electronics

MDPI

Article

Spin Orbit Torque-Assisted Magnetic Tunnel Junction-Based Hardware Trojan

Rajat Kumar, Divyanshu Divyanshu, Danial Khan, Selma Amara and Yehia Massoud *

Innovative Technologies Laboratories (ITL), Computer, Electrical and Mathematical Sciences & Engineering (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal 23955 , Saudi Arabia; rajat.kumar@kaust.edu.sa (R.K.); divyanshu.divyanshu@kaust.edu.sa (D.D.); danial.khan@kaust.edu.sa (D.K.); selma.amara@kaust.edu.sa (S.A.)

* Correspondence: yehia.massoud@kaust.edu.sa

Abstract: With the advancement of beyond-CMOS devices to keep Moore's law alive, several emerging devices have found application in a wide range of applications. Spintronic devices offer low power, non-volatility, inherent spatial and temporal randomness, simplicity of integration with a silicon substrate, etc. This makes them a potential candidate for next-generation hardware options. This work explores the giant spin Hall effect (GSHE)-driven spin-orbit torque (SOT) magnetic tunnel junction (MTJ) as a potential candidate for creating an externally triggered hardware Trojan and insertion into logic-locked hardware security considering the effect of process and temperature variations.

Keywords: giant spin Hall effect (GSHE); hardware security; hardware trojan; magnetic tunnel junction (MTJ); spintronics; spin-orbit torque (SOT); spin-transfer torque (STT)

check for updates

Citation: Kumar, R.; Divyanshu, D.; Khan, D.; Amara, S.; Massoud, Y. Spin Orbit Torque-Assisted Magnetic Tunnel Junction-Based Hardware Trojan. *Electronics* **2022**, *11*, 1753. https://doi.org/10.3390/electronics11111753

Academic Editor: Paris Kitsos

Received: 14 April 2022
Accepted: 30 May 2022
Published: 31 May 2022

1. Introduction

In recent years, the increasing trend of outsourcing integrated circuits (ICs) design and fabrication in their foundries has led the semiconductor companies to rely on third party fabrication facilities [1]. This approach helped to cut costs and accelerated time-to-market, but it also raised serious concerns about whether an IP owner and a third party can establish trust [2]. A number of attacks such as IC overproduction [3], IC cloning [4], IP piracy [5], and hardware Trojan insertion [6] can be carried out by an untrusted foundry. For off-shore fabrication to stay secure, the capability of the IP owner must be thoroughly proven to prevent such attacks. Hardware Trojan insertion is a malicious modification in the original IC design during the fabrication process by the attackers [7,8]. It can lower the IC security by leaking confidential information, causing field malfunctioning, or even destroying the IC using predesigned conditions [9]. Therefore, a hardware Trojan can cause profit loss in consumer devices and be life-threatening if used in military devices. Hence, we can say that the hardware Trojan is a significant threat to both the government and other organizations that require security for their systems.

Figure 1a shows the taxonomy of the hardware Trojan, and the highlighted flow represents the targeted levels for designing the Trojan in this work. Figure 1b represents the taxonomy for Trojan detection based on pre-silicon and post-silicon stages. Figure 1c shows the block diagram of the system-on-chip (SoC) design flow with the targeted Trojan insertion at a later stage in the SoC design flow, thus bypassing primarily pre-silicon tests. Test time detection techniques compare side-channel behavior [9,10] and/or functional verification of the suspected ICs to the "golden model" (Trojan-free IC model). The suspected IC is classified as Trojan infected if it differs significantly from the golden model. However, whether golden models can be generated for real-world applications still remains an open question.

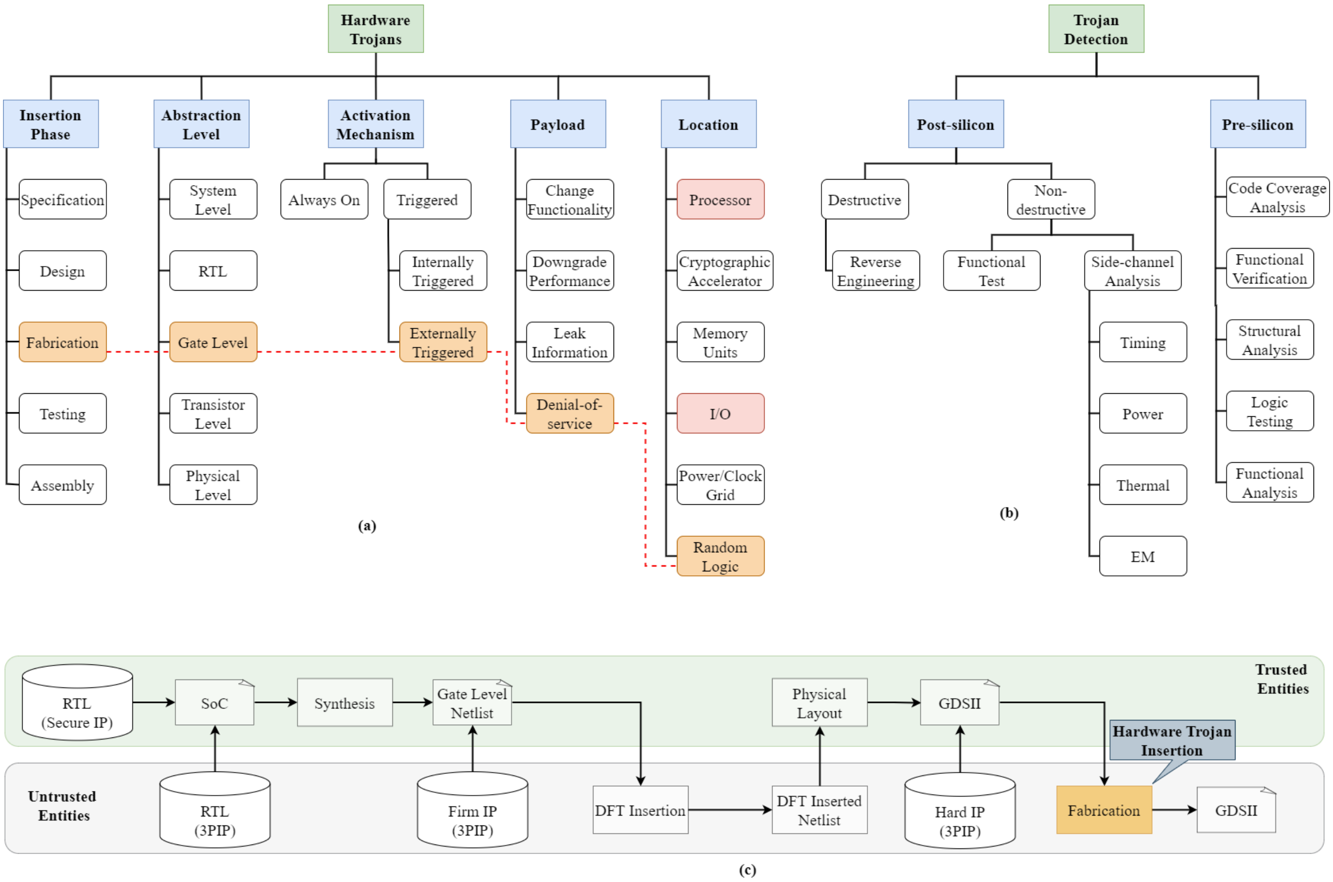


Figure 1. (**a**) Taxonomy of hardware Trojans and selected flow for this work. (**b**) Taxonomy of hardware Trojan detection. (**c**) System-on-chip (SoC) design flow.

