Logic-Encrypted Synthesis for Energy-Harvesting-Powered Spintronic-Embedded Datapath Design

Arman Roohi, Ramtin Zand, and Ronald F. DeMara
Department of Electrical and Computer Engineering, University of Central Florida, Orlando, Florida, 32816

ABSTRACT

The objectives of advancing secure, intermittency-tolerant, and energy-aware logic datapaths are addressed herein by developing a spin-based design methodology and its corresponding synthesis steps. The approach selectively-inserts Non-Volatile (NV) Polymorphic Gates (PGs) to realize datapaths which are suitable for intrinsic operation in Energy-Harvesting-Powered (EHP) devices. Spin Hall Effect (SHE)-based Magnetic Tunnel (MTJs) are utilized to design NV-PGs, which are combined within a Flip-Flop (FF) circuit to develop a PG-FF realizing Boolean logic functions with inherent state-holding capability. The reconfigurability of PGs is leveraged for logic-encryption to enhance the security of the developed intermittency-resilient circuits, which are applied to ISCAS-89, MCNS, and ITC-99 benchmarks. The results obtained indicate that the PG-FF based design can achieve up to 7.1% and 13.6% improvements in terms of area and Power Delay Product (PDP), respectively, compared to NV-FF based methodologies that replace the CMOS-based FFs with NV-FFs. Further PDP improvements are achieved by using low-energy barrier SHE-MTJ devices within the PG-FF circuit. SHE-MTJs with 30kT energy exhibit 40.5% reduction in PDP at the cost of lower retention times in the range of minutes, which is still sufficient to achieve forward progress in EHP devices having more than hundreds of power-on and power-off cycles per minute.

1 INTRODUCTION

Energy-harvesting-powered computing offers intriguing and vast opportunities to dramatically transform the landscape of IoT devices and wireless sensor networks [1]. These devices require drastically-reduced energy consumption such that they are able to operate using only ambient sources of light, kinetic, and electromagnetic energy [2] as a means to achieve battery-free computing [3]. Thus, energy-harvesting-powered devices could enable a sustainable computing platform for future medical, aerospace, and IoT applications. energy-harvesting-powered devices are characterized by intermittent behavior, which can result in disturbances in execution of programs, data loss, glitch conditions, and lack of execution progress that may lead to irregular and unpredictable results [4].

To implement intermittent-resilient computing architectures, Non-Volatile Flip-Flops (NV-FFs) fulfill essential roles as a hardware-based approach. Various techniques are proposed to address the intermittency challenge facing energy-harvesting-powered designs. In [5, 6], a traditional checkpointing approach is utilized to ensure the accurate forward progress of computation, whereby any volatile execution context is proactively preserved in Non-Volatile Memory (NVM) prior to anticipated periods of power failure. A checkpointing approach may suffer from internal and external inconsistencies after each power loss. Internal inconsistency occurs when the execution context is partially-retained in NVM, while external inconsistency arises when the power failure occurs between two checkpoints [7]. DINO [8] innovated a checkpointing-based approach that utilizes non-volatile versioning to retain the memory consistency. Duty Cycling with Scheduling [9] offers another approach for tolerating intermittence. In this method, critical states of the processor will be partially-retained before the power failure, then the device will enter an extremely-low power mode. However, this results in full availability of the device only when power interruption is unlikely, which can incur relatively long sleeping periods due to the inevitable power outages in many energy harvesting-powered systems. Chain [10] is another model for programming intermittent devices, in which forward-progress is ensured at the task granularity level. It utilizes idempotent processing concepts to make tasks restartable, whereas they never incur discrepancies and thus act to keep NVM coherent. In [11], a Non-Volatile MIPS Processor (NVP) is introduced in which specific blocks, such as register files and pipeline registers, were replaced by non-volatile elements. NVP uses a checkpointing approach to retain the processor volatile states, which may result in the mentioned internal and external inconsistencies in non-volatile elements. Additionally, the mentioned approaches require an extra supporting circuitry such as capacitor arrays and voltage detection systems that impose large area consumption, which is a critical challenge for area-constrained IoT devices since conventional NV-FF register-based designs cannot detect power failure to store and to retain checkpoints without these additional circuits.

