Hardware Trojan Detection in Implantable Medical Devices Using Adiabatic Computing

Zach Kahleifeh, S. Dinesh Kumar, Himanshu Thapliyal
Department of Electrical and Computer Engineering
University of Kentucky, Lexington, KY, USA
Email: hthapliyal@uky.edu

***Abstract*—In recent years, Hardware Trojans (HT) have become an increasing concern due to outsourcing the manufacturing of Implantable Medical Devices (IMDs). Power Analysis based Side-Channel Attack (SCA) is one of the main methods of detecting HT in IMDs. However, using SCA in detecting trojans is limited by the large process variation effects in IC technology which has reduced detection sensitivity of ultra-small trojans. Along with the safety of IMDs against HTs, the need for power management has also risen in parallel with the increasing complexity of IMDs. In this paper, we are analyzing the usefulness of Differential Power Analysis (DPA) resistant adiabatic logic gates to detect smaller trojans. DPA resistant adiabatic logic gates consume uniform power irrespective of input data transition and also consume lower power compared to conventional CMOS logic gates. When the HT is triggered in the DPA resistant circuits, the circuit will have non-uniform power consumption which will help us to easily identify HTs. In order to validate our proposed methodology, we have implemented a C17 and a carry save adder using a recently proposed DPA resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic Family (EE-SPFAL). Further, in order to calculate the true energy-efficiency of the EE-SPFAL logic, we have proposed a four phase Power Clock Generator (PCG) and integrated with the EE-SPFAL logic circuits. Simulations are performed in Cadence Spectre using 180nm CMOS technology. From our simulations, we have observed the non-uniform power consumption, during the activation of HT, in EE-SPFAL based C17 and carry save adder circuit. Further, EE-SPFAL based C17 and carry save adder along with its PCG consume 25.8% and 31.4% of less power as compared to the conventional CMOS based C17 and carry save adder respectively.**

I. Introduction

Implantable Medical Devices (IMD) have helped millions of patients to improve their quality of life every year. IMDs are devices that are being used to replace or act as a fraction of or whole biological structure. Currently, IMDs are used in different parts of the body for various applications such as orthopedics, cardiovascular stents, drug delivery system etc. Some of the examples of IMDs include pacemakers, cardiac defibrillators, nerve stimulators, bladder stimulators, diaphragm stimulator, etc [1]. A 2009 study reported that there were over a million pacemakers world-wide with at least 700,000 of them being new and over 200,000 being replaced or repaired [2]. This number does not include many other electrical based IMDs such as implantable infusion pumps, cardiac defibrillators, etc. Though IMDs help to improve the life of patients, they also equally present challenges in terms of security and power management.

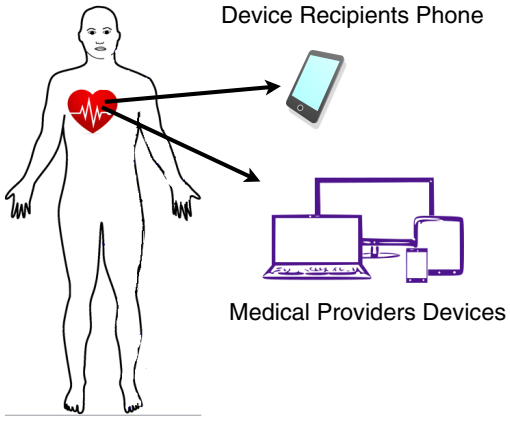


Fig. 1: Trojan Activation Effect

IMDs are very critical to security threats as they may potentially cause life-threatening situations to patients when not properly secured. Among the various security threats to IMDs, Hardware Trojans (HTs) can be considered as one of the emerging serious threats. Hardware Trojan (HT) attack is a type of hardware attack, where the advisory introduces the malicious modifications of a circuit during the design or fabrication [3]. HTs have already been detected in military chips with the purpose of extracting configuration data of the device [4]. It is not far fetched to think the same could happen to the chips inside IMDs [5]. For example, HTs in heart pacemakers to be activated upon specific event can generate unregulated electrical impulses which can cause the patient to lose their life. Another example would be an activated trojan in IMD can send faulty information to doctor which can cause serious threat to the patients as shown in Fig. 1.