With the increasing complexity of IP blocks in the SoC design flow and reduced feature size, the effect of process variations in each block makes it extremely difficult to detect intelligently designed Trojans whose insertion phase, abstraction level, triggering mechanism, type of payload, and location are unknown. This work uses the spin-orbit torque-assisted magnetic tunnel junction (SOT-MTJ) to design a sneaky Trojan. It is designed to be inserted during the fabrication stage. With the improvement in the lithography process, the ability to fabricate MTJ with a smaller dimension in sub-5 nm has been demonstrated recently [11]. The motivation for current work is drawn from the fact that spintronics-based devices offer interesting aspects for hardware security [12]. Insertion of Trojans at the fabrication stage by an untrusted foundry is extremely difficult to detect as the empty spaces in the SoC can be utilized. The fabricated SoC offers limited verification and validation options discussed in more detail in Section 4.4. The Trojan is designed to be externally triggered, thus making its activation an infrequent event. The current trust benchmarks for hardware Trojans are available at http://www.trust-hub.org/benchmarks.php (4 April 2022). There have been no standard benchmarks for comparing the impacts of hardware Trojans and detection techniques for such an emerging MTJ-based device when writing this paper. Thus, sneakier and experimentally validated MTJ-based Trojans can pose a severe threat to IC design which needs to be countered in the near future.

The rest of the paper is organized in the following manner. Section 2 discusses hardware Trojan and MTJ. In Section 3, the operation of the hardware Trojan is explained. Section 4 demonstrates experimental results and post-silicon Trojan detection techniques. Section 5 finally concludes the paper.

2. Background

2.1. Hardware Trojan (HT)

Malicious modification at the hardware level can cause altered IC functionality, leading to disastrous results in security applications. Conventional design-time verification and post-fabrication techniques may not be sufficient to counter emerging hardware Trojan made from emerging beyond-CMOS devices such as spintronic devices, memristors, carbon nanotubes (CNTs), and nanowire FETs (NWFETs), etc. References [13–21] evaluated the performance and reliability of CNT bundles for on-chip interconnect applications due to their large conductivity and current carrying capabilities. Reference [22] presents a comprehensive model for the resistance in graphene nanoribbon (GNR) interconnects. One of our future goals is to explore spintronics devices for memory and/or logic applications, and even for interconnects due to their low-power consumption, non-volatility, and high endurance compared to CMOS technology. CMOS-based hardware Trojans consist of (1) a trigger part that determines when Trojans get activated and (2) a payload that decides what type of changes will happen once the Trojans are triggered. The trigger part usually contains digital or analog counter circuits activated only when certain conditions are satisfied. Spintronic-based Trojans have various advantages over CMOS Trojans. Spintronic hardware Trojans depend on external factors like magnetic field and temperature due to their unique physical characteristics, which can be exploited for external triggering. The hybrid CMOS and MTJ circuits [23] can replace some of the logic gates, and careful designing can make them implement the same functionality with competitive switching, area, and energy consumption compared to the CMOS gates. Reference [24] reports that the amplitude of low-order leakages in masked implementations can be amplified externally by tweaking side-channel measurement setups in a way that is under the control of a power analysis adversary.

2.2. Magnetic Tunnel Junction (MTJ)

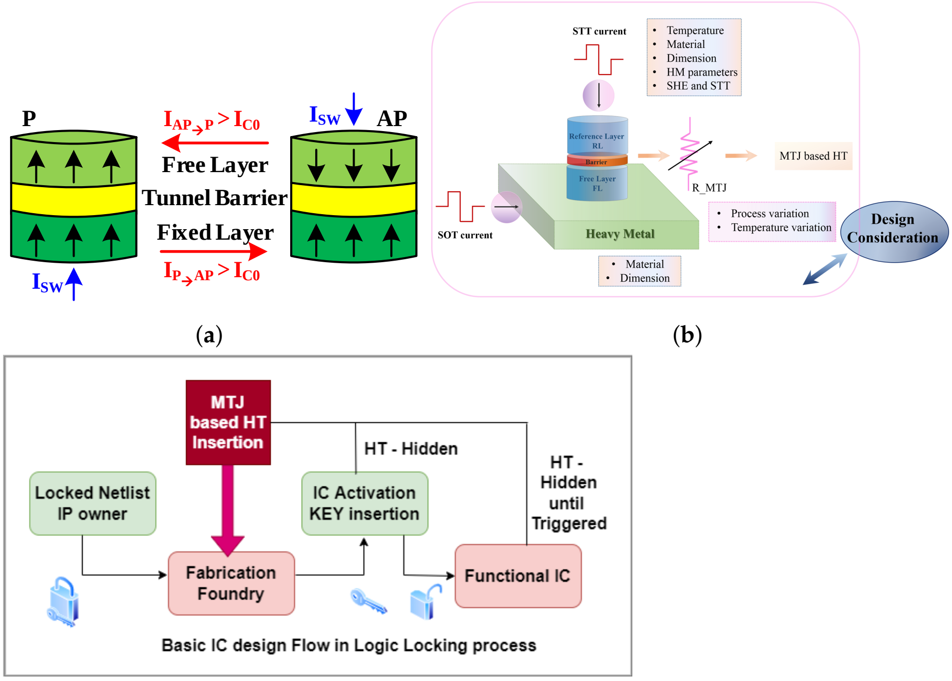
Figure 2a shows a typical MTJ structure comprising two relatively thick ferromagnetic layers (fixed layer and free layer) separated by a relatively thin tunnel barrier layer. When the fixed and free layers have the same magnetic direction (parallel, denoted by P), the MTJ shows a lower resistance (R_P). On the contrary, when the magnetic directions of both layers are opposite (anti-parallel, denoted by AP), the MTJ shows a higher resistance (R_{AP}). The tunnel magnetoresistance (TMR) ratio characterizes the resistance difference and is defined by the following equation:

$$TMR = \frac{R_{AP} - R_P}{R_P} \times 100 \tag{1}$$

If the difference between the resistances in parallel and anti-parallel is significant, it shows higher TMR and readability. When a bidirectional current greater than the critical current (I_{C0}) flows through an MTJ cell, it can switch between parallel and anti-parallel states. The MTJ cell switches from parallel to anti-parallel state when the passing current ($>I_{C0}$) flows from the fixed layer to the free layer. On the contrary, when passing current flows from the free layer to the fixed layer, the MTJ cell switches from the anti-parallel to the parallel state. The magnetic dynamics of the free layer are governed by Landau–Lifshitz–Gilbert (LLG) equation [25], which is given by:

$$\frac{\partial \vec{m}}{\partial t} = -\gamma\mu_0\vec{m} \times \vec{H}_{eff} + \alpha\vec{m} \times \frac{\partial \vec{m}}{\partial t} - \xi P J_{STT}\vec{m} \times (\vec{m} \times \vec{m}_r) - \xi\eta J_{SHE}\vec{m} \times (\vec{m} \times \vec{\sigma}_{SHE}) \tag{2}$$

Here, m and m_r are the unit vector along with magnetization of the free layer and the reference layer, respectively, γ is the gyromagnetic ratio, μ_0 is the vacuum permeability, H_{eff} is the effective magnetic field, α is the Gilbert damping coefficient, P is the polarization factor, J_{STT} and J_{SHE} are the spin-transfer torque (STT) and spin-orbit torque (SOT) current density applied to the MTJ device, and σ_{SHE} is the polarization direction of the spin current injected in the free layer. Figure 2b shows the design consideration for the SOT-MTJ for creating the hardware Trojan.



(**a**) (**b**)

(**c**)

Figure 2. (**a**) A p-MTJ structure and switching between the two states. (**b**) Design consideration for SOT-MTJ. (**c**) Basic IC design flow in logic-locking process.

MTJ has found several applications in hardware security applications like logic locking [26], physically unclonable functions (PUFs) [27], true random number generators (TRNGs) [28], etc. In this work, we designed a hardware Trojan based on SOT-assisted STT-MTJ with an externally initiated triggering (external magnetic field) mechanism. This mechanism allows the Trojan to remain hidden until an external magnetic field of the desired magnitude is applied in the appropriate direction. Due to the unique response of the Trojan block to certain external factors, it may remain hidden to a great extent from the verification process [29]. We have explored Trojan insertion in the logic-locking-based security in this work. The robustness to all detection and verification processes during IC design is currently beyond the work's scope. However, primary Trojan detection methods, as shown in Figure 1b, are discussed in Section 4.4. Nevertheless, new emerging beyond-CMOS devices hold many security concerns and solutions [30]. When both the foundry and user are not trusted, logic locking is widely used to ensure hardware security. The hidden Trojans can bypass the logic-locking mechanism if they operate in the functional IC. The limitations are malfunctioning only for the duration of the external condition, vulnerability to new verification methods to counter it, inability to attack inactivated ICs, design complexity, etc.

