireless medical applications," in *Proc. 3rd Int. Symp. Med. Inf. Commun. Technol.*, 2009, pp. 23–26.

[6] E. Völgyi, F. A. Tylavsky, A. Lyytikäinen, H. Suominen, M. Alén, and S. Cheng, "Assessing body composition with DXA and bioimpedance: Effects of obesity, physical activity, and age," *Obesity*, vol. 16, no. 3, pp. 700–705, 2008.

[7] S. B. Rutkove, K. S. Lee, C. A. Shiffman, and R. Aaron, "Test-retest reproducibility of 50 KHz linear-electrical impedance myography," *Clin. Neuriophysiol.*, vol. 117, no. 6, pp. 1244–1248, 2006.

[8] H. Wi, H. Sohal, A. L. McEwan, E. J. Woo, and T. I. Oh, "Multi-frequency electrical impedance tomography system with automatic self-calibration for long-term monitoring," *IEEE Trans. Biomed. Circuits Syst.*, vol. 8, no. 1, pp. 119–128, Feb. 2014.

[9] Y. Yang and J. Jia, "A multi-frequency electrical impedance tomography system for real-time 2D and 3D imaging," *Rev. Sci. Instruments*, vol. 88, no. 8, 2017, Art. no. 0 85110.

[10] "Eit pioneer set," Swisstom AG, Switzerland, Accessed on: Oct. 1, 2021. [Online]. Available: http://www.swisstom.com/wp-content/uploads/Swisstom_brochure-PioneerSet_GB_1ST500-102_Rev002_web.pdf

[11] A. Hedayatipour, S. Aslanzadeh, S. H. Hesari, M. A. Haque, and N. McFarlane, "A wearable CMOS impedance to frequency sensing system for non-invasive impedance measurements," *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 5, pp. 1108–1121, Oct. 2020.

[12] L. Gerlach, G. Payá-Vayá, and H. Blume, "A survey on application specific processor architectures for digital hearing aids," *J. Signal Process. Syst.*, pp. 1–16, 2021.

[13] C. Kuhlmann *et al.*, "Drive-field frequency dependent MPI performance of single-core magnetite nanoparticle tracers," *IEEE Trans. Magn.*, vol. 51, no. 2, Feb. 2015, Art. no. 6500504.

[14] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[15] M. Zhang, A. Raghunathan, and J. K., "Towards trustworthy medical devices and body area networks," in *Proc. 50th Annu. Des. Automat. Conf.*, 2013, pp. 1–6.

[16] "Medical applications user guide," NXP Semiconductors, Accessed on: Oct. 1, 2021. [Online]. Available: https://www.nxp.com/docs/en/user-guide/MDAPPUSGDRM118.pdf

[17] L. Bu and M. G. Karpovsky, "A design of secure and reliablewireless transmission channel for implantable medical devices," in *Proc. 3rd Int. Conf. Inf. Syst. Secur. Privacy*, 2017, pp. 233–242.

[18] L. Bu, M. G. Karpovsky, and M. A. Kinsy, "Bulwark: Securing implantable medical devices communication channels," *Comput. Secur.*, vol. 86, pp. 498–511, 2019.

[19] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. E-Health Netw., Appl. Serv.*, 2011, pp. 150–156.

[20] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy* 2008, pp. 129–142.

[21] 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. ACM SIGCOMM Conf.*, 2011, pp. 2–13.

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

[23] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," Tech. Rep. MSR-TR-2017-16, 2017.

[24] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Minimum on-the-node data security for the next-generation miniaturized wireless biomedical devices," in *Proc. IEEE 63rd Int. Midwest Symp. Circuits Syst.*, 2020, pp. 1068–1071.

[25] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE Glob. Telecommun. Conf.*, 2010, pp. 1–5.

[26] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.

