LOCK&ROLL: Deep-Learning Power Side-Channel Attack Mitigation using Emerging Reconfigurable Devices and Logic Locking

Gaurav Kolhe, Tyler Sheaves, Kevin Immanuel Gubbi, Soheil Salehi, Setareh Rafatirad,
Sai Manoj PD*, Avesta Sasan, and Houman Homayoun
Dept. of Electrical and Computer Engineering, University of California, Davis, CA, USA
*Dept. of Electrical and Computer Engineering, George Mason University, Fairfax, VA, USA
{gskolhe,tsheaves,kgubbi,ssalehi,srafatirad,asasan,hhomayoun}@ucdavis.edu;*spudukot@gmu.edu

ABSTRACT

The security and trustworthiness of ICs are exacerbated by the modern globalized semiconductor business model. This model involves many steps performed at multiple locations by different providers and integrates various **Intellectual Properties** (IPs) from several vendors for faster time-to-market and cheaper fabrication costs. Many existing works have focused on mitigating the well-known SAT attack and its derivatives. **Power Side-Channel Attacks** (P-SCAs) can retrieve the sensitive contents of the IP and can be leveraged to find the key to unlock the obfuscated circuit without simulating powerful SAT attacks. To mitigate P-SCA and SAT-attack together, we propose a multi-layer defense mechanism called **LOCK&ROLL**: Deep-Learning Power Side-Channel Attack Mitigation using Emerging Reconfigurable Devices and Logic Locking. LOCK&ROLL utilizes our proposed **Magnetic Random-Access Memory** (MRAM)-based Look Up Table called **Symmetrical MRAM-LUT** (SyM-LUT). Our simulation results using 45nm technology demonstrate that the SyM-LUT incurs a small overhead compared to traditional **Static Random Access Memory LUT** (SRAM-LUT). Additionally, SyM-LUT has a standby energy consumption of 20aJ while consuming 33fJ and 4.6fJ for write and read operations, respectively. LOCK&ROLL is resilient against various attacks such as SAT-attacks, removal attack, scan and shift attacks, and P-SCA.

CCS CONCEPTS

• **Security and privacy → Side-channel analysis and countermeasures**; **Hardware attacks and countermeasures**.

KEYWORDS

Reverse Engineering, Logic Locking, Emerging Devices, Side channel attack

ACM Reference Format:
Gaurav Kolhe, Tyler Sheaves, Kevin Immanuel Gubbi, Soheil Salehi, Setareh Rafatirad,, Sai Manoj PD*, Avesta Sasan, and Houman Homayoun. 2022. LOCK&ROLL: Deep-Learning Power Side-Channel Attack Mitigation using Emerging Reconfigurable Devices and Logic Locking. In *Proceedings of the 59th ACM/IEEE Design Automation Conference (DAC) (DAC '22), July 10–14, 2022, San Francisco, CA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3489517.3530414

DAC '22, July 10–14, 2022, San Francisco, CA, USA

ACM ISBN 978-1-4503-9142-9/22/07.
https://doi.org/10.1145/3489517.3530414

1 INTRODUCTION

Segregated manufacturing of the hardware with a globalized supply chain, increasing numbers of **Internet of Things** (IoT) and medical devices, and cyber-physical systems that leverage third-party **Intellectual Property** (IP) cores have given rise to concern over the security of the hardware. The contemporary threat model for security assumes hardware to be secure, and the software counterpart governs the security aspect of the final product. However, the globalization of manufacturing and integration of third-party IP for faster time-to-market with cheaper cost have compromised the hardware. Thus, the system has become increasingly vulnerable even in the presence of security offered by the software. Apart from the security, the globalized fabrication also exposes the hardware to various threats such as IP piracy, overproduction, and counterfeiting, to name a few. These implications of globalized fabrication affects individual users as well as companies.

Over the past few years, various hardware **design-for-trust** (DFT) mechanisms such as watermarking, IC metering, IC camouflaging, split manufacturing, and logic locking were proposed to re-imagine the trust in the silicon. However, recently introduced attack vectors have exploited vulnerabilities in the techniques mentioned above. **Boolean Satisfiability** (SAT) attack is one of the powerful techniques that can exploit the vulnerabilities in many logic locking and camouflaging schemes [11]. Anti-SAT, SAR-Lock, and **Stripped Functionality Logic Locking** (SFLL) [18] are state-of-the-art methods requiring exponential SAT iterations to find the correct key. However, the work in [2, 3, 17] exploit the vulnerability in the implementation of SAT-resilient techniques and shows that the obfuscation key can be found within several minutes. Moreover, SFLL, SAR-Lock, and Anti-SAT obfuscation primitives fall into a category of one-point function [17] which evaluates the correct output upon applying a specific input pattern. Though it requires SAT-attack to apply many inputs to find the correct key, the output corruptibility offered by such techniques is very low, which means that the circuit works almost identical to the oracle circuit even when the wrong key is used [16]. To address the concern of reduced output corruptibility, CASLock [16] provides both increased corruptibility while guaranteeing the SAT-resiliency. However, the work in [4] has successfully defeated the proposed primitive.

