Secure Intermittent-Robust Computation for Energy Harvesting Device Security and Outage Resilience

Arman Roohi and Ronald F DeMara
Department of Engineering and Computer Science
University of Central Florida
Orlando, Florida 32816-2362 USA
aroohi@knights.ucf.edu, demara@mail.ucf.edu

Longfei Wang and Selçuk Köse
Department of Electrical Engineering
University of South Florida
Tampa, Florida, 33620, USA
longfei@mail.usf.edu, kose@usf.edu

***Abstract*— In this paper, we propose Secure Intermittent-Robust Computation (SIRC) for Energy Harvesting Powered Internet of Things (IoT) Devices. This effort innovates a new duty-cycle-variable computing approach to facilitate and invigorate security in energy-harvesting-powered IoT network nodes. The proposed SIRC architecture is developed from the ground up by extending emerging post-CMOS switching elements to realize majority-gate logic that is intrinsically-capable of middleware-coherent, battery-free without check-pointing or micro-tasking, and can be resilient to wireless power transfer attacks including charge attacks and data attacks. Potential countermeasures for these attacks are identified at the circuit-level through gate-resolution immunity of power interruption. As a proof-of-concept, a power-maskable design using SIRC approach is developed for s27 circuit from ISCAS89 benchmark. The obtained results shows SIRC provides reduced area consumption and increase number of power traces to extract crypted data.**

Keywords*— *Power transfer attack; Power failure vulnerability; Charging attack; Internet of things; Battery-free computing; Spintronics; Majority gate logic; Power Masking Unit.

I. INTRODUCTION

Secure energy-harvesting-powered computing offers many intriguing opportunities to dramatically transform the landscape of IoT devices and wireless sensor networks [1]. These devices, operate using only ambient sources of light, thermal, and kinetic energy [2]. Due to this, they require attack prevention methods for various classes of power based attacks, such as wireless power transfer attacks [3]. If secure lightweight embedded computing could be realized with free and/or inexhaustible sources of energy, new classes of maintenance-free, compact, and inexpensive computing applications would become possible [4]. Thus, energy-harvesting-powered devices could enable a sustainable computing platform for future medical, aerospace, and IoT applications. Energy-harvesting devices are projected to develop towards a $2.6B market by 2024 [5]. However, energy-harvesting-powered devices have a limited energy capacity, which creates challenges to realizing secure communication and operation. Furthermore, harvested energy strategies are inherently sensitive to environmental conditions [2]. Therefore, this paper proposes a promising class of primitive processing elements that utilize switching devices capable of leveraging (1) the restricted energy capacity, (2) the intermittent temporal energy profile, and (3) they show resilience to power based attacks in the context of energy harvesting schemes. The *Secure Intermittent-Robust Computation* (SIRC) architecture proposed herein will utilize these elements for improved energy and area metrics, while advancing secure energy-harvesting-powered IoT towards a wider range of applications.

II. ENERGY HARVESTING SYSTEM POWER FAILURE ATTACKS

As shown in Fig. 1(a), a typical energy harvesting system converts ambient energy, such as ambient RF signals, into usable energy via rectification and charge-trapping. Figure 1(b) depicts the energy accumulation on capacitor C_2 to generate a supply voltage, V_{DC}. Once the voltage of the capacitor attains a sufficient level, V_{ON}, then a lightweight embedded processing element can begin its