There are various methods to detect HTs. Some of the HT detection method include logic testing, IP trust verification, side-channel analysis, etc [3]. Among the various HT detection methods, side-channel based approaches have been well studied in the literature, to detect the HTs in IMDs [6]. However, side-channel based approaches are limited due to the large process variation effect of ICs which results in reduced detection sensitivity of small trojans [7].

Further, IMDs are battery operated, which increases the concern for power management. Battery operated IMDs, such as pacemakers and defibrillators, are required to operate with

978-1-5386-9170-0/18/$31.00 ©2018 IEEE

a lower power consumption to increase battery life [8]. Increasing the security in IMDs comes along with the cost of battery life. In this paper, we are solving the problem of HT detection and power management in IMDs by using adiabatic logic technique.

Adiabatic logic technique is one of the low power design methodologies to design low-power hardware [9]. In the past, adiabatic logic has been well explored in the design of IMDs to reduce power consumption. For example, Schu et. al has implemented an adiabatic system in a pacemaker and has noticed considerable power savings [10]. In the recent years, adiabatic logic has also being well explored to solve several hardware security problems in low-power IoT devices such as resisting Differential Power Analysis attack, IC authentication, IC piracy, etc. [11]. However, HT detection in IMDs using adiabatic logic are not yet explored.

A. Contribution of this Paper

In this paper, we are solving the problem of HT detection in IMDs using Differential Power Analysis (DPA) resistant adiabatic logic circuits. DPA resistant adiabatic logic gates consume uniform power irrespective of input data transition and also consume lower power compared to conventional CMOS logic gates. If a CMOS gate is inserted in the DPA resistant adiabatic circuits, then we expect a power glitch to occur due to non-synchronization of power clock. We are using this principle to detect smaller trojans in DPA resistant adiabatic logic circuits. Further, our proposed approach also doesn't require a golden chip for the detection of HT.

As a case study, we have implemented a C17 and a carry save adder using the conventional CMOS logic and a recently proposed DPA resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL). The true energy-efficiency of adiabatic circuits are validated by calculating the energy consumption of adiabatic logic system with the integration of Power Clock Generator (PCG) and the adiabatic logic circuits. In this paper, we have proposed a four phase PCG and integrated it with the EE-SPFAL logic circuits. Simulations are performed in Cadence Spectre simulator using 180nm CMOS technology. From our simulations, we have observed that when a CMOS based HT is activated, EE-SPFAL based C17 and carry save adder circuit has non-uniform power consumption. Further, EE-SPFAL based C17 and carry save adder (with PCG) consume 25.8% and 31.4% of less power as compared to the conventional CMOS based C17 and carry save adder respectively.

B. Organization of this Paper

Section II presents a background on hardware trojans, current hardware trojan detection method and adiabatic logic circuits. Section III provides the brief explanation of a recently proposed DPA resistant adiabatic logic family called Energy-Efficient and Secure Positive Feedback Adiabatic Logic (EE-SPFAL). Section IV provides the description of our proposed four phase power clock generator used in our designs. Section V describes our proposed methodology to detect hardware trojan. Section VI provides the simulation results. Section VII concludes the paper.

II. Background

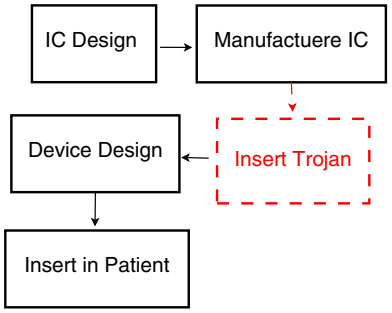


Fig. 2: Trojan Insertion in IC

A. Hardware Tojans

A Hardware Trojan (HT) is defined as an intentional, malicious circuit embedded in an IC to perform faulty operations for a specified set of inputs. There are three main spots in an IC fabrication process where the HT can be inserted [12]. These steps are design, fabrication and manufacturing test. In an IC design process, the chip is commonly designed by the commercially available CAD tools. However, the available standard cells, IP blocks, etc. are considered as untrusted. The fabrication step is considered as untrusted as an attacker can insert malicious circuits during the fabrication of an IC. Manufacturing test only if performed at the production center of client is considered as trusted. Fig. 2 shows the trojan insertion flow in an IC.