Reconfigurable obfuscation such as **Look-Up Table** (LUT)-based obfuscation aims to thwart SAT-attack by exposing the SAT-solver to a vast key search space [8–10]. However, it can incur hefty overheads. Another primitive from the reconfigurable domain uses a **Magneto-Electric Spin-Orbit** (MESO) device for obfuscation [14], which can offer both reconfigurability and dynamic morphing to thwart the SAT-attack. Since most of the works try to mitigate SAT attacks by increasing the time required to find a solution, it is possible that with the increasing computing power and new research directions, it would be possible to break SAT-resilient techniques with new SAT-solvers. Therefore, we explore the ability to eliminate SAT-attack

by morphing in runtime as it is an excellent option for obfuscation. While the community has targeted much of its efforts to mitigate the SAT-attack, the threat model assumes that the keys are stored in a tamper-proof memory. The adversaries can observe the side-channel profile, such as power footprint, to decipher the key stored in the tamper-proof memory. Moreover, a recent study shows the potential of using **Machine Learning** (ML) to understand the underlying behavior of the hardware by monitoring side-channel information such as power consumption in particular [1]. Using P-SCAs with ML techniques can reveal the secret key. Therefore, there is a need for a technique that can eliminate the SAT-attack and the ML-assisted P-SCAs. Thus, we propose a Deep-Learning Power Side-Channel Attack Mitigation using Emerging Reconfigurable Devices and Logic Locking (**LOCK&ROLL**). The contributions of this work are:

- We propose Symmetrical MRAM-based LUT (SyM-LUT) to successfully resists the ML-assisted P-SCA by attaining near-zero power variation in the output.
- We show that LUT-based obfuscation offers SAT-resiliency and we use **Spin Transfer Torque** (STT) **Magnetic Tunnel Junction** (MTJ) to design a reliable and low-overhead LUT with wide read margin for LUT-based obfuscation.
- We complement SyM-LUT with **Scan Enable Obfuscation Mechanism** (SOM) to eliminate the SAT-attack and empirically evaluate our proposed primitive against ML-assisted P-SCA and demonstrate its wide security coverage.
- Finally, we discuss the resiliency offered by the proposed primitive against various attacks to demonstrate the broad applicability and resiliency of the LOCK&ROLL.

2 BACKGROUND AND MOTIVATION

We discuss the existing work and security vulnerabilities in the area of hardware security in this Section.

2.1 Reconfigurable Obfuscation

Among various reconfigurable obfuscation techniques, LUT-based obfuscation has been the prime focus due to its ability to realize many logic elements with non-recurring engineering costs. The initial results of using LUT of size 2 for obfuscation have not been successful due to the invention of the SAT-attack, and thus the community has changed the research aspect of reconfigurable domains to use dynamic morphing for resisting SAT-attack. The Magneto-Electric Spin-Orbit (MESO) [14] and Giant Spin Hall Effect (GSHE) [12] provide the ability to morph during the runtime dynamically. However, the dynamic morphing of these devices is governed by a **True Random Number Generator** (TRNG). Dynamically morphing from one state to other during runtime resists the transformation of the circuit to the SAT-attack formulation, thereby eliminating the threat of SAT-attack. However, randomly morphing from one state to another limits the applicability of the obfuscation to the only applications that tolerate some level of error [14]. Moreover, this defeats the purpose of obfuscation, as the attacker can deliberately fix the functionality of the MESO devices, and the IP may still function correctly as the application can tolerate some level of error. If the TRNG blocks are replaced with more sophisticated logic blocks, the attacker can focus on reverse-engineering the block that governs the functionality of the polymorphic devices. Finally, if the MESO devices are used in a static manner to thwart SAT-attack in the IPs that do not tolerate any errors due to dynamic morphing offered by the gates, the MESO devices can be replaced with static LUT of size 2, which also represent 16 different logical functions. However, the work in [9] shows that when the LUT of size 2 is leveraged, the circuit can be readily de-obfuscated. These challenges in the reconfigurable logic obfuscation domain call for a solution that can resist SAT-attack while being resilient to P-SCA.

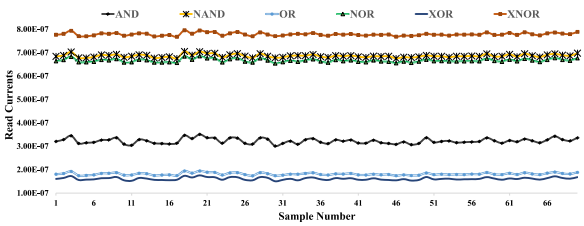


Figure 1: Read current traces of a 2-input MRAM-LUT in [15]. (Y-axis: Read Current in Amps; X-axis samples in collected data)

To resist the SAT-attack, the work in [9] proposes the customized LUT block, which creates the SAT-hard instance even when the LUTs are configured as a static device. Therefore, we use the LUT-based obfuscation as a foundation for building our primitive. The main challenge of using the SRAM-based LUTs is their significant overheads, and they also tend to have high static power with low density. Moreover, SRAM-based LUTs exhibit a power side-channel signature which enables the threat of side-channel attacks. The work in [9] tries to mitigate the limitations of the SRAM-based LUT by using the non-volatile spin-based LUTs. Additionally, spin-based devices offer incredible features such as non-volatility, near-zero static power, high endurance, high integration density, and compatibility with the CMOS fabrication process [9]. However, the majority of the spin-based LUTs proposed in the literature fail to maintain a wide sense margin and suffer from a high error rate, especially in the presence of Process Variation (PV) [15]. While the proposed primitive can thwart the SAT-attack as it renders in SAT-hard instances, it cannot eliminate the threat of SAT-attack. Most of the results in the obfuscation community-run SAT-attack for several days to prove the SAT-resiliency [5, 9, 18], however, implications of running SAT-attack for a month or beyond is never studied. Access to the powerful computing cluster can enable running the SAT-solver for an extended time, enabling the attacker to retrieve keys. Finally, the threat model in logic locking assumes that the key for unlocking the obfuscated circuit is stored in the tamper-proof memory. In the case of LUT-based obfuscation, the MTJs are considered as a tamper-proof memory because contents of the MTJs will be lost in an invasive reverse-engineering attempt. However, the impact of the P-SCA has been missing.

