Secure Logic Locking with Strain-Protected Nanomagnet Logic

Naimul Hassan[1,*], Alexander J. Edwards[1], Dhritiman Bhattacharya[2], Mustafa M. Shihab[1], Varun Venkat[1], Peng Zhou[1], Xuan Hu[1], Shamik Kundu[1], Abraham P. Kuruvila[1], Kanad Basu[1], Jayasimha Atulasimha[2], Yiorgos Makris[1], and Joseph S. Friedman[1,*]

[1]Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080

[2]Department of Mechanical and Nuclear Engineering, Virginia Commonwealth University, Richmond, VA 23284

[*]{naimul.hassan, joseph.friedman}@utdallas.edu

2021 58th ACM/IEEE Design Automation Conference (DAC) | 978-1-6654-3274-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/DAC18074.2021.9586258

***Abstract*—Prevention of integrated circuit counterfeiting through logic locking faces the fundamental challenge of securing an obfuscation key against both physical and algorithmic threats. Previous work has focused on strengthening the logic encryption to protect the key against algorithmic attacks, but failed to provide adequate physical security. In this work, we propose a logic locking scheme that leverages the non-volatility of the nanomagnet logic (NML) family to achieve both physical and algorithmic security. Polymorphic NML minority gates protect the obfuscation key against algorithmic attacks, while a strain-inducing shield surrounding the nanomagnets provides physical security via a self-destruction mechanism.**

I. Introduction

Logic locking is a hardware security technique that aims to protect the intellectual property (IP) inside a digital integrated circuit (IC) from counterfeiting by third-party untrusted foundries and reverse engineering parties. The basic idea is to hide the functionality of the chip behind a secret obfuscation key, to which only the IP owners have access [1], [2].

During design, the IP owner modifies the logic such that key values stored in a non-volatile memory unit obfuscate the functionality, as shown in Fig. 1. The modified circuit only performs the logical function of the original design if and only if it is activated by the correct key being written to the non-volatile memory unit. The physical layout of the locked design is sent for fabrication to an untrusted third-party foundry without any information about the key. When the IP owner receives the fabricated circuits, the circuits are activated by writing the secret key into the memory and are publicly released to the open market. As the key was not revealed to the untrusted foundry, the design is considered secure against counterfeiting as long as the key remains secret.

With the foundry oblivious to the chip's functionality, the fundamental security question becomes whether or not the key itself remains secret. In the open market, the end-users have access to samples of the activated chip that contain the key stored in the non-volatile memory unit. Consequently, the key can be physically revealed through invasive attacks [3], [4]. Alternatively, the key can also be determined by analyzing the input-output combinations of the chip through algorithmic non-invasive attacks [2], [5], [6]. Section II describes these threats to logic locking in detail.

The security of logic locking relies on robustness against algorithmic and physical attacks to discover the key. For algorithmic protection, a strong encryption of the original

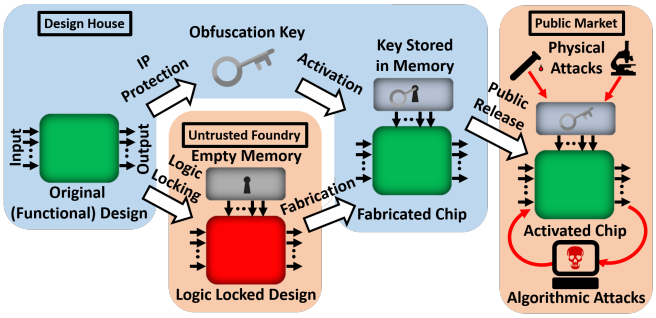

Fig. 1. Logic locking design flow. The logic-locked IC without the obfuscation key is secure from the untrusted foundry that fabricates it. The key is stored in non-volatile memory to activate the chip before release to the open market, where the key can be attacked through algorithmic and physical techniques.

function with respect to the key is necessary, and can be achieved through overhead gates with additional key inputs [1], [7] or polymorphic gates capable of performing multiple functionalities [8]–[10]. The protection can be strengthened by increasing the key size and degree of polymorphism, and by adding overhead logic elements to slow down the algorithmic attacks [11], [12]. The memory elements storing the key should be non-volatile to ensure the key is present for the lifetime of the chip. To prevent the key from being discovered through physical probing, the non-volatile memory and any necessary transportation of the key through the device must be invisible to physical probes. Furthermore, the memory should be tamper-proof to ensure that no other party can corrupt the functionality of the chip by writing an incorrect key [4].