3. Hardware Trojan Operation

3.1. Circuit Description of Hardware Trojan (HT) Block

In the proposed work, a compact model of SOT-assisted PMA MTJ-based on the Verilog-A behavioral model [31] is used. The LLG solver described in the Verilog-A model is used to solve the magnetic dynamics of the MTJ. A detailed switching mechanism for the model is provided in [23]. The MTJ-based hardware Trojan block is shown in Figure 3b. It consists of a pre-charge sense amplifier (PCSA), SOT-assisted MTJ, writing circuit, MOS logic circuitry, and a multiplexer, as shown in Figure 3a. PCSA provides the output in TRUE as well as in complementary form. It is used to sense the outputs of the circuit based on the MTJ state, whether it is parallel or anti-parallel. The resistance of MTJ is low in the parallel state compared to the resistance in the anti-parallel state. In one branch of PCSA, we have a SOT-MTJ and the logic circuitry of MOSFETs, whereas, in another branch, we have a reference resistance to compare the resistances of both branches. Depending on the MOS logic circuitry, the switching of MTJ state occurs, and hence the resistance varies. The read path used to read the state of MTJ is also shown in Figure 3a. A multiplexer is used at the output of PCSA to select the desired operation.

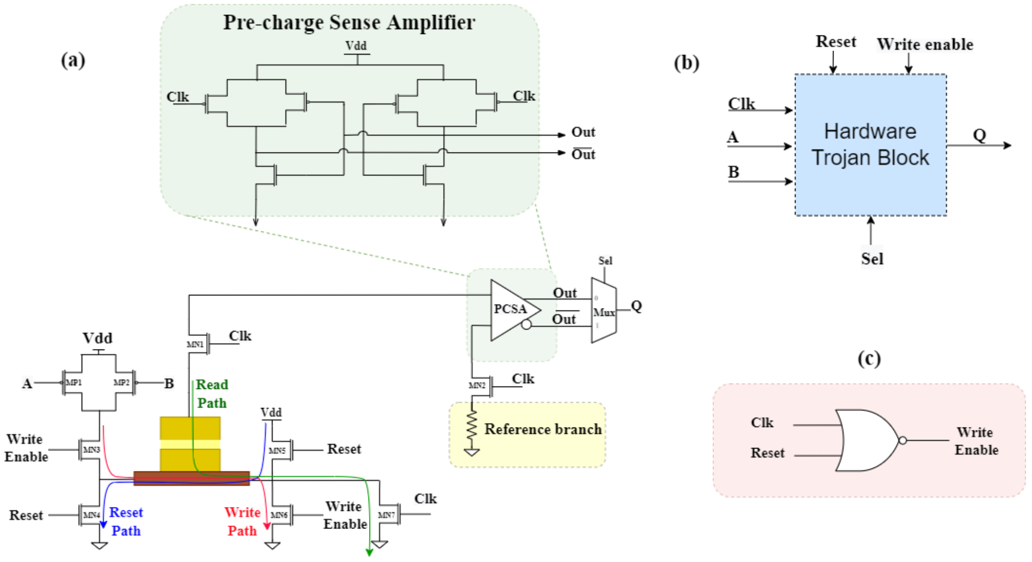


Figure 3. (**a**) Detailed circuit operation of hardware Trojan block. (**b**) Block diagram of Trojan with input and output lines. (**c**) Generation of write enable signal for Trojan block.

The writing circuit for the MTJ comprises four NMOS transistors (MN3–MN6). A reset signal is applied to reset the MTJ to the default state. The reset signal allows the current to flow from supply voltage to the ground through the heavy metal of MTJ and transistors MN5 and MN4. During the writing phase, the write enables signal is made HIGH so that the current flows from the heavy metal through the transistors MN3 and MN6. The amount of current is based on the logic circuitry of PMOS transistors (MP1–MP2). The reset, write, and read paths are shown in Figure 3a using blue, red, and green arrows, respectively.

To write the MTJ correctly, the write enable signal must be turned ON under the following conditions. The first condition is that the clock pulse should be LOW, and the other condition is that the reset signal should be OFF at that time. The condition is displayed using a NOR gate in Figure 3c. If reset, Clk, and write enable signal are made HIGH at the same time, then all three paths (reset, write, and read path) will turn ON simultaneously, and the circuit will perform the false operation. The ability of this kind of architecture to produce complementary output can be utilized to initiate multiple threats. Several counters or timer-based circuits can be designed to activate polymorphic logic. Careful designing of triggering mechanisms and verification will be essential in such cases.

3.2. Logic Locking

Logic locking [32] is a technique that inserts new key inputs and logic mechanisms into the circuit, causing the circuit to behave incorrectly until the correct key combination is provided to the circuit. Various logic-locking techniques have been proposed to protect the privacy and integrity of ICs. When the foundry and user are not trusted, logic locking is the best way to ensure hardware security. The hardware Trojan, which has a low probability of activating, thus can be made operational only when the IC is activated. The logic-locking block will not allow the IC to work. External factors required to trigger the Trojan and the IC can be made to malfunction only after activation.

In Figure 4a, a logic circuit designed using logic gates displaying output Y = AB + BC + CA is present. All gates (G1–G5) are designed using 40 nm CMOS technology. To insert the Trojan block in the circuit, the gate G5 performing AND operation is replaced by a Trojan-based block performing the same operation, as shown in Figure 4b. In logic locking-based hardware security, key management is essential as the attacker aims to obtain the key. Figure 4c shows how the keys are stored in a tamper-proof memory to keep them safe from attackers. These memory units are fabricated on the chip so that the keys are not known to the foundry [33]. Some logically locked blocks are inserted between the logic circuit in Figure 4b so that the correct output is present when the true key is applied. The modified logic circuit is presented in Figure 4d, where the XOR and XNOR gates are used as logically locked blocks. The key for the circuit shown in Figure 4d is k1k2 = 10. For all other values of k1k2, the circuit will provide incorrect output.

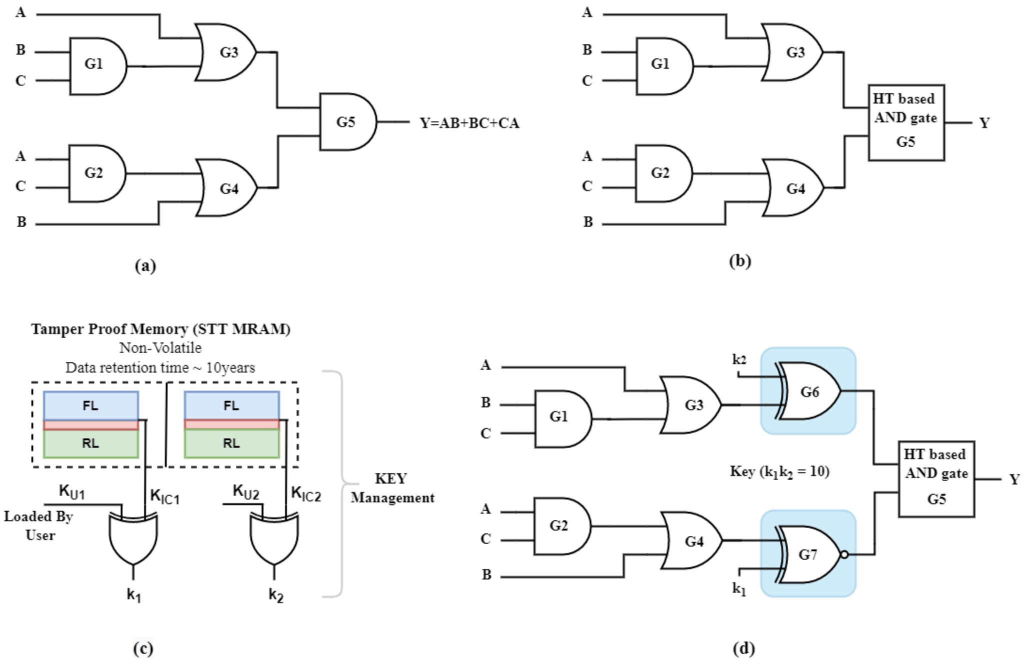


Figure 4. (**a**) Unlocked netlist with Y = AB + BC + CA. (**b**) G5 replaced with MTJ-based hardware Trojan block. (**c**) Key management for logic locking block. (**d**) Locked netlist with MTJ-based hardware Trojan block.