2.2 Power Side-Channel Attacks (P-SCAs)

In the CMOS circuit, to change the state of the logic device, i.e., from zero to one or vice versa, the current is applied. This transition from one state to another reflects a side-channel signature, which can be captured through power consumption of the system or other electrical properties. Since the amount of power required in the system is proportional to the manipulated data, the power traces collected during the processing or transition of states contain vital information. Even a single transistor's effect can appear as a weak correlation in power measurements [7]. We measured the current of 2-input LUT for different functions by the method of simulation in HSPICE. Figure 1 shows how an MRAM-LUT implemented based on the circuit proposed in [15] draws different currents when implementing different functions. Without a need for advanced algorithms, different states that LUTs are configured in can be visually distinguished. By comparing the current drawn from the LUT under test with standard measurements, the functionality of the LUT can be readily inferred. This experiment shows how the obfuscation key can be accessed without the need to execute the SAT-attack.

In the proposed methodology, we use the MRAM-LUT for the obfuscation. It consists of a select tree that selects a MTJ for reading. The value stored in the MTJ is sensed and observed at the output of the LUT. MTJs store the logical value '0' and '1' using two states, i.e., parallel state and anti-parallel state. The MTJ exhibits low-resistance in the parallel state while the anti-parallel state exhibits a high-resistance. When we select different MTJs for reading, the current value will fluctuate based on the state of MTJs. This change in current can be captured using P-SCA and can help the attacker retrieve the rich content of LUT, thereby defeating the purpose of obfuscation. In the following section, we first propose a variant of LUT-based obfuscation, which is resilient to SAT attacks while having a wide read margin in the presence of **Process Variation** (PV). We further discuss how the power footprint can be obfuscated using complementary storage and evaluate the security coverage of our proposed LUT design against P-SCAs.

3 PROPOSED LOGIC LOCKING SCHEME

3.1 Symmetrical MRAM-LUT (SyM-LUT)

Generally, M-input LUTs have 2^M memory cells to implement M-input Boolean functions. A select tree MUX circuit is utilized to select the memory cell that holds the correct value of the function the LUT is implementing. Herein, we propose **Symmetrical MRAM-LUT** (SyM-LUT) design. Our proposed SyM-LUT provides a reliable and energy-efficient operation due to a wide read margin using complementary MTJ memory cells, as elaborated in this Section. Figure 2 depicts a 2-input example of SyM-LUT design. As shown in Figure 2, SyM-LUT contains two select tree MUXes which use **Pass Transistors** (PTs) and **Transmission Gates** (TGs). The proposed SyM-LUT can be reconfigured using **WE** and $\overline{\textbf{WE}}$ signals to perform a write operation. When **WE** and $\overline{\textbf{WE}}$ are asserted, each memory cell can be connected separately to the **BL** and $\overline{\textbf{BL}}$ by using the inputs **A** and **B**. By setting **BL** and $\overline{\textbf{BL}}$, we can change the content of the memory cells. Additionally, in each write operation, we change the content of each memory cell in a complementary fashion. As a result, $\textbf{MTJ}_i$ and $\overline{\textbf{MTJ}_i}$ always hold opposite values. In particular, assuming the data stored in the $\textbf{MTJ}_1$ is in the P or low-resistance state, then $\overline{\textbf{MTJ}_1}$ is going to be in the AP or high-resistance state and vice versa. Thus, we can use each cell's complementary value to reliably read the stored data.

As depicted in Figure 5, in SyM-LUT, after termination of the write operation, **PC** signal is asserted to pre-charge the intermediary output nodes **OUT** and $\overline{\textbf{OUT}}$ and then by disabling **PC** signal and asserting the **RE** and $\overline{\textbf{RE}}$ signals, we enable the discharge path and read the data stored in the MTJs. Read enable signals **RE** and $\overline{\textbf{RE}}$ enable the read path from **OUT** and $\overline{\textbf{OUT}}$ to **GND**. This will result in a race condition between two branches of sense amplifier, which will be used the observe the resistance difference between the $\textbf{MTJ}_i$ and $\overline{\textbf{MTJ}_i}$. The select tree MUXes are used to direct the proper output according to the input signals **A** and **B**. This value of the LUT function is observed at the output nodes **OUT** and $\overline{\textbf{OUT}}$.