Moreover, the ever-increasing growth in the usage of energy-harvesting powered devices amplifies their hardware security issues. Hardware security threats in the integrated circuit (IC) supply chain, including hardware counterfeiting and Trojans, reverse engineering and IP piracy cost the US economy more than $200 billion annually [12]. Logic encryption/locking [13, 14] techniques are developed as highly-used countermeasures for reverse engineering, injecting hardware Trojan and tampering with IP privacy [15]. In [13, 15], XOR-XNOR key gates are inserted to hide designs' logic functionalities. Roy et al. in [13], randomly inserted XOR-XNOR gates to make a design resilient in presence of physical tampering. Alasad et al. [16] inserted MUXs instead of XOR-XNOR gates in a way that maximizes the hamming distance between the correct and incorrect outputs. These techniques are susceptible to most critical reverse engineering attacks, such as sensitization [14] and Boolean Satisfiability (SAT) based attacks [17]. So, several techniques as countermeasures for SAT attacks such as Anti SAT [18], which is vulnerable to SPS attacks [19], and SARLock [20], which is vulnerable to DDIP. Since implementing this technique requires reconfigurability, conventional CMOS-based implementation leads to increase in area/power consumption and complexity. Therefore, emerging technologies, such as Spintronics [21], are being studied.

In this paper, we propose a new approach to eliminate the need for checkpointing while reducing data movement via intrinsic pipelining capabilities of non-volatile elements in the datapath. In particular, non-volatile datapaths will be researched by designing spin-based polymorphic gates which embed non-volatility within the logic elements themselves. The designed polymorphic gates provide limited reconfigurability, which is leveraged to increase hardware security features via logic encryption.

2 PROPOSED APPROACH

2.1 Secure intermittent-robust PG-based design

2.1.1 Spin-based polymorphic gate (PG). Polymorphic electronics were introduced in [22], whereby a PG would be an AND gate or OR gate depending if VDD is 3.3V or 1.5V, respectively. Various CMOS-based polymorphic gates have employed mechanisms such as

Table 1: Simulation Parameters of SHE-based PGs.

Parameter	Description	Value
3-PG	HM Volume (L×W×T)	100×60×3 nm^3
	MTJ Area (L×W)	60×30×$\pi/4$ nm^2
5-PG	HM Volume (L×W×T)	150×80×3 nm^3
	MTJ Area (L×W)	80×40×$\pi/4$ nm^2
$I_{C\text{-}3\text{-}PG}$	SHE1 Critical Current	108 μA
$I_{C\text{-}5\text{-}PG}$	SHE2 Critical Current	139 μA
θ_{SHE}	Spin Hall Angle	0.3
ρ_{HM}	Resistivity	200 $\mu\Omega.cm$
ϕ	Potential Barrier Height	0.4 V
t_{ox}	Thickness of oxide barrier	1.2 nm
α	Gilbert Damping factor	0.08
M_s	Saturation magnetization	10e5 A.m^{-1}

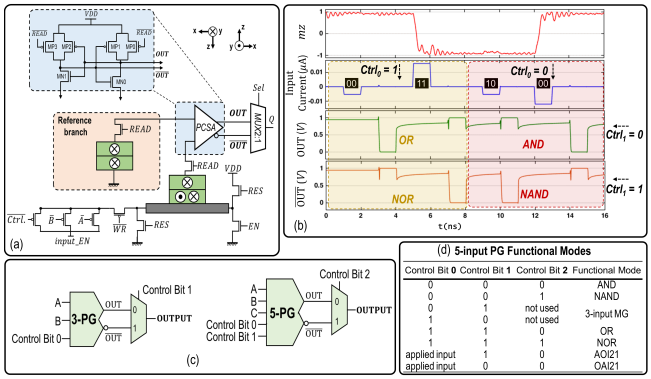

Figure 1: (a) SH-MTJ based 3-input PG, (b) 2-input OR, NOR, AND and NAND logic using 3-input PG, (c) 3-input and 5-input SHE-MTJ based PGs, (d) 5-input PG Functional Modes.

gradations in VDD and signaling levels, or temperature to achieve reconfigurability. Meanwhile, the spin-based devices can naturally function as polymorphic threshold gates since their computational mechanism is accumulation-mode operation that realizes reconfigurable logic functions with inherent security attributes [23, 24]. Figure 1(a) shows the schematic of 3-input Non-Volatile Polymorphic Gates (NV-PGs), which is designed using spin-Hall Effect (SHE)-based Magnetic Tunnel Junction (MTJ) devices. A pre-charge sense amplifier (PCSA) [25] is utilized to sense the state of the SHE-MTJs. Reference MTJ dimensions are designed such that its resistance value in parallel configuration is between low resistance, R_{Low}, and high resistance, R_{High}, of the PG cells. The minimum current required for switching the state of the SHE-MTJ devices is called the critical current (I_C), which is relative to the dimensions of the device. In an n-input NV-PG, the device is designed such that at least (n-1)/2 of the input transistors should be ON to produce a switching current amplitude greater than the critical current. For instance, by affixing one of the three input transistors in ON or OFF states upon demand during the circuit operation, then a 2-input OR gate or a 2-input AND gate can be realized, respectively.