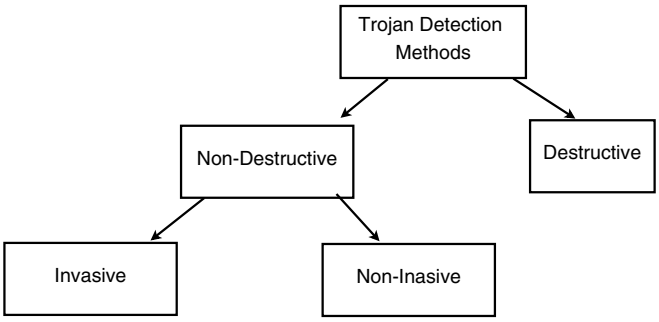


Fig. 3: Current Trojan Detection Methods

B. Current Trojan Detection Methods

There have been numerous proposed solutions to detect hardware trojans. The detection methods can be split into two categories, non-destructive and destructive. Non-destructive can be broken down further into invasive and non-invasive, Fig. 3 shows the broad classification of current HT detection methods [3]. Below is a brief description of each testing methods.

1) Non-Destructive: Non-Destructive testing can also be broken down into two smaller categories, invasive and non-invasive. An example of invasive testing in which an additional circuity is added in each module which activates an embedded FSM [13].

An example of non-invasive testing is Side-Channel Analysis (SCA). Some of the side-channel analysis parameter include power consumption, electromagnetic emissions etc. However, SCA in detecting trojans is limited by the large process variation effects in IC technology which has reduced detection sensitivity of ultra-small trojans in CMOS ICs [7].

2) Destructive Testing: The idea of using destructive testing is to reverse engineer a chip [14] and to make sure that there are no malicious circuits are present. The process involves removing the package, delayering the chip and using a Scanning Electron Microscope to analyze and extract a schematic. This method is expensive and time consuming. It also lacks coverage for the entire chip.

C. Adiabatic Logic

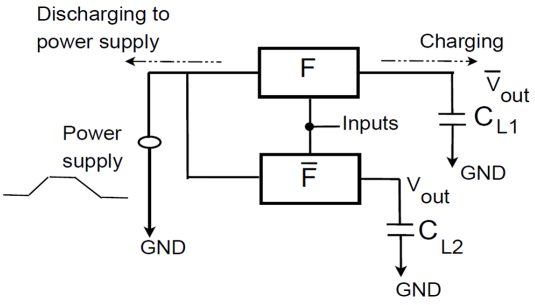


Fig. 4: Adiabatic Charging and Discharging

Adiabatic logic is one of the low-power circuit design techniques for designing ultra-low-power circuits. Adiabatic logic reduces the overall power consumed by the circuit by efficiently recycling the charge stored in the load capacitor after each computation. The recovered energy is reused in the next phase of the computation. The main idea of adiabatic logic technique is shown in Fig. 4. The energy dissipated in an adiabatic circuit considering the charge is supplied through a constant current source is given by,

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

Where T is the charging time of the capacitor, C is the load capacitor, V_{dd} is the full swing of the power clock. If T $>>$ 2RC (time constant), then the energy dissipated by the adiabatic circuit is less than the conventional CMOS circuit.

III. DPA Resistant Adiabatic Logic Family

This section briefly describes the operation of a recently proposed DPA resistant adiabatic logic called Energy-Efficient and Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [15].