The proposed SyM-LUT is designed to increase the security of the design via dynamic obfuscation and P-SCA mitigation. This hypothesis is based on the fact that the output of a LUT is a function of all of the inputs, and the proposed MRAM-based LUT maintains a nearly symmetrical power consumption footprint and delays to provide an output of '0' or '1', and as a result, it maintains a near-zero power variation in the output. Furthermore, the MTJ devices' contents can be reconfigured in every LUT to change the functionality that each LUT is implementing. To define the functionality of each 2-input SyM-LUT, a set of keys are shifted in via the Bit line **BL** signal, and

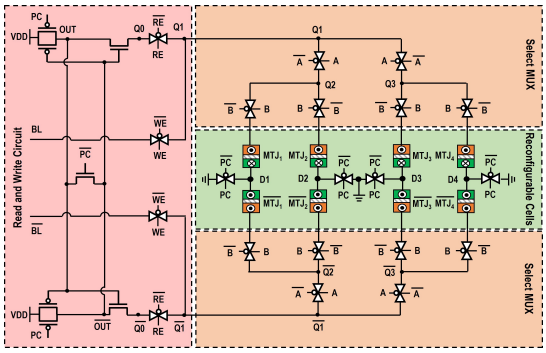


Figure 2: The circuit-level diagram of the proposed 2-input SyM-LUT using STT-MTJ devices.

Table 1: Parameters of 2-terminal STT-MTJ device.

Parameters	Description	Value
MTJ_{Area}	$l_{MTJ} \times w_{MTJ} \times \pi/4$	$15nm \times 15nm \times \pi/4$
t_f	Free Layer thickness	1.3 nm
RA	MTJ resistance-area product	$9\ \Omega \cdot \mu m^2$
T	Temperature	358 K
α	Damping coefficient	0.007
P	Polarization	0.52
V_0	Fitting parameter	0.65
α_{sp}	Material-dependent constant	2e-5

by controlling **A** and **B** inputs, we can control which memory cell we wish to change or update the contents of. For example, for the AND function, **A** and **B** inputs are used to select each memory cell in the order of AB such as 11, 10, 01, and 00 while the keys to configure the functionality of the LUT are shifted through the **BL** as 1, 0, 0, and 0, respectively.

We use the HSPICE circuit simulator to validate the functionality of the proposed SyM-LUT using 45nm CMOS technology and the STT-MRAM model developed in [6]. MTJs are constructed of two ferromagnetic layers, called free layer and fixed layer, and a thin oxide layer [15]. In the STT switching approach used in **Spin Transfer Torque Magnetic Random Access Memory** (STT-MRAM), applying a bidirectional charge current through the terminals of the MTJ using a MOS-based circuit will result in the generation of a spin current that changes the magnetic polarity of the free layer to represent: 1) high resistance or **Anti-Parallel** (AP) state, and 2) low resistance or **parallel** (P) state. The states of the MTJ are determined according to the angle, θ, between the magnetization orientation of the ferromagnetic layers. Herein, we have adopted the MTJ device parameters from [15]. Table 1 lists the experimental parameters used herein to model the MTJ devices. Figure 3 shows the transient response of the proposed SyM-LUT. Figure 3 depicts an implementation of a 2-input XOR gate utilizing SyM-LUT. As shown, the HSPICE simulations verify the correct functionality of our proposed SyM-LUT.

Furthermore, we perform **Monte Carlo** (MC) simulation to analyze the reliability of reading and write operations of SyM-LUT in the presence of PV. The simulation helps in covering a wide range of PV scenarios that may occur in the fabricated device. The MC simulation is performed with 10,000 instances considering the effects of PV on the CMOS peripheral circuit and the MTJs. In particular, the variation of 1% for the MTJ's dimensions along with 10% variation on the threshold voltage and 1% variation on transistors dimensions are assessed [15]. According to the MC simulation results, SyM-LUT provides reliable write performance resulting in less than 0.0001% write errors in 10,000 error-free MC instances. Additionally, since the states of the MTJs are complementary, they provide a wide read

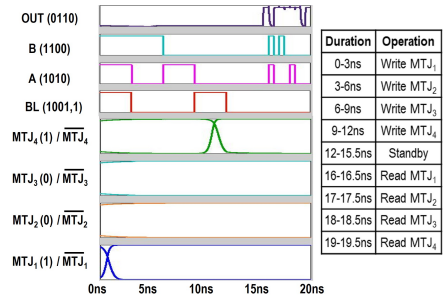


Figure 3: Simulation waveform for implementation of a 2-input XOR gate using SyM-LUT.

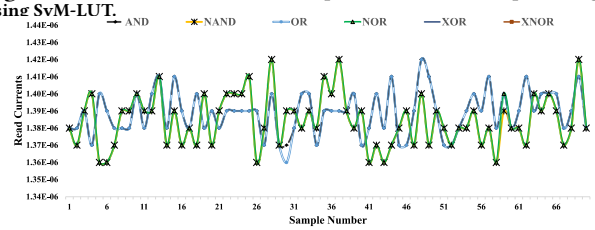


Figure 4: Read current trace samples of 2-input SyM-LUT implementing various functions using Monte Carlo instances.

margin, and as a result, there are less than 0.0001% read errors caused by PV based on the 10,000 error-free MC simulation results for all the different gates that implemented using SyM-LUT.

3.2 SyM-LUT's Resiliency against P-SCA

The side-channel analysis focuses on the variation in the electrical characteristics of the circuit to gain access to the confidential information in the circuit. The power traces target the read current of the LUT under test. By varying the input of the LUT, the select tree selects various MTJs for sensing their content. The various state of the MTJs results in different currents. The MC simulation data from HSPICE provides the values of the MTJ read current in the presence of PV. In our threat vector assumes that the attacker can use an invasive approach to probe the current.