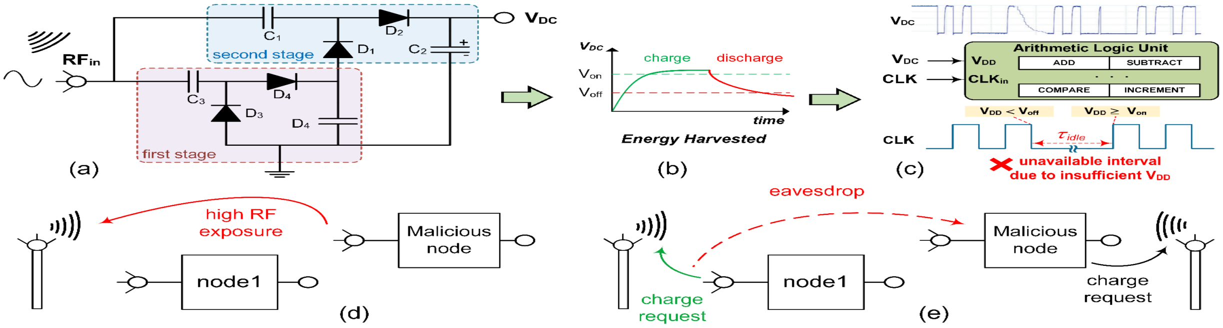

Fig. 1. ALU operating from an intermittent energy supply illustrating (a) dual-stage Dickson voltage multiplier performing Radio Frequency (RF) source energy conversion, (b) $V_{DC}(t)$ available, and (c) $V_{DD}(t)$ supplied to ALU, and depiction of two different types of attacks in wireless power transfer: (d) charging attack, and (e) spoofing attack.

operation. The stored energy will be rapidly consumed, leading to the subsequent decrease of $V(C_2) \leqslant V_{OFF}$, which consequently stops execution due to an insufficient supply voltage. As depicted in Fig. 1(c), the supply voltage, V_{DD}, of the processor experiences intermittent behavior. This results in an interval of unpredictable unavailability, τ_{idle} that can interrupt the data-flow and the processor clock, CLK. This charge/discharge cycle, which is an intrinsic characteristic of energy harvesting devices, may occur more than hundreds of times per second for RF-based sources, and unpredictably for extended durations with kinetic and light-powered sources. Furthermore, the interval τ_{idle} can occur irregularly and vary in duration, leading us to propose a new method to achieve secure energy-harvesting computation as described herein. The hardware realization of this approach addresses one of the major hurdles to the propagation of energy harvesting systems: robust operation despite discontinuities in the ambient energy supplied from its environment to avoid irregular and unpredictable results [6]. As identified in the Introduction, as Internet of things (IoT) devices become more pervasive in our daily lives, energy harvesting technologies will be attracting significant attention as a means to sustain power locally without power supply wiring or batteries. While a vast amount of research continues to be undertaken to improve the power efficiency of the energy harvesting circuitry, little attention has been paid to the potential security issues within the wireless power transfer networks that comprise energy transmitter and receiver devices.

Wireless power transfer attacks have recently attracted attention as possible threats to achieving secure battery-free computing. Such attacks can potentially degrade the power transfer efficiency and even destroy the normal operation of the network. Different types of security attacks on battery-free devices have been summarized in [2], which includes safety attacks, charging attacks, interference attacks, spoofing attacks, application attacks, and monitoring attacks. Monitoring attacks are passive since they do not alter the operation of the wireless power transfer networks, while the rest of the attacks are active. Figure 1(d) and 1(e), shows two different types of attacks in wireless power transfer, charging and spoofing attacks, respectively. In the former, a malicious receiver node may produce redundant requests that generate incorrect feedback to decrease the total power transfer efficiency. Whereas, the latter attack is similar to the concept of a man-in-the-middle attack, in which the important information transferred between two nodes is eavesdropped. Operational constraints on safety regulations, energy transfer requests, and interference can be leveraged by a malicious node to perform, respectively, safety attacks, charging attacks, and interference attacks, to reduce or stop the energy transferred to receivers. Finally, energy depletion or starvation attacks can present a class of irrecoverable denial-of-service vulnerabilities, as well as risk of data loss due to CMOS processors' lack of immunity to power outages. Interference alignment, scheduling, and dynamic power/frequency adaptation can be leveraged as a countermeasure against interference attacks. In this paper, we develop a new approach by providing power outage immunity to processing nodes via circuit-level techniques. While not a complete solution, such methods can help to thwart data loss and errant behavior that can result from outage attacks [2].

III. Secure Intermittent-Robust Computation (SIRC)

Advancing beyond previous intermittent processors that utilize non-volatile memory (NVM) resources, which are distinct from the processing datapath, we propose the SIRC computing architecture based on spintronic devices leveraging their inherent non-volatility within the logic datapath itself, while avoiding the energy overhead of intermittent check-pointing, routine data exchange between tasks, and datapath pipeline registers. Thus, the intermittent operation can be intrinsically supported without the burden of additional circuitry or software-based task decomposition. In the case of unpredictable power interruption, the instantaneous condition of all processor internal states will remain within its own datapath without the need to reload all the previous operands to help mitigate power charging and spoofing vulnerabilities.