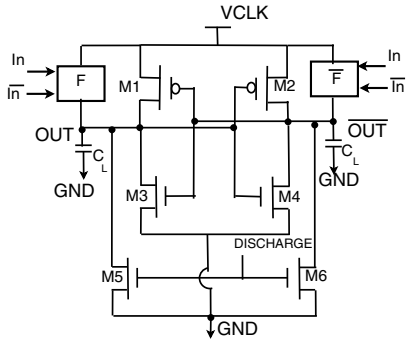


Fig. 5: General Structure of EE-SPFAL Logic Gate

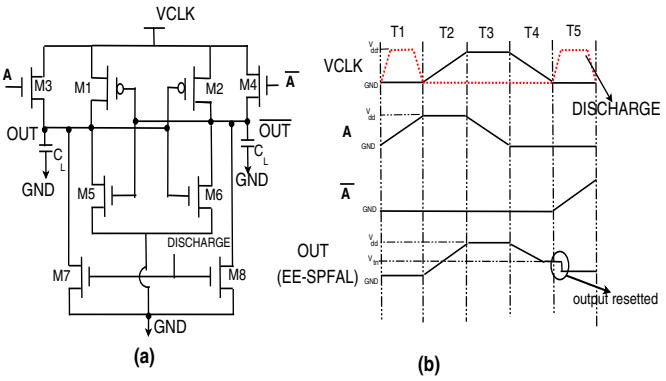


Fig. 6: EE-SPFAL Buffer and Timing Diagram

A. EE-SPFAL logic gates

Figure 5 shows the general structure of EE-SPFAL logic gates. F and $\bar{F}$ in Fig. 5 represent the logic function and its compliment in the EE-SPFAL gates. In EE-SPFAL gates, F and $\bar{F}$ are designed in such a way that the load capacitors are balanced. Transistors M1 and M2 are used to recover the charge from the load capacitances while M5 and M6 are used to discharge the redundant charge present in the load capacitances before the evaluation of the next cycle of inputs.

Fig. 6(a) shows the schematic diagram of the proposed EE-SPFAL buffer. In Fig. 6(a), M1 and M2 are used to recover the charge from the load capacitors. M3 and M4 are the evaluate transistors which are used to perform the logical operation. M7 and M8 are used to reset the outputs. M5 and M6 are used to avoid the minimal logical degradation. In this design, the leakage of information is avoided by resetting the outputs before evaluating the next cycle. Resetting of output before the evaluation of next cycle makes EE-SPFAL logic to consume uniform power, which in turn makes the circuit resistant against DPA attack. Timing diagram of the EE-SPFAL buffer is shown in Fig. 6(b). Further information on EE-SPFAL logic circuits can be found in [15].

IV. Proposed Adiabatic Power Clock Generator

This section discusses the proposed adiabatic Power Clock Generator (PCG) which is used in the EE-SPFAL circuit. The proposed four phase adiabatic clock generator is modified from

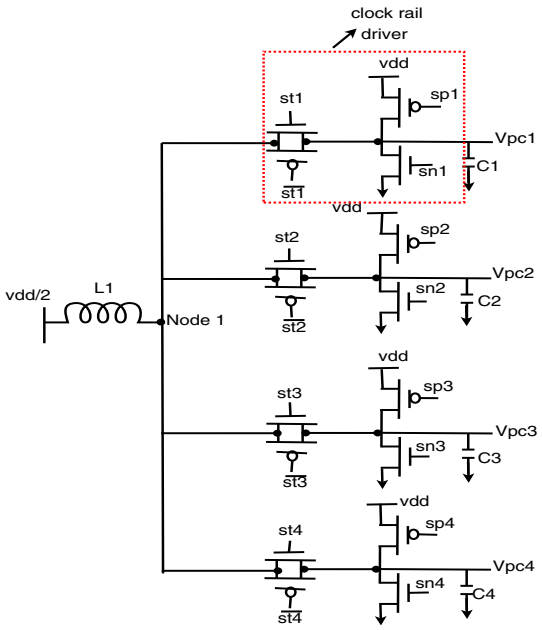


Fig. 7: Schematic of four phase adiabatic Power Clock Generator (PCG)