If the SyM-LUT is representing 'XOR' gate, as shown in Figure 3, we can get 4 different read current measurements for reading four different states of the SyM-LUT (i.e., read current measurement when (1)A=0, B=0; (2)A=0, B=1; (3)A=1, B=0; (4)A=1, B=1). Among 4 different states, the current measurement for MTJ with content '0' and current measurement for MTJ with content '1' should show a difference for the P-SCA to succeed in learning the content of the MTJs. Using MC simulation with 10,000 instances for each logic gate implemented, we gather power trace and current values for all MTJs. Figure 4, demonstrates the read currents of the MTJs from the MC simulation. The same trend is observed over rest of the simulation generated for evaluation of the proposed LOCK&ROLL approach. As shown in Figure 4, the contents of the MTJs cannot be easily distinguished, which is not the case in traditional implementation of the LUT. Therefore, to empirically assess the security of our proposed primitive, we employ ML-assisted techniques to reverse-engineer the contents of the MTJs. We employ a classification model using Random Forest, Multi-class Logistic Regression, and **Support Vector Machine** (SVM). For this experiment, we gather the 4 traces of power for reading different states for 16 logic functions implemented by LUT size 2. The LUT of size 2 has two inputs and the features used for ML are Read Power when the two inputs are (1)A=0, B=0; (2)A=0, B=1; (3)A=1, B=0; (4)A=1, B=1.

For Multi-Class Logistic Regression we used polynomial features of degree 4 for fitting along with lasso regularization for avoiding overfitting on the data. Moreover, in Logistic Regression we used the Multi-Class Cross-Entropy Loss function. The number of classes are 16 for LUT of size 2. In Random Forest, for the quality of the split we used the **entropy** as the criterion. In case of the SVM we used **Radial Basis Function** (RBF) for the kernel function. For the empirical evaluation of the SyM-LUT, We have generated a total of 640,000 different samples using MC simulation for 16 class labels and used 10-fold cross-validation techniques along with accuracy and F-1 score as a metric to evaluate the performance of the ML algorithm. For data pre-processing, we performed feature scaling as well as outlier filtering using z-scores. Table 2 shows the resiliency of the proposed primitive to thwart P-SCAs.

Table 2: Performance of ML-assisted P-SCAs on SyM-LUT

Algorithm	Accuracy	F1-Score
Random Forest	31.55%	0.319
Logistic Regression	30.75%	0.304
SVM	28.09%	0.302
DNN	34.9%	0.343

We evaluated the proposed mechanism against P-SCAs that are assisted using the ML techniques. We use a **Deep Neural Network** (DNN) to classify the functionality implemented by the LUT using the power traces. The work in [13] has shown that DNN can bypass misalignment countermeasures in the ML-assisted P-SCAs. The input to the DNN is the scaled power trace vector with value ranging from 0 to 1 for better convergence. The output layer of the architecture uses a softmax activation with a categorical cross-entropy as a loss function. The softmax activation provides a probability distribution over all possible functions implemented by the LUT. We use the fully-connected layers with the Relu activation function and Adam optimizer for training the model. The 640,000 data traces are used for training and the model is evaluated using 10-fold cross-validation. The accuracy of the DNN model was ~35%.

We trained and tested ML models on the read currents of the traditional LUT-based architectures. It is evident that all models have more than 90% classification accuracy on traditional LUT-based architectures. However, as soon as we use the same ML model and train or test it on read currents from SyM-LUT architecture, it fails to classify or learn the functionality implemented by the LUT. Thus, the inability of the models to distinguish between the states of MTJs proves the ability of the SyM-LUT to mitigate the P-SCA. Moreover, the attacker will need to obtain a training set initially, which can be a challenge in itself. A symmetrical circuit design implementing two identical select tree MUXes that minimize power consumption through circuit optimization and complimentary MTJs results in a robust security primitive. Thus, our results prove our initial hypothesis that SyM-LUT maintains a near-zero power variation in the output and thus is resilient to P-SCAs.

3.3 Building SAT-hard instances using SyM-LUT

Following the discussion in the previous section, reconfigurable obfuscations such as MESO [14] or GHSE [12] fails to provide SAT-resiliency for applications that does not tolerate a certain degree of errors [14]. Moreover, obfuscations such as SFLL, AntiSAT, CAS-Lock [16, 18] have been shown to be vulnerable to the evolving attacks; thus, we use the LUT-based obfuscation as a base obfuscation method for proposing LOCK&ROLL. LUTs truly obfuscates the design by replacing it with a black-box structure. We refer to the latest work in the area of LUT-based obfuscation [9]. Our study reveals that the proposed LUT-based obfuscation in [9] provides more security with low overhead and makes LUT-based obfuscation a great candidate for obfuscation. However, the LUTs used in the [9] are large and would not suit small-scale IPs, and the LUTs are not resilient to power side-channel attacks. Therefore, we replace the LUTs used in the work [9] with the SyM-LUT proposed in our

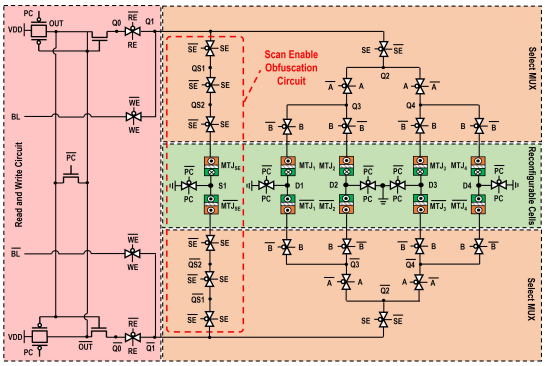


Figure 5: The circuit-level diagram of the proposed 2-input SyM-LUT with SOM using STT-MTJ devices.