In recent works by Engels *et al.* [3] and Rahman *et al.* [4], doubts were raised about the ability for logic locking to protect against physical attacks. Both groups were able to identify the location of the registers that stored the obfuscation keys, and Rahman *et al.* were able to reveal it by optical probing [4], as described in Section II-D. Ever since the initial proposal of logic locking [1], research related to its security has centered around a competition between malicious algorithmic attacks [2], [5], [6] and protective encryption algorithms [11], [12]; however, this research has largely assumed that it was impossible to read the key from the memory, thus overlooking the possibility of physical attacks against the non-volatile memory. While probing content stored in (secure) memory is often difficult, probing during transportation of the memory

content can successfully reveal the key [4]. Furthermore, countermeasures that add extra layers to deter probing [4] may potentially be defeated by delayering (Section II-C). In summary, no matter how strongly the key encrypts the functionality, a key that can be revealed by physical attacks is not secure at all.

The emergence of non-volatile logic functions has spurred interest in their potential use for logic locking with polymorphic gates designed with non-volatile technologies. However, since most of these proposals do not actually use the non-volatility to store the obfuscation key [8]–[10], they remain similarly vulnerable to physical attacks as described in Sections II-B and II-D. In [13], the key is stored in non-volatile memristors; however, the electrical activity of the circuit can be probed to reveal the key through side-channel attacks (Section II-B), and imaging attacks (Section II-D) can enable reading of the non-volatile memory. The solution in [14] uses polymorphic "all-spin logic" (ASL) gates to prevent power analysis side-channel attacks [15], but the obfuscation key can be revealed by magnetic imaging (Section II-E) and electrical side-channel attacks based on spin (Section II-B).

In this work, toward resolving the above limitations and security challenges, we make the following contributions:

- We leverage polymorphism to encrypt nanomagnet logic (NML) circuits by storing an obfuscation key within non-volatile nanomagnets such that the key is never transported, thereby preventing its discovery through physical probing of circuit dynamics.
- We program the obfuscation key in the nanomagnets through spin-orbit torque to activate the logic-locked IC and burn fuses to prevent post-activation tampering.
- We protect the non-volatile key-storing nanomagnets against physical probing via a strain shield that causes self-destruction of the key when delayering is attempted.
- We experimentally demonstrate that a shielding material prevents magnetic imaging of the obfuscation key.
- Finally, we demonstrate that the proposed scheme is secure against all known algorithmic and physical threats against logic locking.

To the best of our knowledge, this is the first proposal for a logic locking scheme that is secure against both algorithmic and physical attacks.

II. Threats Against Logic Locking

A logic-locked IC design consists of a locked layout and a secret obfuscation key. The untrusted third-party foundry gets access to the locked layout in order to manufacture the circuit. To counterfeit the IC, a reverse engineer would need to discover the obfuscation key – as well as the physical layout, if the foundry is not involved in the attack. The following algorithmic and physical attacks have the potential to unlock a logic-locked IC.

A. Satisfiability Attack

The Boolean satisfiability (SAT) decryption algorithm is a powerful non-invasive technique for retrieving the obfuscation key of an activated chip [2], [5]. SAT-based attacks require an activated IC and the netlist of the locked design. By analyzing the input-output combinations of the locked netlist using different key values and comparing to the input-output relationship of the activated chip, the SAT attack efficiently identifies incorrect keys and rapidly narrows down the search for the correct key. No logic locking can ever be completely robust to SAT attacks; the strength of a locking scheme is characterized by the time required to identify the correct key. Complex encryption techniques can improve the locking strength, preventing the identification of the correct key within a reasonable amount of time.

B. Side-Channel Attack

In a side-channel attack, circuit activity is analyzed during operation of the locked circuit to determine the key. Such attacks analyze the physical circuit signatures that are created as by-products of circuit operation, including power consumption, voltage drop, and electromagnetic radiation [16]. Therefore, any obfuscation key which is *electrically* applied to a logic locked circuit is vulnerable to side-channel attacks [1], [7], regardless of whether the key is stored in a non-volatile manner. This is a significant vulnerability for CMOS logic-locked circuits, as well as for polymorphic gates designed with non-volatile technologies [8]–[10].