The functionality of the proposed 2-input OR, NOR, AND, and NAND gates implemented by SHE-MTJ based PGs have been validated by SPICE circuit simulator using parameters listed in Table 1, as shown in Fig. 1(b). Figure 1(c) shows the proposed 3-input and 5-input PGs containing two and three control bits, respectively, which can determine the functional modes of the gates. For instance, various functional modes of a 5-input PG are shown in Fig. 1(d). The PGs utilize intra-gate control to provide a functionally-complete set of Boolean logic expressions.

2.1.2 PG-based flip-flop (PG-FF) design. The PG-FF circuit is composed of an NV-PG based master latch using SHE-MTJ devices, as well as a CMOS-based slave latch, as shown in Fig. 2(a). In A PG-FF, a targeted Boolean logic can be implemented and stored in non-volatile (NV) PG within the master latch, where data can be held during the power OFF interval due to the non-volatility feature of SHE-MTJs. While, the stored data in NV-PG can be read and moved to the slave latch when the power is ON again. The proposed PG-FF circuit can intrinsically compute the primary Boolean expressions, in addition to storing a value with near-zero standby power, resulting in area, complexity, and power reductions. Moreover, utilization of LE-FFs in large scale designs reduces the duration of signal propagation between two NV elements in which data will be lost if a power failure occurs. Without non-volatility, then upon power resumption, pipeline flushing would be required along with a sufficient checkpointing mechanism in hardware and/or middleware. Those may be too costly or prohibitive in lightwieght energy-harvesting circuits.

PG-FF functionality is verified by SPICE circuit simulation using the SHE-MTJ model developed by Kazemi et al. [26], as depicted in Fig. 2(b). The SHE-MTJ is initially in the Parallel (P) configuration, which denotes binary "0". The applied inputs ABC = 001 produces an

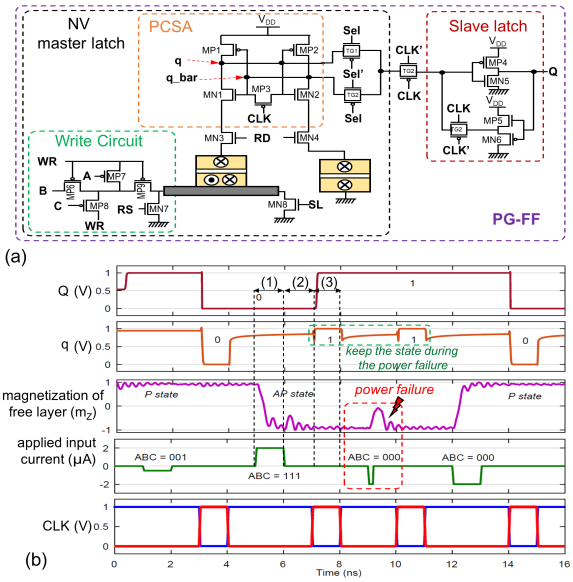

Figure 2: (a) Schematic of PG-FF circuit, and (b) functionality of PG-FF in presence of power failure.

input charge current of |-56| μA, which is smaller than SHE-MTJ critical current, i.e., I_C=108 μA. Thus, the SHE-MTJ state is not changed and remains in the P state, which in the next cycle denotes binary 0 as an output of the slave latch. Then, the input is set to ABC = 111 generating a 196 μA charge current that changes the SHE-MTJ's state from P to an anti-parallel (AP), hence the slave latch outputs one in the next cycle. The third and fourth cycles show its functionality in presence of power failure and power-up situations, respectively. Due to the non-volatility feature of SHE-MTJ devices, its state remains unchanged during the power-off, which verifies the desired forward progress of the design's operation while supporting intermittent operation. In order to design optimized NV architectures using the proposed PG-FF, we will develop a systematic methodology, which incorporates all PG-FF features to design power-failure tolerant architectures. The proposed approach leverages the maximum capability of PG-FFs in terms of replacement and implementation steps.

2.1.3 Low-energy barrier PG-FF design. Energy-harvesting- powered devices are characterized by having charge/discharge cycles, which may occur hundreds of times per minute due to the capacity limitation of power supplies. Although NV-FF and PG-FF implementations provide power failure tolerant designs, the write energy consumption of NV elements remains an issue, which can lead to an increase in the number of charge/discharge cycles. On the other hand, since the power-off periods are normally less than a second in energy-harvesting-powered devices, the NV elements in PG-FFs are required to retain the stored data for only a few seconds to ensure the forward progress. Thus, in this paper the thermal barrier properties of the nanomagnet are leveraged to achieve the required retention time, i.e. the average time period before the magnetization of the nanomagnet flips due to thermal noise, while reducing the write energy consumption.