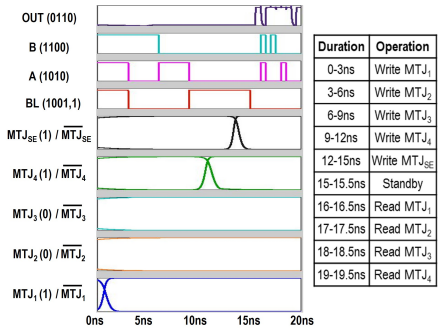
work. This helps in mitigating the threat of P-SCA while providing resiliency against SAT-attack and removal attacks. While we discussed that work in [9] justifies their SAT-resiliency by simulating a limited amount of time, there has been no study on the implication of running the SAT-attack for more extended periods.

4 PROPOSED LOCK&ROLL

4.1 Scan-Enable Obfuscation Mechanism

As demonstrated above, SyM-LUT can be a great candidate to resist P-SCA attacks. Pairing SyM-LUT with LUT-based obfuscation in [9] makes it SAT-resilient. However, to eliminate the threat of SAT attack, we add the Scan-Enable Obfuscation Mechanism (SOM) that aims to provide a multi-layer defense mechanism. It enables the circuit to resist SAT-based attacks as well as other powerful attacks, such as Scan attacks. Figure 5 depicts a 2-input example of SyM-LUT design with SOM. As depicted in Figure 5, once the write operation is terminated, by asserting the **RE** and $\overline{\textbf{RE}}$ signals, we can read the data stored in the MTJs. The read operation of the SyM-LUT with SOM is similar to SyM-LUT and the value of the LUT function is observed at the output nodes **OUT** and $\overline{\textbf{OUT}}$ as shown in Figure 5. As discussed previously, thwarting the SAT attack by building the SAT-hard block is not sufficient. An attacker can apply various inputs to the LUTs using scan chain. Next, we will discuss the scan chain obfuscation of the LUT output. The scan chain locking in our primitive is designed to offer resiliency to both P-SCA and SAT-attack. The SyM-LUT features the SOM circuitry, which is activated when the scan chain is enabled. The SAT-attack uses the scan chain to scan in the input to the oracle circuit and scan out the oracle response. When the scan chain is enabled, the SOM circuitry, i.e., Scan Enable (**SE**), is activated. The SOM will provide the data stored in $\textbf{MTJ}_{SE}$. The $\textbf{MTJ}_{SE}$ bits are configured to either '0' or '1' at random. These values are known to the trusted IP owner, however the untrusted entities cannot know these values. Since the value in $\textbf{MTJ}_{SE}$ is stored randomly, not all of the circuits will be providing the same output if **SE** is enabled. During the read operation, if **SE** is asserted, the data stored in $\textbf{MTJ}_{SE}$ and $\overline{\textbf{MTJ}_{SE}}$ will determine whether the actual function makes it to the **OUT** or the random value in $\textbf{MTJ}_{SE}$ makes it to the **OUT**.

Similar to SyM-LUT, we utilize the HSPICE circuit simulator to validate the functionality of the proposed SyM-LUT with SOM using 45nm CMOS technology and the STT-MRAM model used in [15]. Figure 6 illustrates an implementation of the XOR gate using SyM-LUT with SOM configured to value of '0'. As it can be observed in Figure 6, the content of the $\textbf{MTJ}_{SE}$ is updated to provide the obfuscated output. Additionally, we perform MC simulation study to examine the reliability of the proposed SyM-LUT with



Duration	Operation
0-3ns	Write MTJ_1
3-6ns	Write MTJ_2
6-9ns	Write MTJ_3
9-12ns	Write MTJ_4
12-15ns	Write MTJ_{SE}
15-15.5ns	Standby
16-16.5ns	Read MTJ_1
17-17.5ns	Read MTJ_2
18-18.5ns	Read MTJ_3
19-19.5ns	Read MTJ_4

Figure 6: Simulation waveform for implementation of a 2-input XOR gate using SyM-LUT with MTJ_{SE} being set to value of '0'.

Table 3: Performance of ML-assisted P-SCAs on SyM-LUT with SOM

Algorithm	Accuracy	F1-Score
Random Forest	31.6%	0.322
Logistic Regression	30.93%	0.310
SVM	26.36%	0.284
DNN	35.01%	0.357

SOM in the presence of PV. Similar to the SyM-LUT, SyM-LUT with SOM also maintain error-free write and read operations. SyM-LUT demonstrates less than 0.0001% write errors and less than 0.0001% read errors caused by PV based on the 10,000 error-free MC simulation results for each gate implemented using SyM-LUT with SOM. The Sym-LUT with SOM also exhibits the same current trace as shown in Figure 4. We performed the analysis using ML techniques to infer the functionality implemented by Sym-LUT with SOM, and the results are depicted in Table 3 shows that the functions implemented by the LUTs cannot be distinguished.