One promising beyond CMOS technology, which has non-volatility, is Spintronics. Moreover, the unifying computational mechanism underlying all of the Magnetic Tunnel Junction (MTJ)-based devices is accumulation-mode operation that enables the realization of Majority Gates (MG) as basic computational building blocks. MGs provide a functionally-complete set of Boolean logic expressions due to their intra-gate control, and can realize intermittent robust circuits that are the fundamental building blocks of the SIRC architecture. Figure 2(a) depicts the SIRC architecture at the system block level. It consists of a pool of NV-MGs, which are connected to input, output, and control signals, as well as sensitive NVM (low energy barrier), and NVM containing the encrypted node's information. In Fig. 2(b), SIRC operates as a 2-bit NV Full Adder (NV-FA), whereas, Fig. 2(c) illustrates a 2-bit NV Multiplier (NV-M) by only adjusting control signals, which alter the MGs' functions without any additional device overhead within the computational unit. NV-MGs can be cascaded to realize conjunctive or disjunctive Boolean gate realizations. By affixing one (or

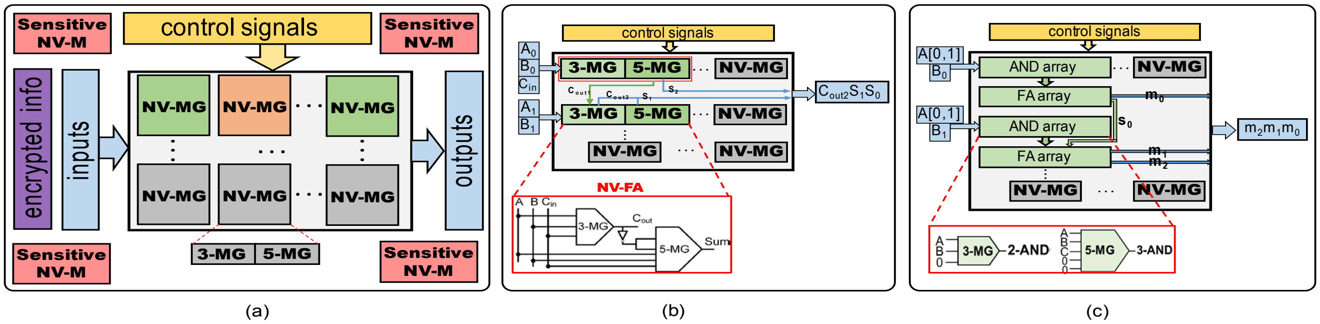

Fig. 2. (a) SIRC computation pool of NV-MGs, (b) NV-FA arrangement using 3-MG and 5-MG, and (c) 2-bit NVM multiplier.

two) of the three (or five) input signals to ON or OFF states on demand during the circuit operation, then a 2(or 3)-input OR gate or a 2(or 3)-input AND gate can be realized, respectively. Both 3 and 5 –input NV-MGs are implemented and validated by SPICE circuit simulations using our model developed in [7-11].

A. Vulernabilites under Charging Attacks

In energy-harvested IoT devices, one of the most significant classes of attacks is a charging attack [2]. In wireless power transfer networks, it is assumed that several mobile and fixed Power Transmitters (PTs) and SIRC-embedded devices, which are considered as Power Receivers (PRs), communicate with each other. The attacker's goal is to decrease the efficiency of PTs, which results in the degradation or interruption of the system functionality. In general, a power transfer channel has some significant attributes that differ from a data communication channel. Therefore, possible attacks against the SIRC architecture can be partitioned into two sub-categories: energy attacks and data (information) attacks.

a) *Energy Attack*: There are two potential scenarios to be considered. Scenario One: malicious PR nodes generate unnecessary energy requests and send false responses and feedback to the PT node (global power source), which results in decreasing efficiency of the overall power of a non-ambient source. In such environments, the malicious receiver nodes send charging requests in a compressed period, which cause other viable nodes to receive reduced or insufficient power for their store/computation operations. In this scenario, the attacker counterfeits its energy state. Scenario Two: a malicious PR node counterfeits or feigns the role of a PT. It emits radio frequency waves with the same frequency as the PT, but with different phase. Hence, the energy harvesting at the victim PRs could potential be modified, or the attacker forms a cooperative relationship with victim PRs.