The NV attributes of SHE-MTJ devices can be tuned to meet these goals. The energy barrier and retention time are related by the following expression [27], $\tau = \tau_0 exp(\Delta/kT)$, where Δ represents the thermal barrier of the nanomagnet and it is related to the uniaxial anisotropy (H_K), saturation magnetization (M_s) and the volume of a nanomagnet (Vol.) through $\Delta = (H_K)(M_s)(Vol.)/2$. τ_0 is a material dependent quantity that can range from 1 ps to 1 ns [27]. For most memory-centric applications, the retention time τ is arranged to be 10-15 years by choosing a Δ between 40-60 kT. On the other hand, the critical spin-current is linearly proportional to the thermal barrier, Δ [28]. Thus, for applications that do not require retention times of years, the thermal barrier of nanomagnets can be reduced by lowering their volume, uniaxial anisotropy or their saturation magnetization. This ultimately reduces the charge currents that are required for write operation, which can result in significant energy improvement due to the quadratic relationship between the Ohmic (I^2R) losses and the input write currents. In this paper, PG-FFs using SHE-MTJ devices with 30kT energy barriers are investigated that can achieve retention times ranging from minutes to hours, while providing at least 50% energy reduction.

2.1.4 Secure PG-FF design. The reconfigurability characteristic of SHE-MTJ based PGs is achieved by means of the multiplexer (MUX) and control bits existing in their structure. Despite the area and performance overheads imposed to the design by using PGs, they can be utilized for logic encryption in addition to enabling intermittent computing, which can provide the hardware with increased security capabilities. In the proposed approach, each PG and its corresponding MUX can be leveraged as the encryption key gates, which increases the key bit space. It means to retain the correct operation of the design, the appropriate key bits of both PGs and MUXs should be applied. The length of the key is determined by the number of inserted PG-FFs, which is normally greater than or equal to the number of output bits. While, in the previous MUX-based logic encryption methods [15, 16], the key length is limited to the number of outputs in a design. The vulnerability of PG-FF based circuits is similar to that of the designs that are secured by the random insertion of XOR/XNOR gates [13, 15]. In the proposed approach, the PGs will be inserted to the logic circuits based on a methodology that is designed to enable intermittent computing. Therefore,

the main focus of the methodology is on intermittency-resilient and the logic encryption is the secondary objective. Thus, the inserted PGs and MUXs may not enable the intermittent-robust design to achieve the optimum Hamming distance (HD) of ~50%, which is a security metric defined based on the number of bit positions at which a correct and faulty output are different. In order to minimize the memory overhead, the configuration bits of PGs and MUXs, which are considered as key bits should be stored in an external non-volatile memory. To implement and synthesize an optimized, secure, and intermittent-resilient logic circuit using PG-FFs, a systematic methodology is developed that is described in the next section.

2.2 PG insertion methodology

To design optimized NV architectures using the proposed PG-FF, we develop a methodology that incorporates all PG-FF features to design partially-secure power-failure tolerant architectures. This approach leverages the maximum capability of PG-FFs in terms of replacement and implementation steps, which incorporates various criteria to design a tolerant circuit in the presence of power failure with minimum PDP overhead.

The proposed algorithm, which is developed in Python consists of two main procedures: (1) `intermittency()`, and (2) `logic encryption()`. The PG insertion methodology takes a Hardware Description Language (HDL) representation of a datapath and PG-based gate modules as its inputs and produces an optimized NV-enhanced datapath. The proposed methodology is described in Algorithm 1, which first explores the HDL of the logic circuit and finds the gates and pipeline registers that can be combined and replaced by spin-based PG-FF circuits, and the remainder of the pipeline registers will be replaced by NV-FFs. Next, the optimized intermittent-robust design is investigated to encrypt the datapath and generate a key based on Hamming distance (HD) calculations as a security metric. In particular, the algorithm first finds all of the FFs in the design, and then checks the cone of logic gates connected to the inputs of the FFs. If each cone of gates meets the circuit-level criteria mentioned below, then the cone and its corresponding FF can be replaced by an PG-FF cell. The three primary criteria regarding the intermittency issue are:

Criterion #1: it should be possible to implement the cone of gates with a single PG. Since each PG-FF operates in one clock cycle, the cone of combinational logic gates that are merged with a master latch should operate within one clock cycle to ensure the correct functionality. Hence, use of more than one PGs for complex functions could increase propagation delay, which might lead to timing violations.