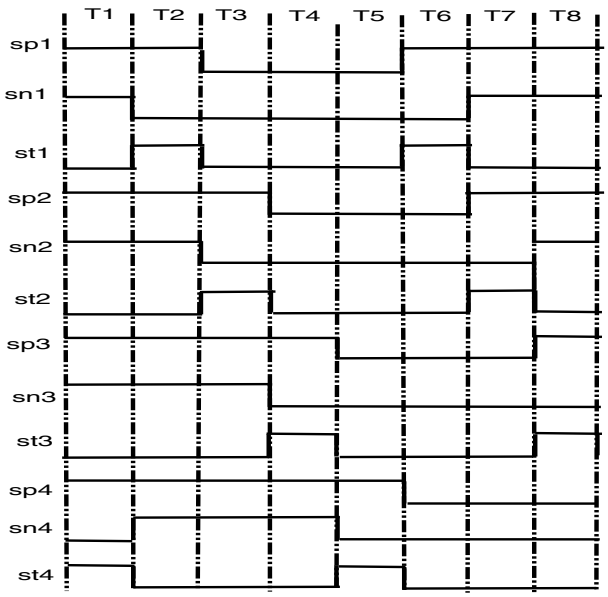


Fig. 8: Timing diagram for the adiabatic PCG

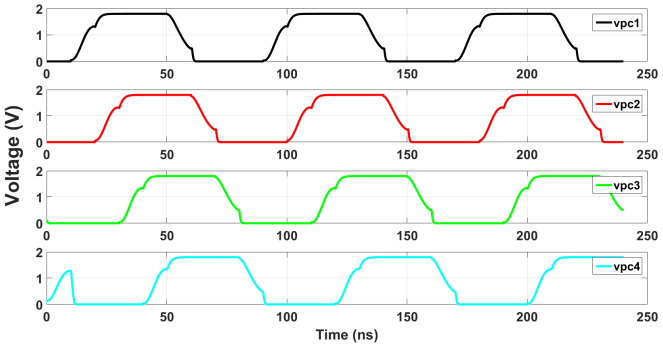


Fig. 9: Four phase clock generated through the adiabatic PCG

the three phase clock generator proposed in [16]. The circuit schematic of the four phase adiabatic clock generator is shown in Fig. 7. External capacitors are added to the power clock generator to balance the capacitance.

The timing diagram of the proposed four phase clock generator is shown in Fig. 8. The waveforms which is shown in Fig. 8 are repeated for every 8 phases. During T1, all the power clocks will be at gnd. At T2, node 1 is connected to vpc1 and vpc1 will slowly increase from gnd to vdd. At T3, vpc1 is clamped to vdd while the node 1 is connected to vpc2 to generate the time ramp. Similarly at T4, node 1 is connected to vpc3 and vpc3 will slowly ramps up to vdd while vpc1 and vpc2 will be clamped at vdd. At T5, vpc4 will slowly ramps up to vdd while the rest of the power clock voltages will be clamped at vdd. At T6, node 1 will be connected to vpc1 and sn1 will be turned. So, the voltage stored at the external capacitor is slowly recovered back to inductor (L1) through the transmission gate. Similarly, in consecutive phases, node 1 will be connected to single clock rail driver which leads to ramping up or ramping down the voltages.

Given the desired value of frequency (f), the inductor value can be found out by,

$$4f = 1/2\pi\sqrt{LC} \tag{2}$$

In our simulations, we fixed the desired frequency to be 12.5MHz and value of capacitor (C) to be 1pF. By equation 2, we found out that the inductor value is $10.132\mu H$. The generated four phase power clock voltage is shown in Fig. 9.