b) *Data Attack*: A plethora of data attacks have been identified in the literature [8-9]. Herein, the scope of data attacks focuses on those relating to power information. A common power-related information attack is a spoofing attack. In wireless power transfer networks, different types of energy-related data such as energy state, energy outage, signature, etc. will be broadcasted between PRs and PTs. In this scenario, an attacker (malicious node) can eavesdrop on the data of the other PRs or even PTs and utilize the captured information to decrease and/or collapse throughput of the network. In this case, three possible scenarios might occur: (1) if a malicious node (attacker) knows its adjacent PR (victim) will deplete its energy at the time T, it can broadcast energy requests at time t<T, to prevent the victim from receiving energy, thus precipitating its interruption; (2) the attacker can change its or the victim's device identity in a way that the victim could not receive energy. It also can feign as a PT to adjacent PRs and store their energy requests without any response; and, (3) the attacker can broadcast fake responses to the received energy from PTs, in particular, the attacker demands additional energy whereas it has sufficient energy.

B. SIRC Mitigation of Charging Attacks

All PTs and PRs are equipped with NV memories to store encrypted data. This data can be fixed, such as the average power consumption for a specific duration at design time, or can be changeable, such as the remaining power, number of received/sent requests, and number of zones at runtime. Power transmission process can be performed using both omnidirectional or directional antennas. (1) The PT propagates RF power via omnidirectional antennas: every PR inside a specific zone starts charging, simultaneously. Meanwhile, the malicious nodes' lives can be extended if they can power off and power on repeatedly, to extend their effect on the entire system. Hence, when a PT receives information and stores it within its NV memory from several PRs in the same zone, it then checks their correctness/incorrectness using a majority voter, as shown in Fig. 3. For instance, if node a1 in Zone A, reports information very different from the other nodes (a_2, a_3, ...) in Zone A, the PT updates NVM and marks a1 as a potential attacker, which receives less power than previously provided until it functions similarly to the other nodes. (2) The PT propagates RF signals using directional antennas: malicious nodes moderately send energy requests to halt other PRs' functionalities. In this case, based on the stored data for each PR node at design time, including approximate power consumption, the PT can determine they are issuing either plausible or unreasonable requests. If a PR shows suspicious behavior, then the PT can penalize it or even modify power transmission parameters so that it receives less energy to preclude the malicious node.

Cryptographic methods can be implemented using both software algorithms and hardware elements. Although the former class is more flexible, the latter one can be significantly more energy-efficient, tailored to the need, and bloat-free, which can make it much more suitable for energy-harvested IoTs. In cryptography, one of the most dangerous and ubiquitous attacks is the side-channel attack, which herein is a power analysis attack (PAA). An adversary can use PAAs to capture different aspects of power supply when the crypt-decrypt process is performed to break the cryptographic algorithm. Our efficient PAA countermeasure is based on the design presented in [9] with the following differences: 1) there are no registers required within datapath; 2) we can reprogram one

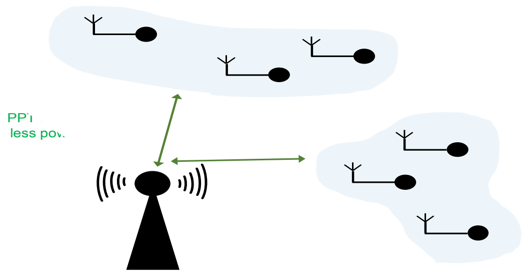

Fig. 3. Feasible countermeasure for charging attack by marking possible malicious node.

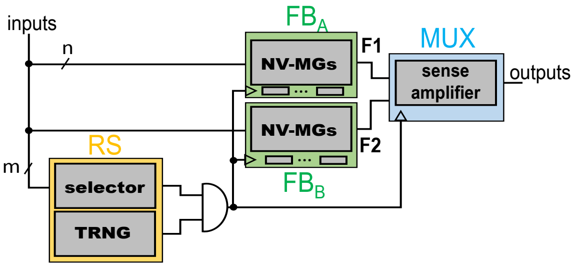

Fig. 4. Power masking countermeasure for possible power analysis attack. F1 and F2 perform the same function with different power consumption.

block to operate with the different functional blocks in different situations at both design time and runtime; 3) a selection operation is performed by using only one selective transistor, which connects appropriate element's output to the final output via sense amplifier; and 4) the random noise insertion process is performed using spin-based low power and high efficiency true random number generator (TRNG). Figure 4, depicts possible power analysis countermeasure utilizing power masking method. The role of the randomized selector (RS), which includes selector and TRNG, is to activate each of functional block (FB) based on the portion of inputs. Due to random behavior of RS, total power consumption of this module will vary randomly, which assists the goal of masking the power consumption.