4. Experimental Results

All simulations are performed in 40 nm CMOS technology using a cadence specter simulator with CMOS aspect ratio W/L = 3, and T = 300 K unless otherwise stated. The energy per bit is calculated according to the following equation:

$$E = \int_{0}^{tsw} V_{dd} * i_{dd}(t)\,\mathrm{d}t \tag{3}$$

where t_{sw} is the switching delay, V_{dd} is the supply voltage, and $i_{dd}(t)$ is the total current from the power supply. The write current is set at a value greater than the critical current density required for obtaining a switching probability of 100%. The hardware Trojan with payload to cause a denial of service or permanent malfunction needs to be designed with low energy consumption to remain hidden during the verification process where energy consumption in the IC block is tested. Additionally, for any practical implementation, a detailed analysis of latency, area consumption, fan-in/fan-out, and other circuit parameters need to be optimized. A well-known issue in spintronics-based circuits is the poor driving capability due to short spin diffusion length, which severely restricts the fan-out capacity. Some Trojans are designed to inflict poor performance, and in such cases, the energy consumption is utilized in Trojan to degrade the performance. So, depending on the application, the design of the Trojan needs to be modeled and is subject to tight design constraints.

4.1. P-MTJ Device Single Block

Figure 2a shows the basic p-MTJ structure. When the magnetization is in the in-plane direction instead of the perpendicular direction, the MTJ stack is called IMA MTJ (in-plane magnetic anisotropy MTJ). In this work, we explore p-MTJ-based HT, due to its faster and lower requirement of write current [34]. The height of the MTJ barrier is an important physical parameter that determines the energy difference between the two stable states and the probability of switching. With high $\Delta \approx 60$ kT, the data retention time is around 10 years and has a deterministic switching characteristic which is utilized for non-volatile memory applications [31]. Table 1 shows the MTJ device parameters selected during simulation. The dimension is selected in such a way to ensure operation in a high energy barrier regime.

Table 1. SOT-assisted MTJ parameters set during electrical simulations.

Parameters	Values
MTJ Dimension and Shape	40 nm × 40 nm, circular
Free Layer Thickness	0.7 nm
Oxide Layer Thickness	0.85 nm
HM Length, Width, and Height	60 nm × 40 nm × 3 nm
Gilbert Damping Coefficient	0.03
Saturation Magnetization	800,000 emu/cm^3
TMR	120%
Anisotropy Field	88,000 A/m
Spin Hall Angle	0.3
Heavy Metal Resistance	1000 Ω
Potential Barrier Height of MgO	0.5 V
Simulation Steps	1 ps
Polarization Factor	0.61
Initial Configuration	Set at Parallel

We performed a parametric sweep to determine the effect of the temperature variation and external magnetic field on the free layer magnetization dynamics of a single MTJ block, as shown in Figure 5. Thus, these external parameters affect the MTJ magnetization dynamics, which can be utilized as externally initiated triggering mechanisms. The SOT current density applied was 15 MA/cm^2, and the STT current density applied was 1.59 MA/cm^2, and simulation was performed for 50 ns. Here, B_{ext} is applied in the +z direction, which is along the direction of the MTJ stack.

The temperature variation and its effects are analyzed during testing to determine the optimum range of operation of an IC. It is thus important to test MTJ sensitivity to variation in temperature as the MTJ thermal stability factor is a function of temperature, i.e., $\Delta = \frac{E_b}{K_B T}$, where E_b is the energy barrier height, k_B is the Boltzmann constant, and T is the temperature. Thus, temperature variation may cause a change in logic operation. We need to obtain the range in which the Trojan block will not be triggered and therefore ensure it can pass the verification phase of the IC to be a viable hardware Trojan option. Although temperature variation is one of the externally initiated hardware Trojan triggering mechanisms that can also be exploited to trigger the Trojan, the testing phase consists of a temperature sweep. Our design tries to minimize the change in output logic due to MTJ resistance variation for such a case. A proper voltage divider circuit design can ensure that the circuit has a large thermal stability factor. Any significant change from the expected output may cause Trojan detection.

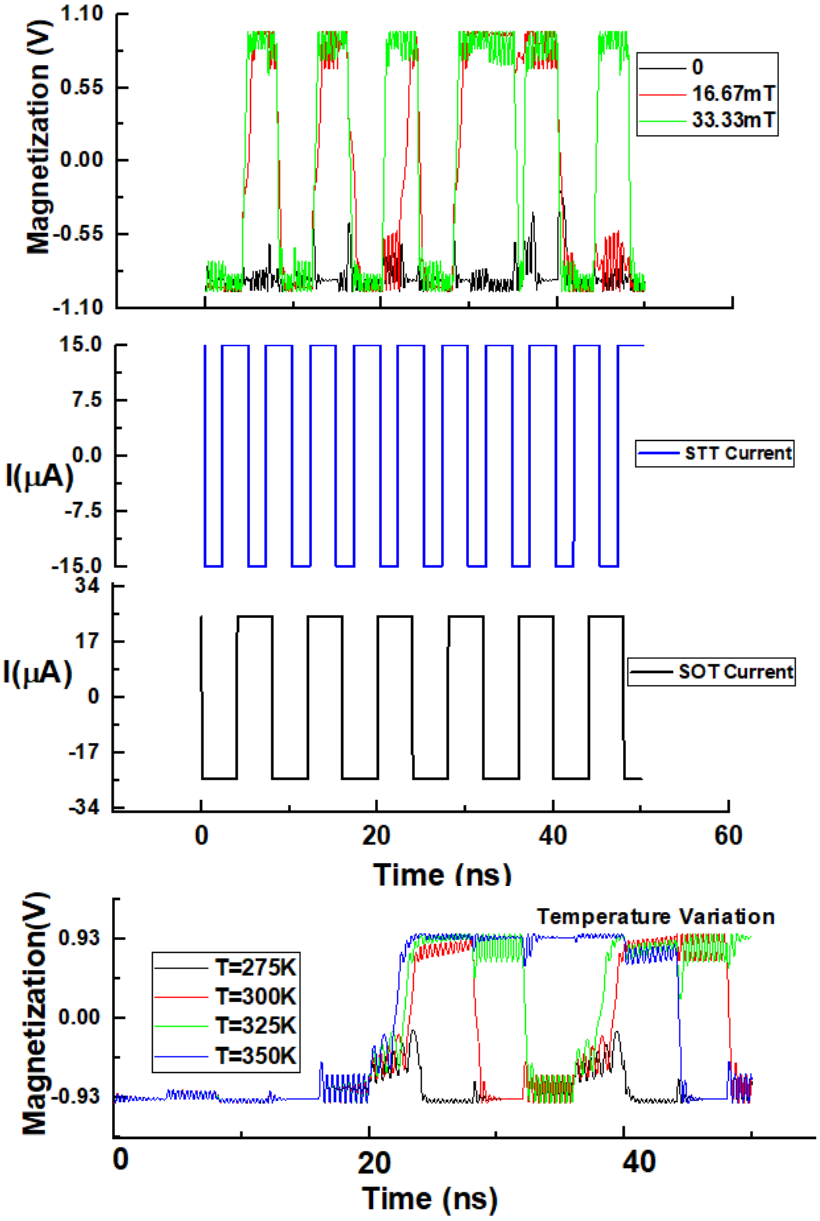
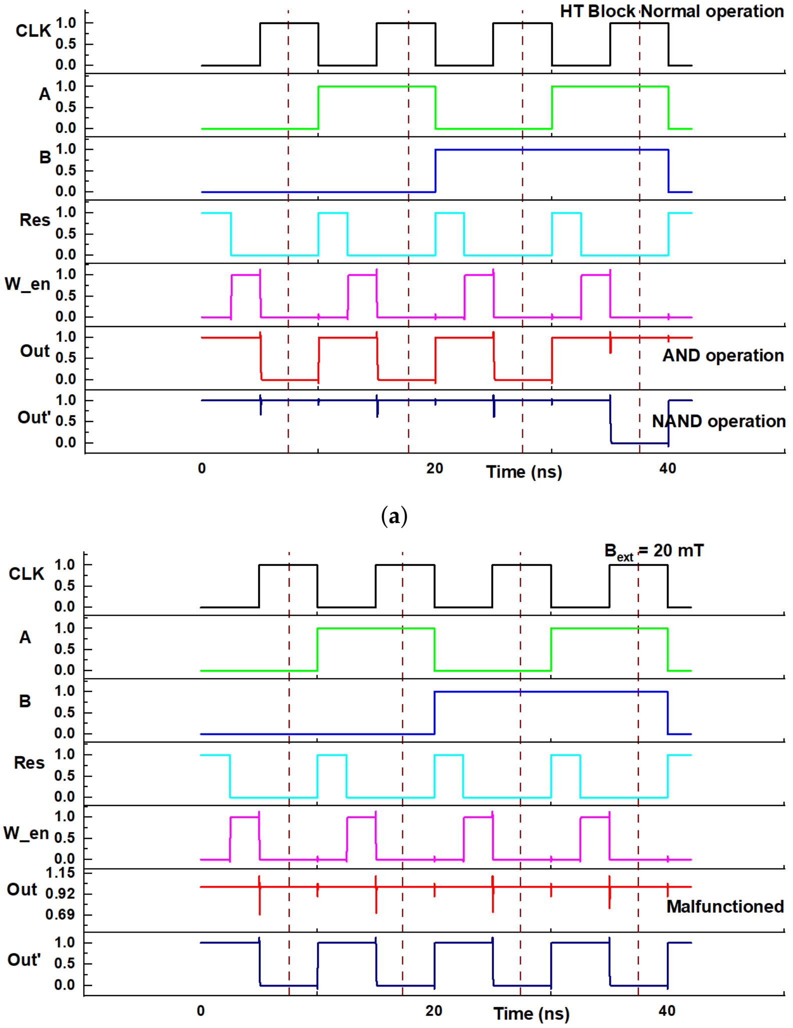