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

[28] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices," in *Proc. 205th Int. Symp. Med. Inf. Commun. Technol.*, 2011, pp. 6–9.
[29] J. Fan, O. Reparaz, V. Rožić, and I. Verbauwhede, "Low-energy encryption for medical devices: Security adds an extra design dimension," in *Proc. 50th Annu. Des. Automat. Conf.*, 2013, pp. 1–6.
[30] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *Proc. 26th Int. Conf. VLSI Des. 12th Int. Conf. Embedded Syst.*, 2013, pp. 203–208.
[31] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptology Conf.*, 1999, pp. 388–397.
[32] 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 *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 1998, pp. 167–182.
[33] T. N. Theis and P. M. Solomon, "In quest of the 'Next Switch': Prospects for greatly reduced power dissipation in a successor to the silicon field-effect transistor," *Proc. IEEE*, vol. 98, no. 12, pp. 2005–2014, Dec. 2010.
[34] T. N. Theis and H.-S. P. Wong, "The end of Moore's law: A new beginning for information technology," *Comput. Sci. Eng.*, vol. 19, no. 2, pp. 41–50, 2017.
[35] Z. Kahleifeh and H. Thapliyal, "2-phase energy-efficient secure positive feedback adiabatic logic for CPA-resistant IoT devices," in *Proc. IEEE 6th World Forum Internet Things*, 2020, pp. 1–5.
[36] A. Degada and H. Thapliyal, "2-SPGAL: 2-phase symmetric pass gate adiabatic logic for energy-efficient secure consumer IoT," in *Proc. IEEE Int. Conf. Consum. Electron.*, 2021, pp. 1–6.
[37] H. Li, Y. Zhang, and T. Yoshihara, "Clocked CMOS adiabatic logic with low-power dissipation," in *Proc. Int. SoC Des. Conf.*, 2013, pp. 0 64–067.
[38] J. A. Ambrose, R. G. Ragel, and S. Parameswaran, "RIJID: Random code injection to mask power analysis based side channel attacks," in *Proc. 44th Annu. Des. Automat. Conf.*, 2007, pp. 489–492.
[39] D. May, H. L. Muller, and N. P. Smart, "Non-deterministic processors," in *Proc. Australasian Conf. Inf. Secur. Privacy*, 2001, pp. 115–129.
[40] D. May, H. Muller, and N. Smart, "Random register renaming to foil DPA," in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.*, 2001, pp. 28–38.
[41] K. Tiri *et al.*, "A side-channel leakage free coprocessor IC in 0.18 μm CMOS for embedded AES-based cryptographic and biometric processing," in *Proc. 42nd Annu. Des. Automat. Conf.*, 2005, pp. 222–227.
[42] A. Moradi and A. Poschmann, "Lightweight cryptography and DPA countermeasures: A survey," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2010, pp. 68–79.
[43] 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. VLSI J.*, vol. 58, pp. 369–377, 2017.
[44] 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. Syst.*, vol. 2, no. 4, pp. 398–407, Dec. 1994.
[45] 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., Regular Papers*, vol. 62, no. 1, pp. 149–156, Jan. 2015.
[46] 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.
[47] H. S. Raghav and I. Kale, "A balanced power analysis attack resilient adiabatic logic using single charge sharing transistor," *Integr. VLSI J.*, vol. 69, pp. 147–160, 2019.
[48] C. Monteiro, Y. Takahashi, and T. Sekine, "Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks," in *Proc. 36th IEEE Int. Conf. Telecommun. Signal Process.*, 2013, pp. 732–736.
[49] B. Fadaeinia and A. Moradi, "3-phase adiabatic logic and its sound SCA evaluation," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 2175–2188, 1 Oct.–Dec. 2021.
[50] H. Mahmoodi-Meimand and A. Afzali-Kusha, "Efficient power clock generation for adiabatic logic," in *Proc. IEEE Int. Symp. Circuits Syst. (Cat. No 01CH37196)*, 2001, pp. 642–645.
[51] Y. Takahashi, T. Sekine, and M. Yokoyama, "Two-phase clocked CMOS adiabatic logic," *Far East J. Electron. Commun.*, vol. 3, no. 1, pp. 17–34, 2009.
[52] A. Bogdanov *et al.*, "Present: An ultra-lightweight block cipher," in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.*, 2007, pp. 450–466.
[53] M. J. Dworkin, *A Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. National Inst. Standards Technol., SP 800-38, 2001.
[54] Y. Zhang, "Research on low power technology by ac power supply circuits," Ph.D. dissertation, Waseda Univ., Tokyo, Japan, 2012.
[55] 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, Oct. 2012.
[56] S. Roy, G. Jana, and M. Chanda, "Analysis of sub-threshold adiabatic logic model using junctionless MOSFET for low power application," *Silicon*, pp. 1–9, 2021.
[57] J.-S. Liu, M. B. Clavel, and M. K. Hudait, "TBAL: Tunnel FET-based adiabatic logic for energy-efficient, ultra-low voltage IoT applications," *IEEE J. Electron. Devices Soc.*, vol. 7, pp. 210–218, Jan. 2019.
[58] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, "Ultra-lightweight implementations for smart devices-security for 1000 gate equivalents," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 2008, pp. 89–103.
[59] Y. Ye and K. Roy, "QSERL: Quasi-static energy recovery logic," *IEEE J. Solid-State Circuits*, vol. 36, no. 2, pp. 239–248, Feb. 2001.

AMIT DEGADA (Graduate Student Member, IEEE) recieved the Masters of Technology degree from the Sardar Vallabhbhai National Institute of Technology Surat, Surat, India. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. His research focuses on the development of hardware assisted cybersecurity primitives for consumer IoT applications.

HIMANSHU THAPLIYAL (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the University of South Florida, Tampa, FL, USA, in 2011. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA. From 2012 to 2014, he was a Designer of processor test solutions with Qualcomm. In 2014, he was an Assistant Professor with the University of Kentucky, Lexington, KY, USA, where he got promoted to an Associate Professor, in 2020. He has authored more than 150 publications that have resulted in over 4700 citations with h-index = 40 (Google Scholar). His research interests include hardware security of IoT and vehicles, quantum computing, and smart healthcare solutions for older adults and Alzheimer's Disease and Related Dementias (ADRD). 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 was the recipient of the NSF CAREER Award, and IEEE-CS TCVLSI Mid-Career Research Achievement Award, the 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), 2012 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Distinguished Graduate Achievement Award from the University of South Florida, and the Qualcomm QualStar Award for contributions to memory built-in self-test from Qualcomm, the Provost's Wethington Award for contributions to the University of Kentucky Research Program. He He is the steering committee Vice-Chair of the IEEE Symposium on Smart Electronic Systems. He was the General Chair of the 2020 IEEE Symposium on Smart Electronic Systems. He was 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 currently 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 the Senior Associate Editor of the *IEEE Consumer Electronics Magazine*, an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, and the Editorial Board Member of the *Microelectronics Journal*.