Most of the obfuscation primitives leverages the heuristic-based approaches to increase the security against the SAT attack. In our proposed primitive, the LUT itself creates the SAT-hard instance despite its location in the circuit [9]. Moreover, it thwarts the SAT-attack using Scan Lock, thus not requiring the IP designer to rely on the heuristics approaches. The IP owner can identify the circuitry that they want to secure and insert the SyM-LUT with SOM. The SyM-LUT with SOM is the hard block that replaces the logic gate with LUT. The typical design flow used for taping out the IP can be leveraged for implementing the proposed approach. While the overhead imposed by the LUTs can be large, [9] shows how the LUT+LUT block provides superior resiliency with lower overheads. Moreover, in our case, the size of LUT can further be reduced as the SyM LUT-based obfuscation is supplemented with the Scan Lock for added security against the SAT attack.

4.2 Security Coverage of LOCK&ROLL

The HackTest [20] attack can reverse engineer the obfuscated circuit by utilizing the ATPG test vectors which the IP manufacturer provides to the testing facility. The ATPG test vectors are usually generated to offer the highest level of fault coverage. Using the testing data provided, the actual response of the oracle IP upon application of the test vectors can be recorded, and the functionality of the obfuscated gates can be deduced/resolved. The SyM-LUT-based obfuscation and its dynamic nature to morph the functionality based on the contents of the MTJ can circumvent the HackTest attack. To do so, the fabricated IP is programmed with the keys, K_d, which are different than the original intended keys, K_o. The ATPG test patterns are generated using K_d and given to the testing facility. Moreover, testing the IP does not require the IP to be functional [19, 20]. The test patterns are generated for key K_d such that it provides maximum fault coverage and the ability to test the IP for

any faults. Once the IP is tested and returned to the trusted regime, the LUTs can be configured using the correct keys K_o.

Another attack, i.e., ScanSAT, tries to model the obfuscated scan chain as a logic-locking problem for leveraging the SAT attack. In the proposed SyM-LUT primitive, when the Scan chain is activated, the Scan Lock circuitry is activated and now becomes part of the circuit. When the resulting circuit is modeled using the SAT-attack [11], the circuit is originally SAT-hard due to LUT-based obfuscation. Moreover, we have discussed how the SOM thwarts the SAT-based attack in Section 4. For Scan and Shift attack, the key values are saved by the secure cell. For programming the SyM-LUT, we choose to use a separate scan chain for programming the MTJs. The keys are shifted in for the configuration of various SyM-LUT blocks, and the scan-out port of this entire scan chain is blocked. This prevents the attacker from reading the values of MTJ during the writing stage. In the proposed primitive, the MTJs are non-volatile, and thus the programming of the MTJs using this entire chain will only be performed in the trusted regime, thus again mitigating the threat of Scan and Shift attack. The structural analysis on the LUTs yields no concrete information that can help in eliminating the LUTs from the circuit. Thus unlike other obfuscation the proposed primitive is resilient to the removal-based attack. In this manner, Sym-LUT with SOM offers a multi-layer defense mechanism to provide resiliency against various attacks.

5 OVERHEAD AND SECURITY ANALYSIS

Our simulation results show significantly reduced standby energy of 20aJ with write energy consumption of 33fJ and read energy consumption of 4.6fJ, on average. It is worth noting that the write operations are significantly less frequent compared to read operations in LUTs. Assuming both SyM-LUT and SRAM-LUT use the same select tree MUX structure, the structure of a 2-input SyM-LUT requires 12 additional MOS transistors due to the addition of a second select tree MUX structure compared to the conventional 2-input SRAM-LUT. However, assuming a 6T-SRAM cell design is used in the SRAM-LUT, SyM-LUT reduces the overhead by using MTJ devices as storage components and requires 25 fewer MOS transistors. Adding the Scan Enable Obfuscation Mechanism to the SyM-LUT comes at an overhead cost of an additional 18 MOS transistors. It is worth noting that MTJs can be fabricated on top of the baseline MOS transistors, thus incurring low area overhead.

The novelty of our work is not just the side-channel resistant polymorphic design but a defense-in-depth logic locking mechanism using emerging devices that can thwart multiple attacks. The discussion provides a brief qualitative evaluation against state-of-the-art obfuscation primitives as it is not feasible to have a fair comparison without a unified metric and model. Compared to the state-of-the-art obfuscation methodologies, the proposed solution offers better SAT-resiliency compared to SFLL [18] and CASLock [16] as we used the symmetric LUT structure for SAT-hardness and also obfuscated the oracle responses using SOM. Moreover, the proposed method does not suffer from limited output corruptibility, as it does not employ a one-point function. More reconfigurable based obfuscation such as FullLock and InterLock [5] provide SAT-resiliency but require extra efforts of mapping the gates to the complicated proposed structure. Moreover, most of these state-of-the-art obfuscation methodologies discussed here have been defeated and cannot be considered secure. Finally, emerging devices such as [12, 14] thwart SAT-attack and removal attack but have limited applicability and also fail to resist P-SCA. The proposed SyM-LUT provides a multi-layer defense mechanism by combining the improved LUT-based obfuscation with SOM. Moreover, we compared our proposed primitive to the LUT-based obfuscation presented in [9] which is another SAT-resilient technique. While both of the studied primitives results in SAT timeout, the proposed technique has a low overhead and can completely thwart SAT-attacks due to the addition of SOM.