Figure 5. Free layer magnetization vs. applied external field and temperature.

4.2. Hardware Trojan Block

Figure 6a displays output waveform indicating dual logical operation of hardware Trojan block of Figure 3. The outputs of PCSA are passed through a 2:1 multiplexer so we can select the desired operation. The reference branch resistance is set to 22 kΩ, and Vdd is set to 1 V.

The P to AP and AP to P switching are not symmetrical, so the asymmetrical is set to 1.1. The field-like torque component, as mentioned in [31], is set at 0.8. We performed a parametric sweep to determine the critical external magnetic field required for triggering the Trojan block in Figure 3. Design optimization is required to ensure that the Trojan block does not get triggered due to a stray magnetic field and that the $B_{ext,critical}$ is not too large. For our design the value of $B_{ext,critical} \approx 10$ mT, in the +z direction. As the magnetic field is a vector quantity, the applied triggering field must have the vector component larger than $B_{ext,critical}$, in the +z direction. In Figure 6b, $B_{ext} > B_{ext,critical} = 20$ mT is applied, and the output logic of AND/NAND operation is completely disturbed, resulting in IC malfunction until the external condition is applied. Hence, in a small magnetic field with a magnitude of a few mT, the state of MTJ changes, whereas in MOS transistors, a magnetic field of the order of 7 T has very less influence on its characteristics which is manageable [35]. Thus the $B_{ext,critical}$ will not induce any general faults in the IC. If the IC is tested in a high magnetic field with proper chip orientation for fault detection, in that case, the Trojan will be triggered and may be detected.



(**a**)

(**b**)

Figure 6. (**a**) Hardware Trojan block waveforms under normal operation (hidden behavior). (**b**) Hardware Trojan block waveforms under triggered operation (malfunction behavior).

As it is impossible to fabricate any two devices with the exact same dimension, and some deviation is expected, especially in such a multilayer MTJ stack; the robustness to device imperfection is a critical parameter. To analyze the HT block for practical application and tolerance towards process variation (PV), we have considered the PV in some key MTJ parameters: TMR ratio, free layer thickness, and oxide layer thickness. The percentage of PV is varied, and the variation is selected in the form of Gaussian distribution. We then performed 200 Monte-Carlo simulations using the random sampling method. Figure 7a–c show the average MTJ resistance values for different PV percentages with the reference value mentioned in Table 1. MTJ resistance is a critical parameter because the MTJ is practically utilized as a variable resistor in most circuit operations. Table 2 contains the details of the Monte-Carlo results obtained. In the presence of 3% PV, 97.50% of the results obtained implemented the correct logic operation. As the PV percentage increases, the success ratio decreases drastically. Therefore, for any practical insertion of such MTJ-based hardware Trojan, the amount of PV needs to be considered and should be kept to a minimum.

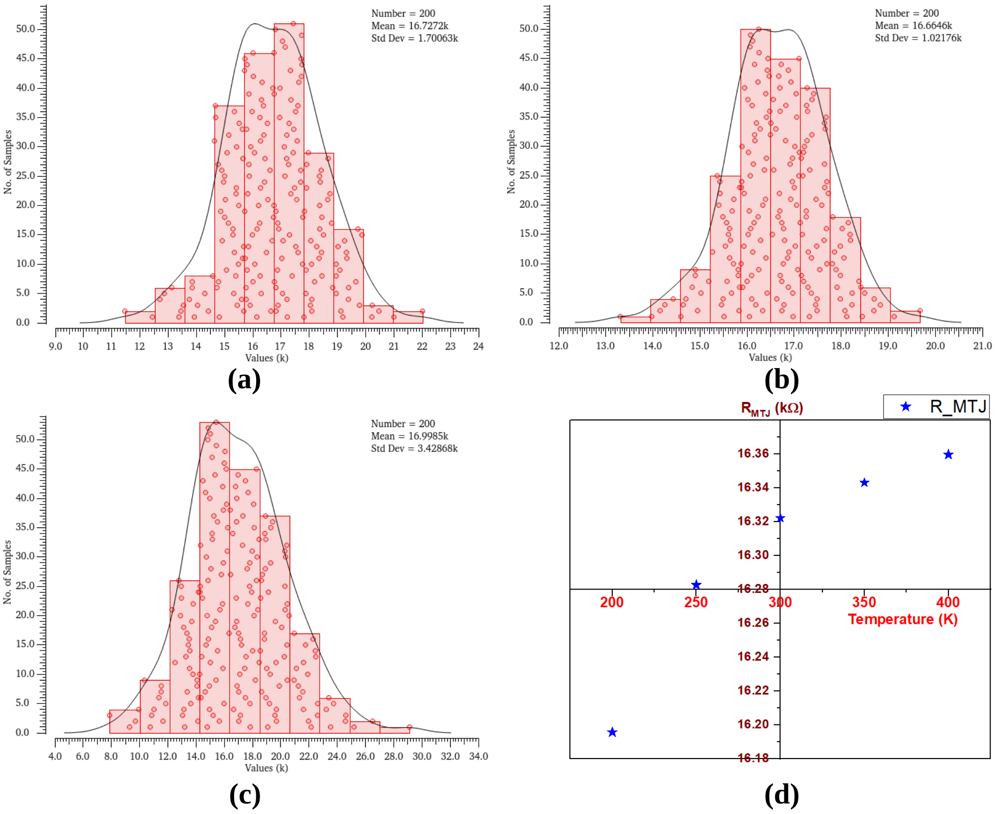


Figure 7. (**a**–**c**) Results of 200 Monte-Carlo simulations for variation in MTJ resistance in presence of different values of PV percentage. (**d**) MTJ resistance vs. temperature sweep.

Table 2. Results of 200 Monte-Carlo simulations for average MTJ resistance value under various PV.