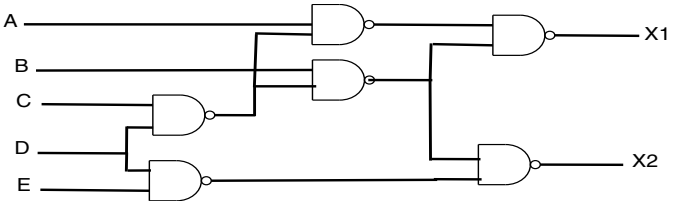
V. Hardware Trojan Detection Method

This section describes our proposed method of detecting Hardware Trojans (HTs) without a golden (non-trojan) chip. As described in Section III, DPA resistant adiabatic logic family (EE-SPFAL) consumes uniform power irrespective of input data transition also consume lower power compared to conventional CMOS logic gates. If a CMOS gate is inserted in the adiabatic based gate then we expect a power spike to occur once the CMOS gate turns on. We are using this principle to detect smaller trojans in DPA resistant adiabatic logic based IMD devices. Usually, hardware trojans are built using conventional CMOS circuits. When the HT is triggered in the DPA resistant based circuit, the circuit will have non-uniform power consumption which will help us to easily identify HTs by simple analysis methods.

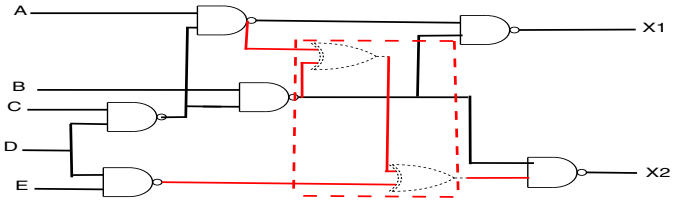
Further, it will be tedious for the attacker to implement an DPA-resistant adiabatic logic gate based trojan in the circuit. Usually, adiabatic logic based circuits uses pipeline based clocking methods to recover energy from each gates. Insertion of trojans changes the clocking zones which will help us to easily identify the trojans.

As a case study, in this paper, we are showing the insertion of CMOS based HT in the EE-SPFAL based c17 benchmark

circuit and a carry save adder circuit. Fig. 10 and Fig. 11 shows the schematic of 'golden' and 'infected circuit' of C17 benchmark and carry save adder circuit [17].

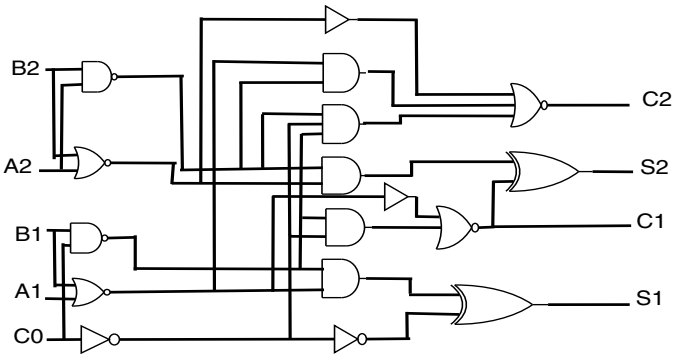


(a) Golden C17 Circuit

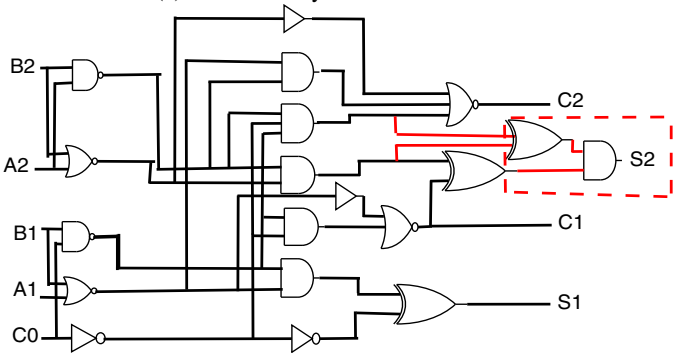


(b) Infected C17 Circuit

Fig. 10: C17 Golden vs Infected Circuit



(a) Golden Carry Save Adder Circuit



(b) Infected Carry Save Adder Circuit

Fig. 11: Carry Save Adder Golden vs Infected Circuit

VI. Results and Discussion

All the simulations reported in this paper are performed using Cadence Spectre simulator with 180nm CMOS technology. Additional buffers are inserted in EE-SPFAL based C17 and Carry Save Adder (CSA) to synchronize the power clocks for proper operation of the circuits. The power reported