Criterion #2: fan-out of every gates in the cone should not exceed one. This is mainly because in the process of PG-insertion a multiple logic gates can be implemented by a single PG that exists in the structure of the PG-FF's master latch. Therefore, the logic gates existing in the cone will not have separate outputs to drive other logic gates, and there will be only one output for the PG showing the combined logic of the merged gates.

Criterion #3: none of the gates in the cone should be connected to the output of another FF. This will cause the selected cone to include two FFs requiring two clock cycles for operation, while based on the developed algorithm the cone will be replaced by a single PG-FF resulting in a timing violation. Therefore, due to the timing considerations, each of the cones can include only a single FF and multiple logic gates.

If all of the aforementioned conditions are satisfied, then the cone of gates and their corresponding FF will be replaced by a single PG-FF. Otherwise, only the FF is replaced by a simple NV-FF. Herein, the primary objective of the algorithm is implementation of intermittent-robust datapaths. The secondary objective is enhancing hardware security through logic encryption using the inserted PGs. In order to reduce the overhead of logic encryption, the proposed algorithm follows a recursive process to find the minimum key length required to achieve a desired security, which is directly related to the number of inserted PGs utilized for encryption. In particular, first the logic-encryption procedure takes the intermittent-resilient datapath from the intermittency procedure, and starts with using only one PG to generate the key and calculates the HD between the correct and wrong output bits. Then, the procedure checks the below criteria (4) and (5), and if they are achieved it will stop. Otherwise it will increment the number of PGs utilized for producing the key and repeats this process until one of the below criteria are met:

Criterion #4: roughly 50% HD is achieved. To maximize the security of a PG-inserted design, the correlation between the wrong output and the correct output should be minimized to achieve better encryption. Thus, the measured HD value needs to be approximately 50% to demonstrate a highly-encrypted implementation.

Criterion #5: increasing the key length has less than 1% effect on the calculated HD values. This means that if increasing the number of PGs used for logic-encryption is not significantly improving the HD values, then the procedure stops and outputs the key. In particular, every time that the key length is incremented, the following expression $HD_{(n)} \simeq \frac{1}{m} \sum_{i=n-m-1}^{n-1} HD\_list[i]$ is used to compare the current HD value with the average of last m measured HDs, where m is defined by user based on the security demands, and n is the total number of inserted 3- and 5- input PG-FFs. Finally, the key bits that satisfy the security metrics with the minimum overhead, are stored in an external NVM, and the encrypted intermittent-resilient datapath is generated.

3 SIMULATION RESULTS

In this section, we have utilized ISCAS-89, ITC-99, and MCNC benchmark circuits to evaluate the performance of our proposed PG-insertion methodology. For instance, third row in Table 2 lists the gate counts of various ISCAS-89 benchmark circuits when the FFs are simply replaced by NV-FF, while the fourth row shows the decreased number of logic gates when the PG-insertion methodology is applied. Moreover, the last three columns illustrate the investigated security metrics including key length, HD, and logic key that is the maximum number of PG-FFs used within the datapath. The key length is directly proportional to the number of 3-input and 5-input PGs inserted into the design.

Algorithm 1 PG-insertion Methodology

Input: Hardware Description Language (HDL) code
Output: Logic-encrypted intermittent-robust HDL code
procedure `intermittency()`
    gate_list ⟵ all FFs in a netlist
    for i ⟵ 1 to length(*gate_list*) **do**
        input_list ⟵ inputs of connected gate to $gate_i$
        for item in *input_list* **do**
            check (criterion #3)
            update (*input_list*)
            check (criterion #1 and criterion #2)
            update (*gates_cone*)
            go to 6 until one of each criterion is violated.
        end for
        replace (*gates_cone* by PG_FF) **if** size (*gates_cone*) > 2 **else replace** (*gates_cone* by NV_FF)
        update HDL code
    end for
end procedure
procedure `logic encryption()`
    for n ⟵ 1 to #inserted PG-FFs **do**
        key_size ⟵ $2^{3n_1+2n_2}$ ▷ n ⟵ n_1(#5-PG-FFs) + n_2(#3-PG-FFs)
        compute $HD_{(n)}$ based on *key_size*
        store (key bits in NVM) **if** (criterion #4 or criterion #5) **else** (HD_list ⟵ $HD_{(n)}$)
    end for
end procedure