PV (TMR, T_{FL}, T_{OX})	Min Value	Max Value	Mean Value	Std. Dev	Pass Ratio
3%	13.31 kΩ	19.69 kΩ	16.66 kΩ	1.022 kΩ	97.50%
5%	11.47 kΩ	22.04 kΩ	16.73 kΩ	1.701 kΩ	89%
10%	7.878 kΩ	29.16 kΩ	17.00 kΩ	3.429 kΩ	58%

As discussed in Section 4.1, the free layer magnetization dynamics are a temperature function. The MTJ device should have a sufficient energy barrier so that the fluctuation in temperature does not cause a state change. Although externally initiated signals like magnetic field and temperature fluctuation can be utilized as a possible triggering mechanism during the IC testing process, the MTJ-based Trojan has a higher probability of getting detected for a temperature-based test. Therefore, in this work, we have only used a magnetic field as the external trigger and kept the barrier height sufficient to suppress the effect of temperature variation in the range of T = 200 to 400 K. Figure 7d shows the variation in MTJ resistance of Trojan block as a function of temperature. The effect of temperature variation is also considered for CMOS transistors present in the circuit to include a more realistic analysis. For the selected temperature range, $\Delta R_{MTJ} \approx 160\ \Omega$, which did not lead to any incorrect logic operation of Trojan block. This signified that the Trojan block has a good stability factor, and the temperature sweep is a critical performance measure for MTJ-based hardware Trojan.

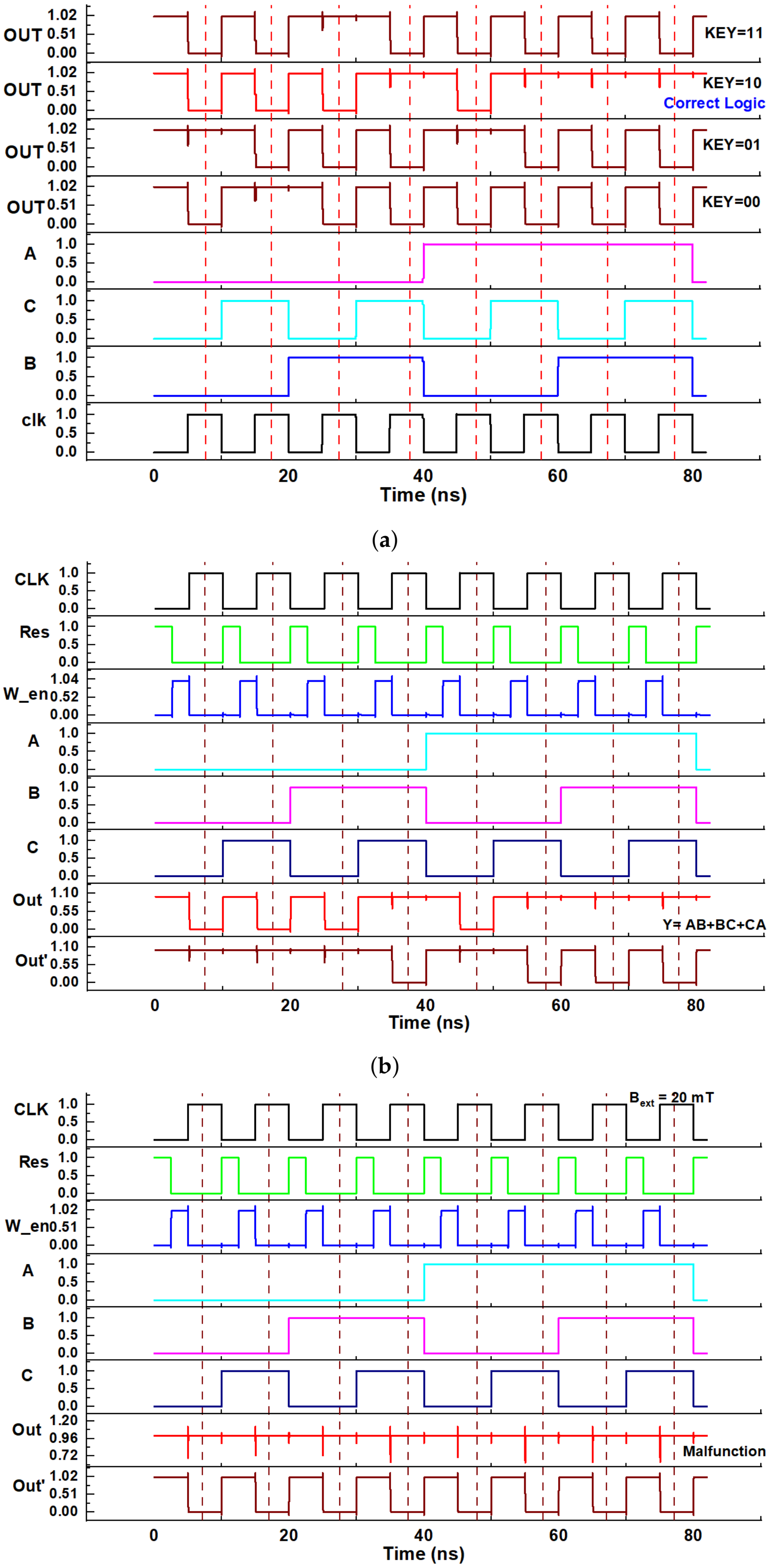
4.3. Hardware Trojan Inserted in Logic-Locking Circuit

Logic locking is one of the most viable options to ensure hardware security for a wide range of threats. Intelligent logic-locking mechanisms are being developed to effectively lock the netlist and counter multiple threats effectively [36,37]. In this method, the designer locks the netlist before sending it to an untrusted foundry and untrusted user. The untrusted entities in the SoC design flow mentioned in Figure 1c do not have easy access to the keys and the logic-locking mechanism, so they can not easily unlock the chip. Our Trojan design focuses on targeting the activated chip after the user has fed in the correct key value and remains hidden and undetected until that, as shown in Figure 2c. Figure 4 shows the hardware Trojan insertion approach. It is important to note that the logic-locking mechanism has also been proposed as a hardware metering technique [37] to keep track of the IC post-fabrication. It is a very effective way to prevent the Trojan from delivering its payload, but this method is not used to detect the Trojan. Our work targets only the activated chip, and the foundry inserting Trojan is assumed to have no idea about the logic locking done by the IP owner. However, it is possible that a functional IC with an activated Trojan may not launch its payload due to the possibility of having another part of the IC still inactivated. Thus, logic locking as a hardware metering technique is definitely a very effective Trojan effects prevention technique. Since IP owners also have no idea about the number/type/triggering/payload/location of the hidden Trojan inserted, therefore, according to our understanding, the only solution to this is to increase the number of Trojans and target different nets. However, increasing the Trojans will increase the detection probability. So, a very balanced and sophisticated approach needs to be taken to ensure 100% success. In this section, we demonstrate the idea of utilizing MTJ-based hardware Trojan in a logically locked netlist. There are two modes of operation for hardware Trojan in the logic-locking circuit. In the first mode, the Trojan needs to remain hidden until the system is unlocked by the user (insertion of correct keys) and should not disturb the correct logic even upon insertion of the keys and should pass all the IC verification and probe analysis. In the second mode of operation, the hardware Trojan needs to be triggered and needs to deliver the payload. The second mode needs to be activated only when the IC is activated. We have selected a simple logic-locking circuit as shown in Figure 4, where the correct logic at the output is the Boolean function Y = AB + BC + CA and the correct key value is $k_1 - k_2 = 10$. The key is designed in two-layer security where k_{IC1} and K_{IC2} is stored in a tamper-proof STT-MRAM and requires input from user K_{1U1} and K_{1U2} to generate key-value $k_1 - k_2$. The IC will not be unlocked for any other incorrect key combination, as shown in Figure 8a. Figure 8b shows the MTJ-based hardware Trojan operation in the first mode of operation in the activated IC as described earlier. The dotted line demonstrates the reading phase during the positive level of the clock signal. The read path is shown in Figure 3a, and the read current needs to be properly optimized so that the state of MTJ will not get disturbed.