Although several possible solutions are recommended, such as storing encrypted information like device identity and power transmission parameters at the design time in a NVM, complete energy attack prevention is impossible. Therefore, due to the non-volatility of the proposed spin-based SIRC units, they can maintain their computation state and ensure forward progress in the presence of unpredictable energy failures without programmer burden or execution overhead incurred by idempotent and other re-tasking techniques. It implies that the proposed design can impart resilience against charging attack classes of vulnerabilities. To verify the intermittent operation of the proposed design, we have implemented a majority gate (MG)-based FA circuit using a preliminary model of SHE-MTJ devices, as shown in Fig. 5. The circuit is implemented using combinations of 3-input and 5-input SHE-MTJ based MGs. The logic function of FA can be expressed by C_{out}= AB+AC+BC= 3MG(A,B,C), and SUM= $A\oplus B\oplus C$= 5MG (A,B,C,C_{out}',C_{out}'). In addition to the two mentioned scenarios, NVMs of SIRC are exposed to magnetic attacks when they are in sleep-mode. Therefore, our proposed SIRC architecture is equipped with an additional array of NVM to prevent magnetic attacks [10]. These NVMs in this array, namely the sensitive NVM: a) are programmed at design time with a specific pattern; b) their energy barrier are lower than the regular NVMs in SIRC, which are used to store the encrypted data. It means with an external magnetic field, even a small one, the state of sensitive NVMs can be flipped, while the other NVMs might not be affected. This kind of structure provide a passive security scheme for SIRC. For example, if an adversary tries to change the information of a PR's secured data, the pre-written pattern in the sensitive NVM will change, certainly. Then, a PT can detect an infected PR node by checking/comparing its pattern with its original one. Additionally, the altered sensitive NVMs can be modified using the stored original pattern, which might guarantee a secured communication.

IV. Proof-of-Concept

Although, a general way to make a design resilient to power failure is that all FF should be replaced by NV-FFs [6], in our approach which leverages NV-MGs, non-volatile elements are also able to realize logic operations while storing values. Therefore, a cone (sequence) of gates with only one fan-out connected to a flip-flop can be implemented using one (more) MG-FF(s). This enables reconfiguration of the design to implement a function with different structures, which results in different power profiles. Hence, this technique can be utilized within the power-masked cryptosystem implementations. To exemplify functionality of this method, the **s27** circuit from the ISCAS89 benchmark suite is selected as a proof-of-concept, as shown in Fig. 6. First, a cone of gates including the FF is selected, which is shown with red dashed lines. Then, this selection is implemented using two MG-FFs and

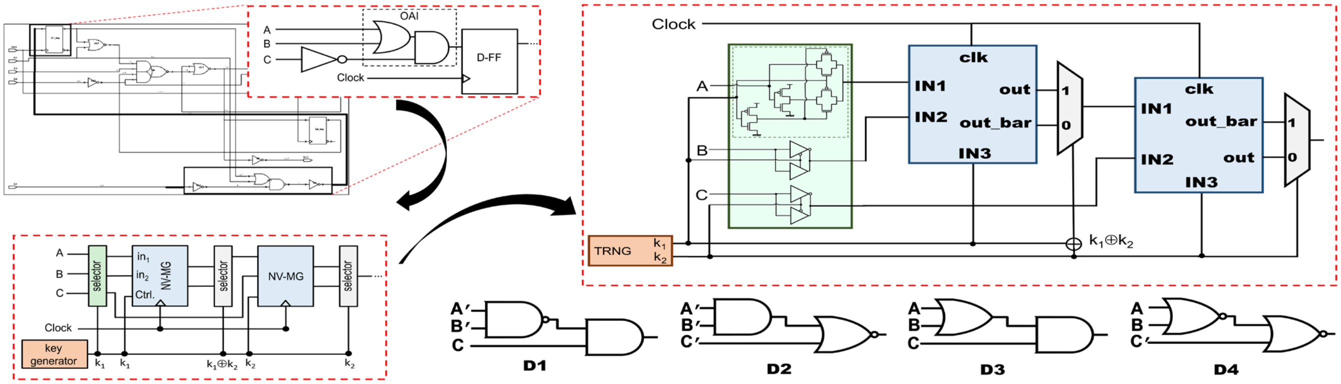

Fig. 6. **s27** schematic (top left), selected cone gate (bottom left), developed MG-FF based design (top right), and equivalent logic realizations (bottom right).