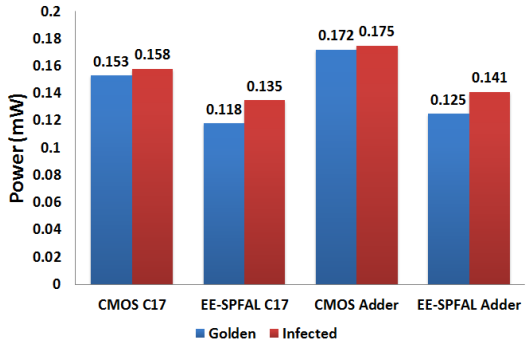


Fig. 12: Power Differences in Golden and Infected circuits

in this paper for EE-SPFAL based circuits are total power consumption including the power clock generator and the logic circuits.

Table I shows the average power consumption of the conventional CMOS and EE-SPFAL based C17 benchmark and CSA circuit. From the table, we can see that the EE-SPFAL based C17 and CSA saves 25.8% and 31.4% less power as compared to the conventional CMOS circuits.

Table II shows the average power difference between the EE-SPFAL and CMOS based c17 and CSA circuits with trojan and without trojan. From Table II, we can see that the CMOS based C17 and CSA circuit has 3% and 2% difference in power consumption of the golden and infected circuit. However, EE-SPFAL based c17 and CSA circuit has 14% and 12% difference in power consumption of the golden and infected circuit.

Circuit	CMOS	EE-SPFAL	power savings
C17	.153 mW	.118 mW	25.8%
CSA	.172 mW	.125 mW	31.4%

TABLE I: CMOS vs EE-SPFAL Power Consumption

Circuit	CMOS			EE-SPFAL		
	Golden	Infected	Difference	Golden	Infected	Difference
C17	.153mW	.158mW	3%	.118mW	.135mW	14%
CSA	.172mW	.175mW	2%	.125mW	.141mW	12%

TABLE II: Golden vs Infected Power Consumption for CMOS and EE-SPFAL based circuits

Fig. 12 shows the power difference between a 'golden' and 'infected' circuits in CMOS and EE-SPFAL logic. Fig. 13 presents the power consumption of the EE-SPFAL based C17 and adder circuit with and without trojan. From Fig. 13 (a) and (c), we can see that the 'golden' EE-SPFAL based c17 and CSA circuit has uniform power consumption irrespective of input data transition. However, Fig. 13 (b) and (d) shows the non-uniform power consumption of the 'infected' EE-SPFAL based C17 and CSA circuit.

VII. Conclusion

In this paper, we have studied the usefulness of DPA resistant adiabatic logic family for the detection of hardware