For example, as the non-volatile memristors storing the obfuscation key in [13] are read electrically during logical operation, side-channel attacks can discover the key in this paradigm. Likewise, although the electrical power consumption for different polarities of ASL nanomagnets are identical [14], [15], the ASL clock connections may be used to electrically measure the non-local resistance between neighboring nanomagnets [17]. In particular, the non-local resistance between two ASL nanomagnets is dependent on their relative magnetic orientation, thereby providing a potential electrical side-channel to reveal the nanomagnet polarities that encode the obfuscation key.

C. Material Delayering

Removing material layers from an IC, termed delayering, is a critical part of invasive reverse engineering that allows a locked layout to be physically imaged or an obfuscation key stored in the memory unit to be directly probed. State-of-the-art reverse engineering facilities utilize a combination of techniques, including etching and polishing to get access to critical material layers that are not normally accessible [18]. This attack is often used to enable the imaging attacks of Sections II-D through II-F.

D. Imaging Attack on Electrical Properties & Behavior

A variety of imaging attacks can be used to reveal the electrical behavior of a circuit, and therefore the obfuscation key. For example, sophisticated optical tools can probe an IC to track the electrical signals passing through specific nodes over time [19]. Following the basic approach of [19] and utilizing electro-optical frequency mapping (EOFM), Rahman *et al.* produced an activity map of a logic-locked design

implemented on an FPGA, which they then used to reveal the key [4]. Any logic-locked system that produces an electrical signature of the obfuscation key is vulnerable to this type of physical attack.

Imaging can reveal the obfuscation key for logic-locked CMOS designs [1], [7] as well as polymorphic gates designed with non-volatile elements [8]–[10] when the key is applied electrically to the obfuscated gates. Likewise, the obfuscation key stored in non-volatile memristors [13] can be revealed when it is used electrically for logic. In short, no logic locking scheme that electrically transports or utilizes the key is secure against imaging, regardless of the use of non-volatility.

E. Imaging Attack on Magnetic Properties & Behavior

As conventional computing systems do not incorporate magnetism in a manner that makes them vulnerable to magnetic attacks, such attacks have not previously received significant attention. The secure system proposed herein, however, is based on magnetism, hence it is important to consider magnetic imaging attacks. In particular, magnetic probing schemes can be classified in two categories: (i) detection of stray field, and (ii) interaction between electrons/X-rays/light and sample magnetization.

The first type of imaging techniques includes magnetic force microscopy (MFM), in which the stray field emanating from the sample interacts with an oscillating magnetic tip and thus changes its frequency and phase. For the second type, which includes the magneto-optic Kerr effect (MOKE), the magnetic information is contained in the light reflected from the surface of the magnetic sample. For both magnetic imaging techniques, probing can be blocked by a thick, opaque shield. However, delayering of this shield can enable probing of the magnetic polarities; this approach can be used to reveal the obfuscation key stored in the polymorphic ASL gates of [14].

F. Imaging Attack on Physical Layout

For successful counterfeiting of a logic-locked IC, both the physical layout and the obfuscation key are required; the physical layout is also required in order to generate the netlist necessary to run the SAT attack. Imaging attacks can reveal the layout through scanning electron microscopy and other imaging techniques [20].

G. Untrusted Foundry Attacks

In order to manufacture the locked IC, untrusted foundries require the physical layout. Foundries are also equipped with sophisticated tools to launch both algorithmic and physical attacks for accessing the obfuscation key, making them a particularly dangerous threat against the locked chip.

III. Strain-Protected Nanomagnet Logic Locking

NML is a nanoscale energy-efficient logic family in which logical operations are performed through dipolar coupling between nanomagnets [21]. In this work, we propose the use of polymorphism in NML for developing a logic locking scheme that is secure against algorithmic and physical attacks. The non-volatility of nanomagnets with strain-induced perpendicular magnetic anisotropy (PMA) provides a physically secure memory that shields the obfuscation key from electrical or magnetic imaging, thus overcoming a fundamental challenge for logic locking. Furthermore, fuses in the spin-orbit torque (SOT) programming path prevent tampering with the non-volatile memory in which the key is stored. The proposed scheme drastically increases the attractiveness of NML, which has heretofore been hindered by its limited operational speed [22].