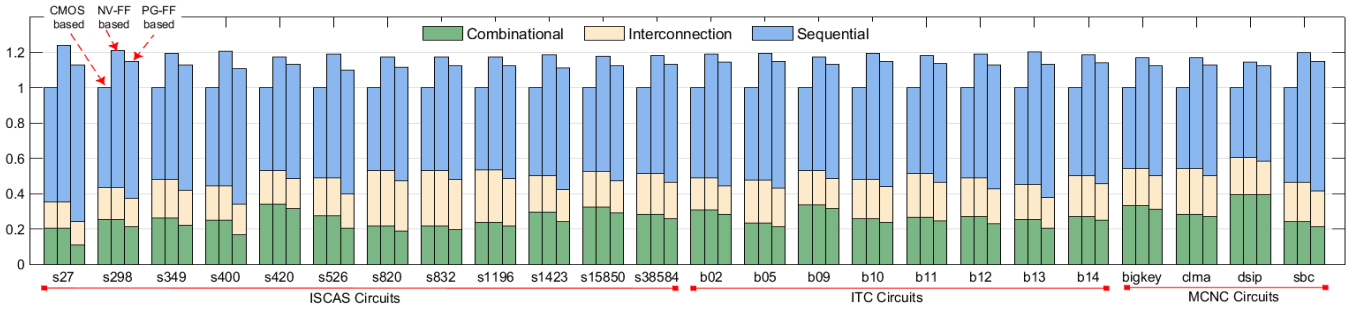

Figure 3: Normalized area consumption compared to CMOS-based implementations for ISCAS, ITC, and MCNC benchmarks.

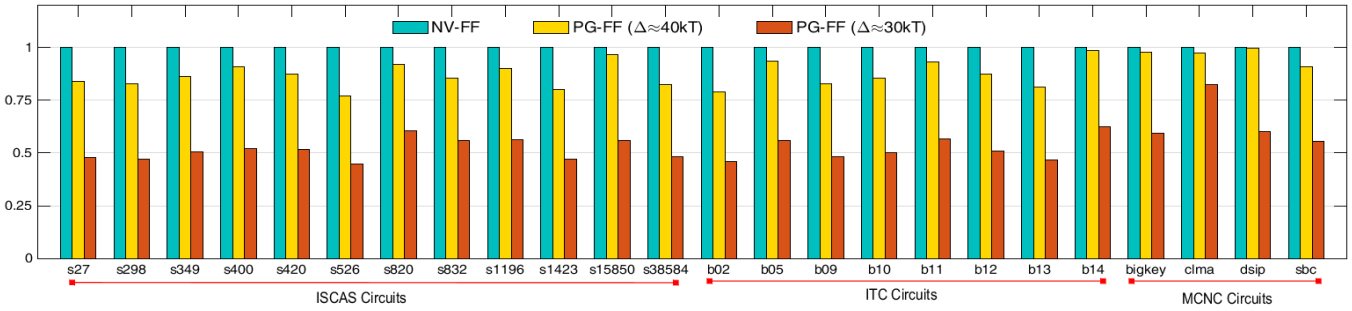

Figure 4: Normalized PDP compared to NV-FF based implementations for ISCAS, ITC, and MCNC benchmarks.

The best HD values are achieved when all of the PG-FFs are considered as logic keys. However, in larger designs, the obtained HD values are relatively low since the ratio of inserted PGs to total number of gates existing in the design is small. This is mainly because the primary goal of the proposed PG-insertion methodology is to support intermittent-computing, while various alternative methods proposed in [14, 15] can be leveraged to further fortify the security of the design.

Table 2: PG-insertion results for ISCAS benchmarks.

ISCAS 89	Circuit Function	Gate-Equivalent NV-FF	Gate-Equivalent PG-FF	#Logic Key	#Key bits	Best HD
s27	Logic	10	8	2	4	0.142
s298	PLD	119	49	11	24	0.125
s349	4-bit Mult.	161	102	7	14	0.063
s400	TLC	164	144	22	49	0.229
s420	Frac. Mult.	218	152	6	12	0.057
s526	TLC	193	83	22	50	0.196
s820	PLD	289	259	10	20	0.035
s838	Frac. Mult.	446	329	14	28	0.061
s1196	Logic	529	459	8	20	0.015
s1423	Logic	657	396	54	116	0.135
s15850	Logic	9772	8942	207	423*	0.092
s38584	Logic	19253	12504	303	675*	0.037

*Using 128-length key bit, obtains 0.028 and 0.007 HD, respectively.