In Figure 8c, after the IC is activated, we apply $B_{ext} > B_{ext,critical} = 20$ mT and the output logic is malfunctioned, and the circuit no longer performs the desired operation. For $B_{ext} < B_{ext,critical}$, the circuit operates normally as desired. We performed Monte-Carlo simulations as done in Section 4.2 to calculate the effect of PV in the circuit of Figure 4d, and the result for the same is mentioned in Table 3.

4.4. Hardware Trojan Detection

In Figure 1b, the taxonomy of Trojan detection is shown. They can be done at the design stage (pre-silicon) to validate SoC design or verify the fabricated SoCs (post-silicon). As the Trojan is inserted at the fabrication stage, it can bypass all the pre-silicon-based detection techniques, and inserting such emerging devices with CMOS at an earlier stage of the SoC design flow will have a higher probability of getting detected. The various post-silicon tests are discussed below [38].



(**a**)

(**b**)

(**c**)

Figure 8. (**a**) Logic-locking mechanism with different key values. (**b**) Hardware Trojan block waveforms in logic-locking circuit (hidden behavior). (**c**) Hardware Trojan block waveforms in logic-locking circuit with external triggering (malfunction behavior).

Table 3. Results of 200 Monte-Carlo simulations for average MTJ resistance value under various PVs.

PV (TMR, T_{FL}, T_{OX})	Min Value	Max Value	Mean Value	Std. Dev	Pass Ratio
3%	14.16 kΩ	19.42 kΩ	16.77 kΩ	1.027 kΩ	99%
5%	12.68 kΩ	21.49 kΩ	16.85 kΩ	1.719 kΩ	89.50%
10%	11.13 kΩ	27.62 kΩ	17.34 kΩ	3.662 kΩ	59%

4.4.1. Destructive Tests

The destructive method uses reverse engineering (RE) to obtain images of each layer. The RE-based technique is costly, time-consuming, and error-prone as the de-packaging could itself cause errors and can validate only a single chip at a time. Thus, RE is not a very viable strategy for Trojan detection.

4.4.2. Functional Tests

In this test, test vectors are applied to compare the responses with the correct response. However, the conventional manufacturing tests using functional or structural patterns poorly detect Trojans [39]. Sneaky Trojans can be designed to become active under low conditions and rarely activated nets. In complex SoC with vast logical states, it is highly impractical to utilize specially designed test patterns [40] to trigger rarely activated nets. If properly designed, Trojans that are externally triggered and placed on rarely activated nets can bypass functional tests.

4.4.3. Side Channel Analysis

In this approach, detection is carried out by measuring various circuit parameters. No matter how carefully designed, any malicious altercation will cause some side effects, such as path delay, heat, power, or electromagnetic radiation. Side-channel analysis is a powerful tool for detecting Trojans. Nevertheless, it is challenging to detect the proposed Trojan designed in this work for the following reasons: (1) Difficulty in achieving high coverage of every net. (2) Spintronics-based devices utilize low operational voltage, competitive cell area, and delay [23]; thus, minor deviations in such parameters under process and environmental variation are very hard to detect. In complex SoC with sneaky Trojans, the side channel effects can be masked due to such effects. (3) In Figure 7d, we performed MTJ resistance variation vs. temperature sweep for the entire Trojan block as mentioned in Section 4.2. For the 200 K to 400 K temperature sweep, the logic function is not altered for the selected MTJ parameters. However, with reduced dimension, the issue of state reversal due to thermal energy may cause the failure of the operation, which may be detected.

5. Conclusions

Emerging technologies for hardware security have enabled new security primitives and applications. With the advancement in the fabrication of such nano-devices, unique physical characteristic offers both new attack and defense possibilities. In this work, we designed a hardware Trojan block based on SOT-assisted STT PMA MTJ and utilized its sensitive response to an external magnetic field to create a logic malfunction. We designed the circuit to have a robust performance to device imperfection by analyzing the performance using Monte-Carlo simulation. The thermal stability factor is kept high to ensure non-triggering of temperature variation (T = 200–400 K) and lower detection probability during IC testing. The logic-locking mechanism is used to lock the netlist, and a carefully designed spintronics-based hardware Trojan is used to cause a malfunction in the logic-locked circuit. Currently, this design can cause malfunction for a short period until the external parameters are applied, and the hardware Trojan operation is subjected to tight design consideration. With proper design, they can have very low trigger probability, low operational power, delay, and EM radiation. Although design techniques for several other testing mechanisms like side-channel fingerprinting, X-ray-based reconstruction of the chip, and use of thermal cameras for infrared mapping of the IC, etc., were not included in this work. SCA leakage can be analyzed for further performance analysis [24], and the effect of external (adversary/evaluator) and internal (crosstalk) EM can be seen by doing EM simulation in future work. However, the possibility of utilizing such spintronic devices as a potential threat to IC design is increasing, which creates the need to develop a general hardware security mechanism for spintronics-based devices.

Author Contributions: Conceptualization, R.K. and D.D.; methodology, R.K. and D.D.; software, D.D.; validation, R.K., D.D., D.K., S.A. and Y.M.; formal analysis, R.K. and D.D. ; investigation, R.K., D.D., D.K. and S.A.; resources, S.A., D.K. and Y.M.; data curation, R.K. and D.D.; writing—original draft preparation, D.K. and S.A.; writing—review and editing, D.K. and S.A.; visualization, R.K. and D.D.; supervision, Y.M.; project administration, Y.M.; funding acquisition, Y.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Semiconductor Industry Association (SIA), Global Billings Report History (3-Month Moving Average) 1976-March 2009. 2008. Available online: http://www.sia-online.org/galleries/Statistics/GSR1976-March09.xls (accessed on 4 April 2022).
2. Guin, U.; Forte, D.; Tehranipoor, M. Anti-counterfeit techniques: From design to resign. In Proceedings of the 14th International Workshop on Microprocessor Test and Verification, Austin, TX, USA, 11–13 December 2013; pp. 89–94.
3. Guin, U. Establishment of Trust and Integrity in Modern Supply Chain from Design to Resign. Ph.D. Dissertation, University of Connecticut Electrical and Computer Engineering, Mansfield, CT, USA, 2016. Available online: https://opencommons.uconn.edu/dissertations/1063 (accessed on 4 April 2022).
4. Tehranipoor, M.M.; Guin, U.; Forte, D. Counterfeit integrated circuits. In *Counterfeit Integrated Circuits*; Springer: Cham, Switzerland, 2015; pp. 15–36.
5. IARPA Trusted Integrated Circuits (TIC) Program Announcement. Available online: https://www.iarpa.gov/index.php/research-programs/tic/baa (accessed on 15 February 2019).
6. Xiao, K. Techniques for Improving Security and Trustworthiness of Integrated Circuits. Ph.D. Dissertation, University of Connecticut Electrical and Computer Engineering, Mansfield, CT, USA, 2015. Available online: https://opencommons.uconn.edu/dissertations/947 (accessed on 2 April 2022).
7. Agrawal, D.; Baktir, S.; Karakoyunlu, D.; Rohatgi, P.; Sunar, B. Trojan detection using IC fingerprinting. In Proceedings of the Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007; pp. 296–310.
8. Karri, R.; Rajendran, J.; Rosenfeld, K.; Tehranipoor, M. Trustworthy hardware: Identifying and classifying hardware trojans. *IEEE Comput.* **2010**, *43*, 39–46. [CrossRef]
9. Tehranipoor, M.; Koushanfar, F. A survey of hardware Trojan taxonomy and detection. *IEEE Des. Test Comput.* **2010**, *27*, 10–25. [CrossRef]
10. Piliposyan, G.; Khursheed, S.; Rossi, D. Hardware Trojan Detection on a PCB Through Differential Power Monitoring. *IEEE Trans. Emerg. Top. Comput.* **2020**. [CrossRef]
11. Jinnai, B.; Igarashi, J.; Shinoda, T.; Watanabe, K.; Fukami, S.; Ohno, H. Fast Switching Down to 3.5 ns in Sub-5-nm Magnetic Tunnel Junctions Achieved by Engineering Relaxation Time. In Proceedings of the 2021 IEEE International Electron Devices Meeting, San Francisco, CA, USA, 12–15 December 2021; pp. 1–4.
12. Ghosh, S. Spintronics and security: Prospects, vulnerabilities, attack models, and preventions. *Proc. IEEE* **2016**, *104*, 1864–1893. [CrossRef]
13. Massoud, Y.; Nieuwoudt, A. Modeling and design challenges and solutions for carbon nanotube-based interconnect in future high performance integrated circuits. *ACM J. Emerg. Technol. Comput. Syst.* **2006**, *2*, 155–196. [CrossRef]
14. Nieuwoudt, A.; Massoud, Y. Predicting the Performance of Low-Loss On-Chip Inductors Realized Using Carbon Nanotube Bundles. *IEEE Trans. Electron Dev.* **2008**, *55*, 298–312. [CrossRef]
15. Massoud, Y.; Ismail, Y. Grasping the Impact of On-Chip Inductance in High Speed ICs. *IEEE Circuits Devices Mag.* **2001**, 17, 14–21. [CrossRef]
16. Eachempati, S.; Nieuwoudt, A.; Gayasen, A.; Narayanan, V.; Massoud, Y. Assessing Carbon Nanotube Bundle Interconnect for Future FPGA Architectures. In Proceedings of the IEEE Design Automation and Test in Europe, Nice, France, 16–20 April 2007.
17. Nieuwoudt, A.; Ragheb, T.; Nejati, H.; Massoud, Y. Increasing Manufacturing Yield for Wideband RF CMOS LNAs in the Presence of Process Variations. In Proceedings of the IEEE Symposium on Quality Electronic Design, Washington, DC, USA, 26–28 March 2007.