five selector circuits. As depicted in Fig. 6, the implemented design can be reconfigured using two reprogramming random bits, K_1K_2, in order to produce all equivalent implementations. The portion of the design which can be reconfigured through K_1 and K_2 bitstream are: 1) select *input* or its inverted (*input_bar*) signal, 2) determine MGs functionalities, and 3) drive *out* or *out_bar* to the output pin. Fig. 6 depicts all four possible designs with a similar functionality. For instance, if generated keys are K_1K_2= 00, first A', B', and K_1 are connected as inputs to the first MG-FF, which functions as a 2-input AND gate (K_1=0). Then K_1K_2 signal is XORed and selects *out_bar* and pass it to the second MG-FF. Its other inputs are *C* and K_2. Due to the produced connection using K_1K_2= 00, the equivalent behavior of the design is $\overline{(\bar{A}\cdot\bar{B})}\cdot C$. This methodology can be leveraged for all cone gates connected to FFs to convert them to power maskable units with the intermittence resiliency feature.

TABLE I. GENERATED KEYS AND THEIR CORRESPONDING AVERAGE POWER CONSUMPTION.

K_1K_2	Inputs	Functionality		Equivalent Design in Fig. 6	Avg. Power Consumption (μW)
		MG1	MG2		
00	A'B'C	NAND	AND	D1	68.6
01	A'B'C'	AND	NOR	D2	101.5
10	ABC	OR	AND	D3	98.8
11	ABC'	NOR	NOR	D4	131.7

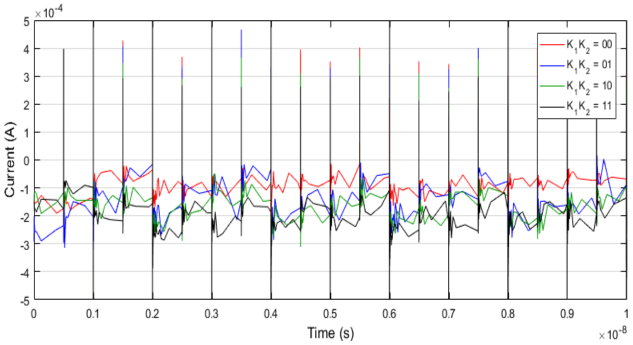

Fig. 7. Power traces results for all possible K_1K_2 combinations.

Herein, the SHE-MTJ model developed in [7], [11] is utilized to design a 3-input MG. The functionality of the SHE-MG based designs are verified by SPICE circuit simulation. Table I summarizes power consumption results for four different implementations regarding to generated keys. For instance, design produced by keys, K_1K_2= 11, which is equivalent to D4 circuit in Fig. 6 has the highest average power consumption for all possible input combinations. The reason is that because MG-FFs function as 2-input OR gates, which leads to a higher number of ON transistors, which pass a higher input current and thus incur a higher power dissipation. If after generating K_1K_2, the keys remain fixed during operating for all possible 3-input combinations, eight distinct possible power traces produced. Whereas, keys can have four different values, which result in 32 different combination for power traces, which are shown in Fig. 7. Based on our approach, the generalized equation for calculating all required power traces is expressed by $2^m \times 2^n$, where *m* is the number of key bits and *n* is the number of input bits. Therefore, by extending this method for all possible cone gates, more number of power traces are required by attacker to extract the private key using differential power analysis attacks.

As mentioned above, the conventional power-maskable approaches include two separate units, in which their inputs are latched by registers and function similarly with different power cost [9-12]. This results in an area overhead almost twice as large as the original design, in addition to the limited variety in power-managed units for masking power. Both contribute significant drawbacks of conventional power masking methods. Whereas, the proposed SIRC architecture leverages non-volatile SHE-based MG-FFs, a power-obscured area-dense energy-aware intermittent PAA resilient design is obtained. It realizes increased side channel immunity for IoT due to the MGs' capability to transform between AND, OR, etc. gates at runtime.