3.1 Area Analysis

Figure 3 compares the area consumption between CMOS, NV-FF, and PG-FF based implementations using various ISCAS-89, ITC-99, and MCNC benchmarks. The results obtained are normalized to the area consumption of conventional CMOS-based circuits. In all of the investigated designs the interconnection area remains relatively unchanged, since replacing FFs does not significantly affect the interconnection circuitry. In the NV-FF based design, the combinational logic remains unchanged compared to CMOS-based design, while the area of the sequential logic is increased since the NV-FF includes more transistors in their structure than CMOS-based FF circuit due to the additional write and read circuitry. The proposed PG-insertion methodology leverages PGs to implement portions of the combinational logic within the PG-FFs without adding overhead to the sequential logic. Thus, the combinational logic in PG-FF based datapaths is smaller than CMOS and NV-FF based designs. For instance, benchmark circuit *s1423* originally has 657 gates, which is reduced to approximately 60% of the original number of gates, i.e. 396 gates, after the PG-insertion algorithm is applied. This improvement leads to a reduction in area consumption, as well as routing complexity. Since the spintronic devices can be vertically fabricated on top of CMOS transistors, their corresponding area overhead is negligible. The results shown in Fig. 3 exhibit that the proposed PG-insertion methodology can achieve an average of 7.1%, 4.2%, and 3.4% improvements in terms of area consumption for ISCAS-89, ITC-99, and MCNC benchmark circuits, respectively, compared to NV-FF based implementations.

3.2 Power-Delay Analysis

Figure 4 shows the power-delay-product (PDP) values for NV-FF, PG-FF, and low-energy barrier PG-FF based implementations using various ISCAS-89, ITC-99, and MCNC benchmark circuits. The results exhibit an average of 13.6%, 12.3%, and 3.5% PDP improvements, respectively, for PG-FF based designs compared to NV-FF based implementations, in which the CMOS-based FFs are simply replaced by NV-FFs. This improvement is mainly achieved through reducing the combinational logic in the PG-inserted designs as explained in previous section, while the PDP values for interconnection and sequential logic remain unchanged. As shown in Fig. 4, further PDP improvements can be achieved by using low energy barrier SHE-MTJ devices within PG-FFs at the cost of smaller retention times. However, in the energy-harvesting-powered IoT devices, a retention time in range of days and hours could be sufficient to achieve proper functionality. Therefore, the energy barrier of SHE-MTJ devices can be reduced to 30kT, realizing 25% reduction in switching critical current ($I_C \propto \Delta$) and approximately 44% decrease in write energy consumption ($E \propto I^2$), while providing non-volatility for a few hours. Thus, leveraging SHE-MTJ devices with 30kT energy barrier provides up to 48.5% and 40.5% average PDP improvements compared to NV-FF based designs and PG-FF based implementations with SHE-MTJ devices having $\Delta = 40kT$, respectively, without incurring any area overhead. It is worth noting, that the results provided herein are obtained at the gate level and physical design parameters are not considered within the document space available.

4 CONCLUSIONS

Energy-harvesting-powered (EHP) devices have recently attracted considerable attentions as a sustainable computing platform for a wide range of applications. These devices are characterized by intermittent operation due to unpredictable energy failures. In this paper, we have developed a systematic methodology to realize middleware-transparent intermittent computing through insertion of NV-PGs within the logic datapath. The developed PG-insertion methodology takes the HDL representation of a datapath and generates an NV-enhanced datapath using SHE-MTJ based PG-FF circuits, which are used as state-holding elements also realizing basic Boolean logic functions. Therefore, a portion of the combinational logic is implemented within the sequential blocks, leading to area and energy savings compared to the conventional intermittent computing circuits where all of the registers are replaced with NV-FFs. Moreover, the power consumed by the sequential logic can be reduced by using SHE-MTJ devices with lower energy barriers, which can significantly reduce their write operation at the cost of shorter retention times that can be tolerated in EHP devices due to frequent refresh of devices on the datapath, while imparting the intrinsic provision of power outage resilience in energy-harvesting. Finally, PGs can be used for logic encryption due to their reconfigurability characteristic. Therefore, the logic encryption is defined as secondary objective of our proposed methodology, according to which a logic key will be generated based on Hamming distance calculations as a security metric. We applied the proposed algorithm to

various benchmark circuits, including ISCAS-89, ITC-99, and MCNC, to evaluate the performance of our methodology in comparison with NV-FF based implementations. Results obtained exhibit that PG-FF based implementations using SHE-MTJ devices with 30kT energy barrier achieve up to 48.5% and 7.1% reductions in terms of average PDP and area consumption, respectively.

REFERENCES

[1] M. T. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013.

[2] S. Bandyopadhyay and A. P. Chandrakasan, "Platform architecture for solar, thermal, and vibration energy combining with mppt and single inductor," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 9, pp. 2199–2215, 2012.

[3] M. Philipose, J. R. Smith, B. Jiang, A. Mamishev, S. Roy, and K. Sundara-Rajan, "Battery-free wireless identification and sensing," *IEEE Pervasive computing*, vol. 4, no. 1, pp. 37–45, 2005.

[4] A. Ma and A. S. Poon, "Midfield wireless power transfer for bioelectronics," *IEEE Circuits and Systems Magazine*, vol. 15, no. 2, pp. 54–60, 2015.