6 CONCLUSION

In this work, we proposed a Power Side-Channel Attack (P-SCA) resilient block using emerging reconfigurable devices and logic locking. We proposed Symmetrical MRAM-LUT (SyM-LUT) for resisting the P-SCA. Proposed Sym-LUT resists the threat of the powerful ML-assisted P-SCA because it maintains a near-zero power variation in the output. Furthermore, our proposed LOCK&ROLL approach utilizes the SyM-LUT design to eliminate the threat of the SAT attack. To yield the SAT-resiliency, we used the reconfigurable LUT-based obfuscation with modified LUT architecture to provide a wide read margin for reliable reads given the increase in the impact of process variation in scaled technology nodes. Moreover, SyM-LUT maintains a standby energy consumption of 20aJ. Our results certify that our proposed LOCK&ROLL is a multi-layer defense mechanism that increases resiliency against various attacks such as state-of-the-art SAT-based attacks, removal attacks, and ML-assisted P-SCA while incurring a small overhead.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation through Computing Research Association for CIFellows #2030859.

REFERENCES

[1] Mohammed Ali et. al. Al-Garadi. 2020. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys Tutorials* 22, 3 (2020), 1646–1685.
[2] Kimia Zamiri *et al.* Azar. 2018. SMT Attack: Next Generation Attack on Obfuscated Circuits with Capabilities and Performance Beyond the SAT Attacks. *IACR TCHES* 2019, 1 (Nov. 2018), 97–122.
[3] D. Sirone *et al.* 2019. Functional Analysis Attacks on Logic Locking. In *2019 Design, Automation Test in Europe Conference Exhibition (DATE).*
[4] Abhrajit Sengupta et. al. [n.d.]. Breaking CAS-Lock and Its Variants by Exploiting Structural Traces. Cryptology ePrint Archive, Report 2021/581.
[5] Hadi Mardani et al. Kamali. 2020. InterLock: An Intercorrelated Logic and Routing Locking. In *ICCAD* (Virtual Event, USA). New York, NY, USA, Article 78, 9 pages.
[6] Jongyeon Kim and *et al.* 2015. A technology-agnostic MTJ SPICE model with user-defined dimensions for STT-MRAM scalability studies. In *2015 IEEE Custom Integrated Circuits Conference (CICC).* IEEE.
[7] Paul et.al. Kocher. 1999. Differential Power Analysis. In *Advances in Cryptology — CRYPTO' 99.* Berlin, Heidelberg, 388–397.
[8] G. Kolhe and *et al.* 2019. On Custom LUT-Based Obfuscation. In *Proceedings of GLSVLSI* (USA). Association for Computing Machinery, 477–482.
[9] G. Kolhe and *et al.* 2019. Security and complexity analysis of LUT-based obfuscation: From blueprint to reality. In *IEEE/ACM ICCAD.*
[10] G. Kolhe and *et al.* 2021. Securing Hardware via Dynamic Obfuscation Utilizing Reconfigurable Interconnect and Logic Blocks. In *2021 58th ACM/IEEE Design Automation Conference (DAC).* 229–234.
[11] P. Subramanyan *et al.* 2015. Evaluating the Security of Logic Encryption Algorithms. In *Int'l Symp. on Hardware Oriented Security and Trust (HOST).*
[12] S. Patnaik and *et al.* 2018. Advancing hardware security using polymorphic and stochastic spin-hall effect devices. In *2018 DATE.*
[13] Stjepan et.al. Picek. 2018. On the Performance of Convolutional Neural Networks for Side-Channel Analysis. In *Security, Privacy, and Applied Cryptography Engineering.*
[14] Nikhil Rangarajan and *et al.* 2020. Opening the Doors to Dynamic Camouflaging: Harnessing the Power of Polymorphic Devices. *IEEE Transactions on Emerging Topics in Computing* (2020), 1–1. https://doi.org/10.1109/tetc.2020.2991134
[15] Soheil Salehi and *et al.* 2019. Clockless Spin-Based Look-Up Tables with Wide Read Margin. In *GLSVLSI* (USA) *(GLSVLSI '19).* New York, NY, USA, 4 pages.
[16] Bicky Shakya and *et al.* 2020. CAS-Lock: A Security-Corruptibility Trade-off Resilient Logic Locking Scheme. *IACR TCHES* (2020), 175–202.
[17] Fangfei Yang and *et al.* 2019. Stripped Functionality Logic Locking With Hamming Distance-Based Restore Unit (SFLL-HD)–Unlocked. *IEEE Transactions on Information Forensics and Security* 14, 10 (2019).
[18] M. Yasin and *et al.* 2019. SFLL-HLS: Stripped-Functionality Logic Locking Meets High-Level Synthesis. In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD).* 1–4. https://doi.org/10.1109/ICCAD45719.2019.8942150
[19] Muhammad et. al. Yasin. 2016. Activation of logic encrypted chips: Pre-test or post-test?. In *DATE.*
[20] Muhammad et.al Yasin. 2017. Testing the Trustworthiness of IC Testing: An Oracle-Less Attack on IC Camouflaging. *IEEE Transactions on Information Forensics and Security* 12, 11 (2017), 2668–2682.