V. CONCLUSION

The non-volatility of SHE-MTJ three terminal emerging devices provides a new approach against power outages during charging attacks. SIRC leverages the atomicity of the MTJ's magnetic state to realize majority logic gates, which are immune to power outage corruption down to the fine-granularity level of each logic gate. Meanwhile, data attacks are also thwarted by the same mechanism. These are combined with majority gate based power masking countermeasures for possible power analysis attacks which have several advantages such as more flexibility and low area overhead in comparison to previous power-maskable units such. The resulting SIRC strategy realizes intermittent-robust operability, along with energy-conserving and area-sparing features suitable for future IoT applications.

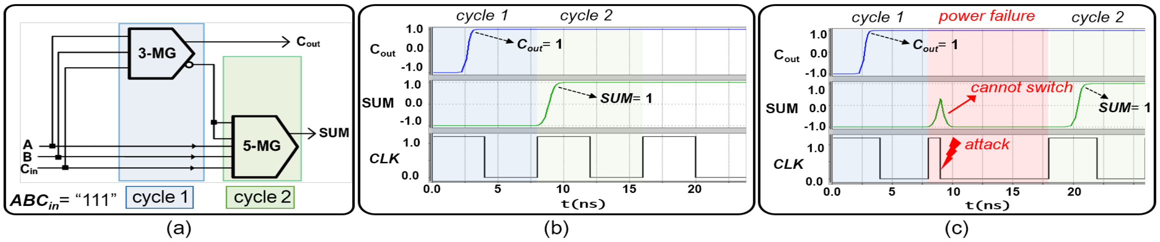

Fig. 5. (a) MG-based 1-bit full adder circuit, (b) transient response for FA normal operation with ABC= "111" input, and (c) intermittent operation of proposed FA design in presence of unpredictable power failure.

REFERENCES

[1] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE Trans. Emerg. Sel. Topics Circuits Syst*., vol. 3, pp. 45-54, 2013.

[2] Q. Liu, K. S. Yıldırım, P. Pawełczak, et al., "Safe and Secure Wireless Power Transfer Networks: Challenges and Opportunities in RF-Based Systems," *IEEE Commun. Mag*., 54(9), pp.74-79, 2016.

[3] B. Lucia and B. Ransford, "A simpler, safer programming and execution model for intermittent systems," in ACM *SIGPLAN Notices*, 2015, pp. 575-585.

[4] W.-H. Lee and R. Lee, "Implicit Sensor-based Authentication of Smartphone Users with Smartwatch," in *Proc. of the Hardware and Architectural Support for Security and Privacy*, 2016, p. 9.

[5] A. Poor, "Reaping the Energy Harvest [Resources]," *IEEE Spectrum,* vol. 52, pp. 23-24, 2015.

[6] K. Ma, Y. Zheng, S. Li, et al., "Architecture exploration for ambient energy harvesting nonvolatile processors," in 2015 IEEE 21st Int. *Symp. on High Performance Computer Architecture*, 2015, pp. 526-537.

[7] A. Roohi, R. Zand, D. Fan, et al., "Voltage-based Concatenatable Full Adder using Spin Hall Effect Switching," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*., vol. PP, pp. 1-1, 2017.

[8] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, H. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Commun. Mag*., 53(8), pp.114-121, 2015.

[9] L. Benini, A. Macii, E. Macii, E. Omerbegovic, F. Pro, and M. Poncino, "Energy-aware design techniques for differential power analysis protection," in *Proceedings of the 40th DAC*, pp. 36-41. ACM, 2003.

[10] S. Motaman, S. Ghosh, N. Rathi, "Cache Bypassing and Checkpointing to Circumvent Data Security Attacks on STTRAM," in *IEEE Trans. Emerg. Topics Comput.*, vol.PP, no.99, pp.1-1, 2017.

[11] R. Zand, A. Roohi, D. Fan and R. F. DeMara, "Energy-Efficient Nonvolatile Reconfigurable Logic Using Spin Hall Effect-Based Lookup Tables," in *IEEE Trans. Nanotechnol.*, vol. 16, no. 1, pp. 32-43, Jan. 2017.

[12] L. Benini, A. Macii, E. Macii, E. Omerbegovic, M. Poncino, and F. Pro. "A novel architecture for power maskable arithmetic units." in *Proceedings of the 13th ACM GLSVLSI*, pp. 136-140. ACM, 2003.