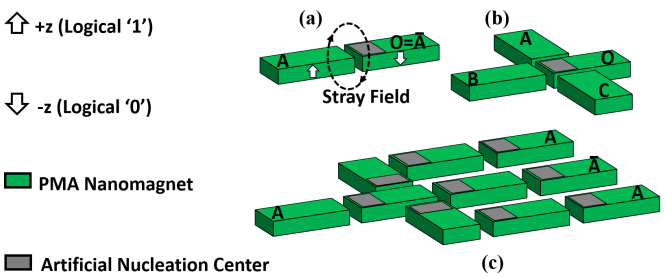

Fig. 2. (a) NML inverter encoded with nanomagnet polarity, where A is the input and O is the output. (b) Three-input NML minority gate with output O and inputs A, B, and C. (c) Fan-out of NML signals.

Our proposed approach to use strain to protect magnets from imaging attacks that require delayering can also increase the physical security of ASL polymorphic gates [14] from magnetic imaging (Section II-E). Similar approaches may also be considered based on magnetoelectric spin–orbit (MESO) logic, which promises a 30x improvement in energy efficiency relative to CMOS [23]. However, the ASL and MESO gates may remain vulnerable to spin-based side-channel attacks, as mentioned in Section II-B. In contrast to ASL and MESO, NML does not require electrical connections to the magnets during logical operation, thereby precluding side-channel attacks that reveal the obfuscation key.

A. Background on Nanomagnet Logic

NML encodes binary logic values in the magnetic polarity of bistable nanoscale magnets. While NML can be implemented both with in-plane and PMA nanomagnets, this paper only considers PMA due to its potential for superior protection against physical attacks. The bistable magnetic polarity encodes binary '0' and '1' signals, and logical operations in NML are performed by magnetostatic interactions between the

TABLE I
NML Polymorphism

C	A	B	O	Function with Fixed C
$-z$	$-z$	$-z$	$+z$	$O = \overline{A \wedge B}$
$-z$	$-z$	$+z$	$+z$	
$-z$	$+z$	$-z$	$+z$	
$-z$	$+z$	$+z$	$-z$	
$+z$	$-z$	$-z$	$+z$	$O = \overline{A \vee B}$
$+z$	$-z$	$+z$	$-z$	
$+z$	$+z$	$-z$	$-z$	
$+z$	$+z$	$+z$	$-z$	

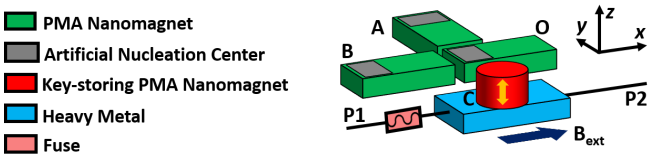

Fig. 3. Polymorphic NAND/NOR gate with fan-in nanomagnets A and B, fan-out nanomagnet O, and a programmable non-volatile nanomagnet C that stores one bit of the obfuscation key. The obfuscation key bit is programmed to nanomagnet C via SOT with tamper-proof fuse connections.

neighboring nanomagnets. As shown in the NML inverter gate of Fig. 2(a), the output nanomagnet has an artificial nucleation center (ANC) with reduced anisotropy that enables the stray magnetic field from the input nanomagnet to switch this ANC to the opposite magnetic polarity. The magnetic orientation of the ANC then propagates through the remainder of the output nanomagnet by magnetic domain wall motion.

Fig. 2(b) shows a three-input NML minority gate. As shown in Table I, the magnetic state of the output nanomagnet is the opposite of the majority of the magnetic states of the input nanomagnets. Fan-out of NML signals can be achieved with a tree of nanomagnets similar to Fig. 2(c). The speed of NML circuits is dependent on the rate of domain wall propagation through the magnets [22].

Both the switching at the ANC and the domain wall propagation are assisted by an alternating z-directed clocking magnetic field. This clocking approach, combined with the use of PMA, limits the impact of errors [24] that affect in-plane NML resulting from imprecise fabrication [25]. Several other clocking approaches have been proposed in which nanomagnets are electrically contacted similar to ASL, with energy efficiency benefits. However, in order to preclude side-channel attacks as described in Section II-B, this paper considers only clocking with an alternating applied magnetic field.