[5] B. Ransford, J. Sorber, and K. Fu, "Mementos: System support for long-running computation on rfid-scale devices," *Acm Sigplan Notices*, vol. 47, no. 4, pp. 159–170, 2012.

[6] H. Jayakumar, A. Raha, and V. Raghunathan, "Quickrecall: A low overhead hw/sw approach for enabling computations across power cycles in transiently powered computers," in *VLSI Design and 2014 13th International Conference on Embedded Systems, 2014 27th International Conference on*. IEEE, 2014, pp. 330–335.

[7] B. Ransford and B. Lucia, "Nonvolatile memory is a broken time machine," in *Proceedings of the workshop on Memory Systems Performance and Correctness*. ACM, 2014, p. 5.

[8] B. Lucia and B. Ransford, "A simpler, safer programming and execution model for intermittent systems," *ACM SIGPLAN Notices*, vol. 50, no. 6, pp. 575–585, 2015.

[9] D. Balsamo, A. S. Weddell, G. V. Merrett, B. M. Al-Hashimi, D. Brunelli, and L. Benini, "Hibernus: Sustaining computation during intermittent supply for energy-harvesting systems," *IEEE Embedded Systems Letters*, vol. 7, no. 1, pp. 15–18, 2015.

[10] A. Colin and B. Lucia, "Chain: tasks and channels for reliable intermittent programs," in *Proceedings of the 2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications*. ACM, 2016, pp. 514–530.

[11] K. Ma, Y. Zheng, S. Li, K. Swaminathan, X. Li, Y. Liu, J. Sampson, Y. Xie, and V. Narayanan, "Architecture exploration for ambient energy harvesting nonvolatile processors," in *High Performance Computer Architecture (HPCA), 2015 IEEE 21st International Symposium on*. IEEE, 2015, pp. 526–537.

[12] F. Economics, "Estimating the global economic and social impacts of counterfeiting and piracy," *A report commissioned by business action to stop counterfeiting and piracy (BASCAP), An ICC Initiative*, 2011.

[13] J. A. Roy, F. Koushanfar, and I. L. Markov, "Epic: Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, 2010.

[14] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 83–89.

[15] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault analysis-based logic encryption," *IEEE Transactions on computers*, vol. 64, no. 2, pp. 410–424, 2015.

[16] Q. Alasad, Y. Bi, and J.-S. Yuan, "E2lemi: Energy-efficient logic encryption using multiplexer insertion," *Electronics*, vol. 6, no. 1, p. 16, 2017.

[17] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 137–143.

[18] Y. Xie and A. Srivastava, "Mitigating sat attack on logic locking," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2016, pp. 127–146.

[19] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Security analysis of anti-sat," in *Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific*. IEEE, 2017, pp. 342–347.

[20] M. Yasin, B. Mazumdar, J. J. Rajendran, and O. Sinanoglu, "Sarlock: Sat attack resistant logic locking," in *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*. IEEE, 2016, pp. 236–241.

[21] Q. Alasad, J. Yuan, and D. Fan, "Leveraging all-spin logic to improve hardware security," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*. ACM, 2017, pp. 491–494.

[22] A. Stoica, R. Zebulum, and D. Keymeulen, "Polymorphic electronics," *Evolvable Systems: From Biology to Hardware*, pp. 291–302, 2001.

[23] A. Roohi, R. Zand, D. Fan, and R. F. DeMara, "Voltage-based concatenatable full adder using spin hall effect switching," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 12, pp. 2134–2138, Dec 2017.

[24] A. Roohi, R. F. DeMara, L. Wang, and S. Köse, "Secure intermittent-robust computation for energy harvesting device security and outage resilience," 2017.

[25] W. Zhao, C. Chappert, V. Javerliac, and J.-P. Noziere, "High speed, high stability and low power sensing amplifier for mtj/cmos hybrid logic circuits," *IEEE Transactions on Magnetics*, vol. 45, no. 10, pp. 3784–3787, 2009.

[26] M. Kazemi, G. E. Rowlands, E. Ipek, R. A. Buhrman, and E. G. Friedman, "Compact model for spin–orbit magnetic tunnel junctions," *IEEE Transactions on Electron Devices*, vol. 63, no. 2, pp. 848–855, 2016.

[27] L. Lopez-Diaz, L. Torres, and E. Moro, "Transition from ferromagnetism to superparamagnetism on the nanosecond time scale," *Physical Review B*, vol. 65, no. 22, p. 224406, 2002.

[28] J. Z. Sun, "Spin-current interaction with a monodomain magnetic body: A model study," *Physical Review B*, vol. 62, no. 1, p. 570, 2000.