18. Nieuwoudt, A.; Mondal, M.; Massoud, Y. Predicting the Performance and Reliability of Carbon Nanotube Bundles for On-Chip Interconnect. In Proceedings of the IEEE ASP Design Automation Conference, Yokohama, Japan, 23–26 January 2007.
19. Nieuwoudt, A.; Massoud, Y. Accurate Resistance Modeling for Carbon Nanotube Bundles in VLSI Interconnect. In Proceedings of the IEEE Conference on Nanotechnology, Cincinnati, OH, USA, 17–20 July 2006.
20. Nieuwoudt, A.; Massoud, Y. Assessing the Implications of Process Variations on Future Carbon Nanotube Bundle Interconnect Solutions. In Proceedings of the IEEE Symposium on Quality Electronic Design, San Jose, CA, USA, 26–28 March 2007.
21. Nieuwoudt, A.; Massoud, Y. Performance Implications of Inductive Effects for Carbon Nanotube Bundle Interconnect. *IEEE Electron Devices Lett.* **2007**, *28*, 305–307 [CrossRef]
22. Ragheb, T.; Massoud, Y. On the modeling of resistance in Graphene Nanoribbon (GNR) for future interconnect applications. In Proceedings of the 2008 International Conference on Computer-Aided Design (ICCAD'08), San Jose, CA, USA, 10–13 November 2008; pp. 10–13.
23. Barla, P.; Joshi, V.K.; Bhat, S. Design and analysis of SHE-assisted STT MTJ/CMOS logic gates. *J. Comput. Electron.* **2021**, *20*, 1964–1976. [CrossRef]
24. Levi, I.; Bellizia, D.; Standaert, F.-X. Reducing a Masked Implementation's Effective Security Order with Setup Manipulations and an Explanation Based on Externally-Amplified Couplings. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2*, 293–317. [CrossRef]
25. Wang, Z.; Zhao, W.; Deng, E.; Klein, J.; Chappert, C. Perpendicular-anisotropy magnetic tunnel junction switched by spin-Hall-assisted spin-transfer torque. *J. Phys. D Appl. Phys.* **2015**, *48*, 065001. [CrossRef]
26. Roohi, A.; Zand, R.; Demara, R. Logic-Encrypted Synthesis for Energy-Harvesting-Powered Spintronic-Embedded Datapath Design. In Proceedings of the GLSVLSI '18: Proceedings of the 2018 on Great Lakes Symposium on VLSI, Chicago, IL, USA, 23–25 May 2018.
27. Zhang, J.; Guo, Z.; Zhang, S.; Cao, Z.; Li, R.; Cao, J.; Song, M.; Wan, M.; Hong, J.; You, L. Spin-orbit torque-based reconfigurable physically unclonable functions. *Appl. Phys. Lett.* **2020**, *116*, 192406. [CrossRef]
28. Choi, W.; Lv, Y.; Kim, J.; Deshpande, A.; Kang, G.; Wang, J.; Kim, C. A Magnetic Tunnel Junction based True Random Number Generator with conditional perturb and real-time output probability tracking. In Proceedings of the IEEE International Electron Devices Meeting, San Francisco, CA, USA, 15–17 December 2014.
29. Chakraborty, R. S.; Narasimhan, S.; Bhunia, S. Hardware Trojan: Threats and emerging solutions. In Proceedings of the 2009 IEEE International High Level Design Validation and Test Workshop, San Francisco, CA, USA, 4–6 November 2009; pp. 166–171.
30. Knechtel, J. Hardware Security for and beyond CMOS technology. In Proceedings of the ISPD '21: 2021 International Symposium on Physical Design, Portland, OR, USA, 19–22 March 2021; pp. 115–126.
31. Wang, M.; Cai, W.; Zhu, D.; Wang, Z.; Kan, J.; Zhao, Z.; Cao, K.; Wang, Z.; Zhang, Y.; Zhang, T.; et al. Field-free switching of perpendicular magnetic tunnel junction by the interplay of spin-orbit and spin-transfer torques. *Nat. Electron.* **2018**, *1*, 585–588 [CrossRef]
32. Chakraborty, A.; Jayasankaran, N.G.; Liu, Y.; Rajendran, J.; Sinanoglu, O.; Srivastava, A.; Xie, Y.; Yasin, M.; Zuzak, M. Keynote: A Disquisition on Logic Locking. *IEEE Trans.-Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 1952–1972. [CrossRef]
33. Roy, A.J.; Koushanfar, F.; Markov, L.I. EPIC: Ending Piracy of Integrated Circuits. In Proceedings of the 2008 Design, Automation and Test in Europe, Munich, Germany, 10–14 March 2008; pp. 1069–1074.
34. Kitagawa, E.; Fujita, S.; Nomura, K.; Noguchi, H.; Abe, K.; Ikegami, K.; Daibou, T.; Kato, Y.; Kamata, C.; Kashiwada, S.; et al. Impact of ultra low power and fast write operation of advanced perpendicular MTJ on power reduction for high-performance mobile CPU. In Proceedings of the 2012 International Electron Devices Meeting, San Francisco, CA, USA, 10–13 December 2012; pp. 29.4.1–29.4.4.
35. Hébrard, L.; Nguyen, D.V.; Vogel, D.; Schell, J.B.; Po, C.; Dumas, N.; Pascal, J. On the influence of strong magnetic field on MOS transistors. In Proceedings of the 2016 IEEE International Conference on Electronics, Circuits and Systems (ICECS), Monte Carlo, Monaco, 11–14 December 2016; pp. 564–567.
36. Yue, M.; Tehranipoor, S. A Novel Probability-Based Logic-Locking Technique: ProbLock. *Sensors* **2021**, *21*, 8126. [CrossRef] [PubMed]
37. Kamali, H.M.; Azar, K.Z.; Farahmandi, F.; Tehranipoor, M. Advances in Logic Locking: Past, Present, and Prospects. *Cryptol. Eprint Arch.* **2022**. Available online: https://eprint.iacr.org/2022/260.pdf (accessed on 2 April 2022).
38. Bhunia, S.; Tehranipoor, M. *Hardware Security: A Hands-on Learning Approach*; Morgan Kaufmann: Burlington, VT, USA, 2018; pp. 109–140.
39. Bhunia, S.; Hsiao, M.S.; Banga, M.; Narasimhan, S. Hardware Trojan attacks: Threat analysis and countermeasures. *Proc. IEEE* **2014**, *102*, 1229–1247. [CrossRef]
40. Waksman, A.; Suozzo, M.; Sethumadhavan, S. FANCI: Identification of stealthy malicious logic using boolean functional analysis. In Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, Berlin, Germany, 4–8 November 2013; pp. 697–708.