B. Logic Locking with Nanomagnet Logic Polymorphism

We propose a logic locking concept based on polymorphic NML gates. Polymorphism in NML is introduced by programming the polarity of particular input nanomagnets with bits of the obfuscation key. While the fan-in and fan-out nanomagnets have ANCs to perform and cascade logical operations, the ANC-free hard-coded non-volatile nanomagnets store the key bits and remain fixed for the lifetime of the chip.

Fig. 3 shows a polymorphic version of the three-input minority gate of Fig. 2(b) with input C being the hard-coded nanomagnet. When the polarity of input C is programmed to the -z(+z)-direction, the polymorphic gate performs the logical NAND (NOR) operation between inputs A and B and propagates the result to output O. An AND/OR polymorphic gate can also be realized with the inverter of 2(a) concatenated to the NAND/NOR gate output.

The use of three-input minority gates as polymorphic two-input NAND/NOR gates necessitates an increase in the number of gates required to perform logic functions, as the hard-coded nanomagnet cannot be utilized as a variable gate input. It is worth noting that any n-input polymorphic NAND (NOR) function can be performed by hard-coding $n-1$ nanomagnets to -z (+z) polarity. To increase the polymorphism for increased robustness to algorithmic attacks (Section II-A), some of these additional input nanomagnets can be hard-coded; the total number of different functions possible from a polymorphic gate scales as $m+1$ for m hard-coded nanomagnets with $m+1$ fan-in nanomagnets.

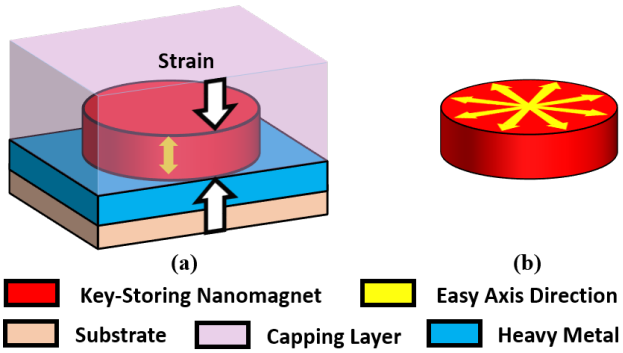

Fig. 4. (a) PMA due to strain from the capping layer and the substrate. (b) Strain-free isotropic in-plane easy magnetization direction after substrate and/or capping layer is etched. Arrows show easy magnetization orientation.

C. Spin-Orbit Torque Programming of Nanomagnet Keys

The hard-coded nanomagnets can be programmed to the obfuscation key bits by SOT. As shown in the polymorphic gate of Fig. 3, the key-storing nanomagnet is fabricated on top of a heavy metal. The heavy metal is connected to the programming path P1-P2 through a fuse that functions as conductive interconnect, allowing the IP owner to program the nanomagnets. Bidirectional current through the heavy metal in the $+(-)x$ direction generates spins polarized in the $+(-)y$ direction via SOT [26]; this current is continually increased until the fuse burns, cutting off the current flow. A $+x$-directed magnetic field is applied throughout this process, causing the nanomagnet polarity to relax in the $+(-)z$ direction after the current is removed [26]. This protocol prevents the obfuscation key from being reprogrammed by any other party to corrupt the chip or perform future algorithmic attacks that rely on rewriting the key. Therefore, the non-volatile hard-coded nanomagnets are tamper-proof.

D. Protection from Delayering and Imaging with Strain-Dependent Nanomagnet Anisotropy

In order to prevent discovery of the obfuscation key through imaging techniques that require proximity or visibility, an opaque "strain shield" surrounding the nanomagnets induces their anisotropy such that key bits stored in the hard-coded nanomagnets self-destruct if delayering is attempted. To achieve this, we propose that the PMA of the hard-coded nanomagnets be induced by strain between the nanomagnets and the materials surrounding them, including the substrate, heavy metal, and capping layer, as shown in Fig. 4. It has been experimentally demonstrated that interfacial anisotropy can arise in magnetic/non-magnetic multilayer due to strain. The strength of the anisotropy depends on the non-magnetic layer thickness [27].