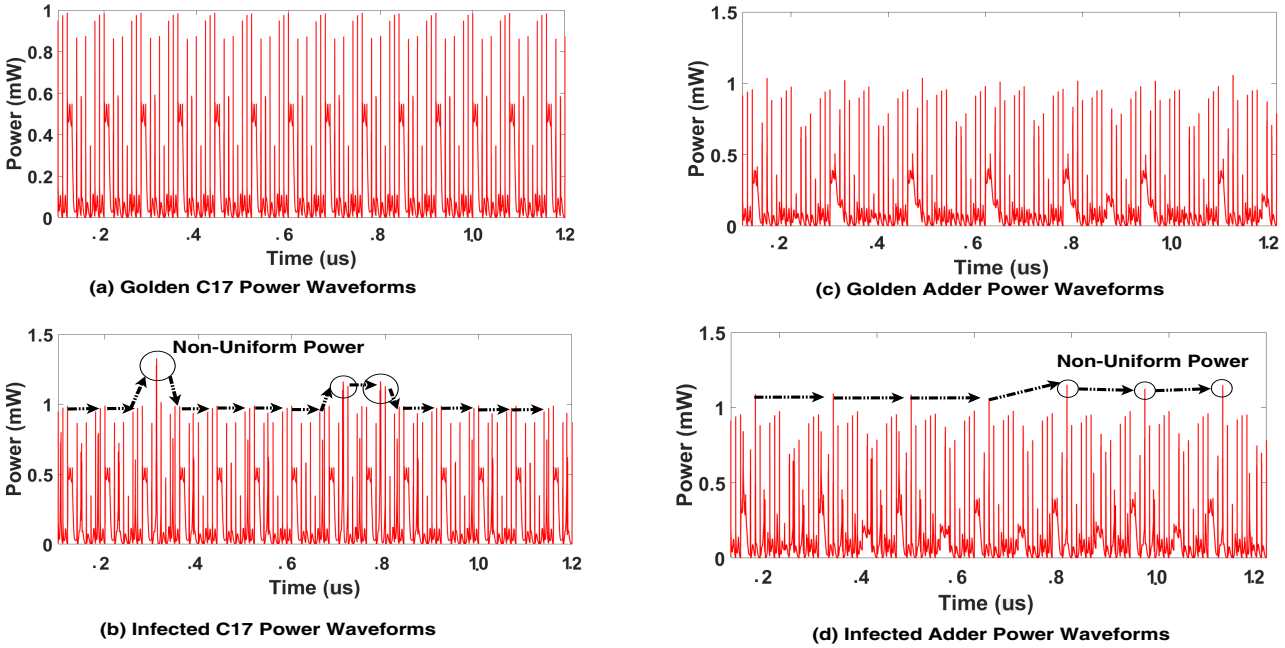


Fig. 13: Golden vs Infected Power Waveforms of EE-SPFAL C17 and Adder

trojans in medical devices. From the simulation results, it is shown that the EE-SPFAL (DPA resistant adiabatic logic family) based circuits consume less power as compared to the conventional CMOS circuits and also consume uniform power irrespective of input data transition. When the CMOS based hardware trojan is triggered in the EE-SPFAL circuits, the circuit have non-uniform power consumption which will help to easily identify the malicious circuits. The low power and easy hardware trojan detection technique in DPA resistant adiabatic logic circuits has opened new research avenues for the low-power and inexpensive hardware trojan detection in IMD devices.

REFERENCES

[1] 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, 2008.

[2] H. G. Mond and A. Proclemer, "The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: calendar year 2009–a world society of arrhythmia's project," *Pacing and clinical electrophysiology*, vol. 34, no. 8, pp. 1013–1027, 2011.

[3] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[4] S. Skorobogatov and C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012, pp. 23–40.

[5] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Communications of the ACM*, vol. 58, no. 4, pp. 74–82, 2015.

[6] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy, and S. Bhunia, "Multiple-parameter side-channel analysis: A non-invasive hardware trojan detection approach," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 13–18.

[7] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using ic fingerprinting," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 296–310.

[8] C. A. Schu, D. R. Greeninger, and D. L. Thompson, "Implantable medical device incorporating adiabatic clock-powered logic," Jul. 2 2002, uS Patent 6,415,181.

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

[10] C. A. Schu, D. R. Greeninger, and D. L. Thompson, "Power dissipation reduction in medical devices using adiabatic logic," Aug. 20 2002, uS Patent 6,438,422.

[11] H. Thapliyal, T. Varun, and S. D. Kumar, "Adiabatic computing based low-power and dpa-resistant lightweight cryptography for iot devices," in *VLSI (ISVLSI), 2017 IEEE Computer Society Annual Symposium on*. IEEE, 2017, pp. 621–626.

[12] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, 2010.

[13] R. S. Chakraborty, S. Paul, and S. Bhunia, "On-demand transparency for improving hardware trojan detectability," in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 2008, pp. 48–50.

[14] Chipworks, "Semiconductor manufacturing - reverse engineering of semiconductor components, parts and process," available: http://www.chipworks.com.

[15] S. D. Kumar, H. Thapliyal, and A. Mohammad, "Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card," *IEEE Transactions on Emerging Topics in Computing*, 2016.

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

[17] K. Lingasubramanian, R. Kumar, N. B. Gunti, and T. Morris, "Study of hardware trojans based security vulnerabilities in cyber physical systems," in *Consumer Electronics (ICCE), 2018 IEEE International Conference on*. IEEE, 2018, pp. 1–6.