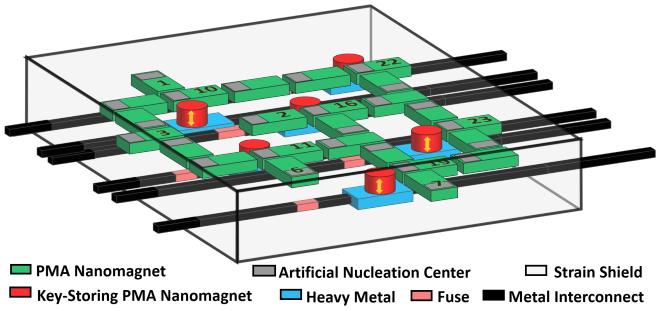

Fig. 5. Physically protected logic-locked c17 circuit with programming port for the IP owner. Numbered nanomagnets correspond to the c17 net numbering.

If an attacker tries to etch the strain shield surrounding a hard-coded nanomagnet, the magnetic polarity will switch from PMA to isotropic in-plane easy magnetization, thereby erasing the bit of the obfuscation key hard-coded in the nanomagnet. Furthermore, it has been shown that etching a surrounding layer degrades the magnetic properties well before reaching the magnet [28]. By modifying the anisotropy, delayering of the strain shield from any direction will therefore destroy the obfuscation key and prevent discovery of the key through magnetic imaging attacks.

E. Overview of Complete Secure System

Fig. 5 shows a circuit (ISCAS'85 benchmark c17) locked with NML polymorphism as an example of a simple circuit that illustrates the complete security concept [29]. As can be seen in the figure, there are six nanomagnets hard-coded with obfuscation bits written with SOT currents through the heavy metal regions, setting each minority gate to either the NAND or NOR function. The entire circuit is surrounded by a strain shield such that any attempt at delayering near the hard-coded nanomagnets causes self-destruction of the key bits.

IV. Security of Strain-Protected Nanomagnet Logic Against Logic Locking Threats

The polymorphism of the NML gates in concert with the strain-mediated self-destruction mechanism protects the proposed logic locking scheme against all physical and algorithmic attacks on the obfuscation key. Though the physical layout of a logic-locked design can be discovered, protection of the obfuscation key is sufficient to prevent illegal reproduction and tampering of unlocked ICs.

A. Satisfiablity (SAT) Attack

To demonstrate the algorithmic security offered by NML polymorphism, we performed the SAT attack on ISCAS'85 benchmark circuits [29] locked with polymorphic NML gates using the SAT attack tool developed in [2]. The results are shown in Table II, and are similar to results conventionally achieved with logic-locked CMOS circuits. Similar to conventional CMOS circuits, SAT protection can be enhanced with increased overhead through techniques similar to SARLock and anti-SAT [11], [12]. Furthermore, NML can provide superior algorithmic encryption relative to CMOS through the use of logic-locked gates with more than three inputs as described at the end of Section III-B.

B. Side-Channel Attack

After the hard-coded nanomagnets are programmed and the fuses are burnt, the activated logic circuits released to the public perform no electrical activity. There is no movement of the key either electrically or magnetically and no magnetic to electric conversion, and there is consequently no electrical signature of the obfuscation key. Therefore, there are no side-channels available for launching an attack to reveal the key.

C. Material Delayering

As discussed in Section III-D, any attempt to delayer the strain shield surrounding the nanomagnets causes the anisotropy to switch from PMA to in-plane easy magnetization. This causes the nanomagnet to move to a random in-plane state, thus destroying the obfuscation key. Moreover, the etching process degrades the magnetic properties of the nanomagnets, resulting in complete destruction of the IC.

D. Imaging Attack on Electrical Properties & Behavior

Imaging attacks on electrical properties or behavior are not possible, as NML functions through magnetic interactions instead of electrical interactions.

E. Imaging Attack on Magnetic Properties & Behavior

As delayering will cause self-destruction of the obfuscation keys stored in the nanomagnets, any imaging attack on magnetic properties or behavior must be performed through the strain shield surrounding the nanomagnets. However, stray-field detection of magnetization requires proximity to the nanomagnet, and electron/X-ray/light requires that there be no opaque layer between the source and the nanomagnet.

To demonstrate resilience of the proposed system against magnetic imaging attacks, we have performed MFM imaging of magnetic domains within a Co(15nm)/Ti(5nm)/Substrate film. Over half of the film, an additional 100 nm Ti capping

TABLE II
ISCAS'85 SAT Attack Summary

Benchmark	NML		
	Key (bits)	Time to Solve (s)	Iterations
c17	6	0.011595	3
c432	102	0.078054	8
c499	58	0.133059	18
c880	294	4.55835	65
c1355	474	19788	169
c1908	441	187.389	106
c2670	676	Timeout[1]	4743
c3540	956	Timeout[1]	25
c5315	1413	Timeout[1]	192
c6288	2384	Timeout[1]	17
c7552	2102	Timeout[1]	47

[1] With a timeout of 12 hours.

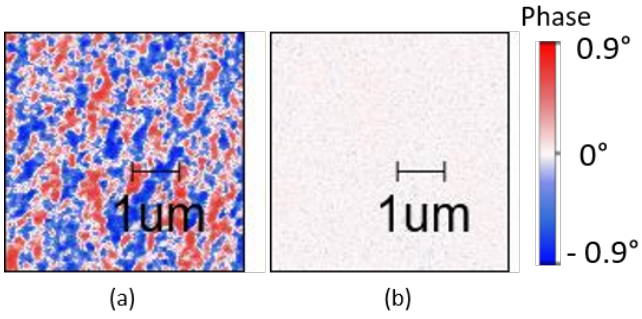

Fig. 6. MFM imaging of in-plane magnetic domains (a) without and (b) with a 100 nm capping layer. Phase contrast disappeared when the capping layer was deposited, and the remaining signal is random noise.

layer was deposited on top of the Co layer. When MFM imaging is performed on bare Co, in-plane magnetic domains can be easily observed, as shown in Fig. 6(a). On the other hand, phase contrast disappears in the MFM image when an area over the capping layer is scanned, as shown in Fig. 6(b). Therefore, the MFM is no longer able to determine the magnetic polarities, thus demonstrating the ability of a sufficiently thick strain shield to prevent the attacker from discovering the magnetic information.

F. Imaging Attack on Physical Layout

After delayering, a reverse engineer can image the physical layout of the logic-locked design by scanning electron microscopy or any other material probing technique. However, a locked physical layout cannot be unlocked or reproduced without the obfuscation key, which in the proposed scheme is robust against all known attacks.

G. Untrusted Foundry Attacks

The third-party foundry is provided with the physical layout as well as the netlist of the logic-locked design during the manufacturing process. However, once again, without access to the physically and algorithmically secure obfuscation key, counterfeiting of the functional design is impossible.

V. Conclusions

This work proposes a physically and algorithmically secure hardware platform based on NML to implement logic locking that could be applied to both purely-spintronic and hybrid NML-CMOS systems. While the drawbacks of NML have impeded its progress, its unique algorithmic and physical security features justify further investigation into the adoption of logic-locked NML systems in adversarial environments. The polymorphic minority gates provide the algorithmic protection of the proposed system, while the strain-controlled PMA of the nanomagnets ensures physical protection of the obfuscation key. Probing the magnetic state of the hard-coded nanomagnets to reveal the obfuscation key is prevented by the opacity and thickness of the strain shield, and any attempt to delayer will cause self-destruction of the obfuscation key through strain relaxation. By exploiting the unique physics of nanomagnet logic and strain-dependent magnetic anisotropy, the proposed method provides an intriguing solution to secure an obfuscation key from physical attacks, thereby opening new pathways for logic locking.

VI. Acknowledgements

Friedman, Makris, Hassan, and Edwards acknowledge funding from the NSF IUCRC Center for Hardware and Embedded Systems Security and Trust. The VCU authors acknowledge NSF grants CCF 1815033 and ECCS 1954589. Fabrication and characterization was carried out at VCU VMEC and NCC.

References

[1] J. A. Roy *et al.*, "Epic: Ending piracy of integrated circuits," in *Proc. DATE*, 2008, pp. 1069–1074.
[2] P. Subramanyan *et al.*, "Evaluating the security of logic encryption algorithms," in *Proc. IEEE HOST*, 2015, pp. 137–143.
[3] S. Engels *et al.*, "The end of logic locking? a critical view on the security of logic locking." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 796, 2019.
[4] M. T. Rahman *et al.*, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes." in *Proc. HOST*, 2020, pp. 262–272.
[5] K. Shamsi *et al.*, "AppSAT: Approximately deobfuscating integrated circuits," in *Proc. IEEE HOST*, 2017, pp. 95–100.
[6] J. Rajendran *et al.*, "Security analysis of logic obfuscation," in *Proc. DAC*, 2012, pp. 83–89.
[7] S. Dupuis *et al.*, "A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans," in *Proc. IEEE IOLTS*, 2014, pp. 49–54.
[8] F. Parveen *et al.*, "Hybrid polymorphic logic gate with 5-terminal magnetic domain wall motion device," in *Proc. IEEE ISVLSI*, 2017, pp. 152–157.
[9] S. Patnaik *et al.*, "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in *Proc. DATE*, 2018, pp. 97–102.
[10] N. Rangarajan *et al.*, "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," *arXiv:1811.06012*, 2018.
[11] M. Yasin *et al.*, "SARLock: SAT attack resistant logic locking," in *Proc. IEEE HOST*, 2016, pp. 236–241.
[12] Y. Xie and A. Srivastava, "Anti-SAT: Mitigating SAT attack on logic locking," *IEEE TCAD*, vol. 38, no. 2, pp. 199–207, 2018.
[13] A. Rezaei *et al.*, "Hybrid memristor-CMOS obfuscation against untrusted foundries," in *Proc. IEEE ISVLSI*, 2019, pp. 535–540.
[14] Q. Alasad *et al.*, "Leveraging all-spin logic to improve hardware security," in *Proc. GLSVLSI*, 2017, pp. 491–494.
[15] ——, "Resilient and secure hardware devices using ASL," *ACM JETC*, vol. 17, no. 2, 2021.
[16] M. Yasin *et al.*, "Hardware security and trust: Logic locking as a design-for-trust solution," in *The IoT Physical Layer*. Springer, 2019, pp. 353–373.
[17] S. Takahashi and S. Maekawa, "Spin current in metals and superconductors," *Journal of the Physical Society of Japan*, vol. 77, no. 3, pp. 031 009–031 009, 2008.
[18] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proc. DAC*, 2011, pp. 333–338.
[19] R. Desplats *et al.*, "Faster IC analysis with PICA spatial temporal photon correlation and CAD autochanneling," *Microelectronics Reliability*, vol. 43, no. 9-11, pp. 1663–1668, 2003.
[20] B. Shakya *et al.*, "Covert gates: Protecting integrated circuits with undetectable camouflaging," *IACR TCHES*, pp. 86–118, 2019.
[21] A. Imre *et al.*, "Majority logic gate for magnetic quantum-dot cellular automata," *Science*, vol. 311, no. 5758, pp. 205–208, 2006.
[22] F. Riente *et al.*, "MagCAD: tool for the design of 3-D magnetic circuits," *IEEE JXCDC*, vol. 3, pp. 65–73, 2017.
[23] S. Manipatruni *et al.*, "Scalable energy-efficient magnetoelectric spin–orbit logic," *Nature*, vol. 565, no. 7737, pp. 35–42, 2019.
[24] I. Eichwald *et al.*, "Nanomagnetic logic: Error-free, directed signal transmission by an inverter chain," *IEEE TMAG*, vol. 48, no. 11, pp. 4332–4335, 2012.
[25] D. Carlton *et al.*, "Investigation of defects and errors in nanomagnetic logic circuits," *IEEE TNANO*, vol. 11, no. 4, pp. 760–762, 2012.
[26] S. Fukami *et al.*, "A spin–orbit torque switching scheme with collinear magnetic easy axis and current configuration," *Nature Nanotechnology*, vol. 11, no. 7, pp. 621–625, 2016.
[27] F. den Broeder *et al.*, "Magnetic anisotropy of multilayers," *Journal of Magnetism and Magnetic Materials*, vol. 93, pp. 562–570, 1991.
[28] J. Read *et al.*, "Magnetic degradation of thin film multilayers during ion milling," *APL Materials*, vol. 2, no. 046109, 2014.
[29] "ISCAS'85 Benchmark." [Online]. Available: http://www.pld.ttu.ee/~maksim/benchmarks/iscas85/bench/