Physically Secure Logic Locking with Nanomagnet Logic

Alexander J. Edwards[1*], *Student Member, IEEE*, Naimul Hassan[1], *Member, IEEE*, Jared D. Arzate[1,2], *Student Member, IEEE*, Alexander N. Chin[1], *Student Member, IEEE*, Dhritiman Bhattacharya[3], *Member, IEEE*, Mustafa M. Shihab[1], *Member, IEEE*, Peng Zhou[1], Xuan Hu[1], *Member, IEEE*, Jayasimha Atulasimha[3], *Senior Member, IEEE*, Yiorgos Makris[1], *Senior Member, IEEE*, and Joseph S. Friedman[1*], *Senior Member, IEEE*

[1]Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080
[2]Department of Electrical and Computer Engineering, University of Texas at Austin, Austin, TX 78712
[3]Department of Mechanical and Nuclear Engineering, Virginia Commonwealth University, Richmond, VA 23284
*{alexander.edwards, joseph.friedman}@utdallas.edu

***Abstract*—Securing integrated circuits against counterfeiting through logic locking presents the fundamental challenge of protecting a locking key from physical, Boolean satisfiability (SAT)-based, and structural threats. Prior research has mainly focused on enhancing logic locking to thwart SAT-based and structural attacks but overlooked the necessity of robust physical security. Our work introduces a novel approach: a logic locking scheme utilizing the non-volatile properties of nanomagnet logic (NML) to provide comprehensive protection. Polymorphic NML minority gates along with conventional locking techniques fortify the locking key against SAT-based and structural threats, while a protective shield, inducing strain in the nanomagnets, offers physical security via a self-destruct mechanism.**

Although the NML system improves physical security and preserves security against SAT-based and structural attacks, it suffers from drawbacks related to limited reliability and speed, which result in a notable security overhead cost. Consequently, we propose a hybrid CMOS/NML logic locking approach in which NML islands are integrated into a predominantly CMOS-based system. This hybrid solution continues to deliver security against physical, SAT-based, and the known structural attacks while minimizing the associated overhead. We evaluate the security of such hybrid systems against conventional and physically-enhanced SAT attacks. The hybrid logic systems are found to retain the security against conventional SAT-based attacks. We further find that these hybrid logic systems are also robust to physically-enhanced SAT attacks in which the attacker has access to all internal electrical signals. These hybrid logic systems are thus shown to provide security against all known physical attacks as well as SAT-based attacks, with minimal efficiency trade-offs resulting from the use of emerging technologies.

***Index Terms*—logic locking; nanomagnet logic; hardware security; polymorphic logic; perpendicular magnetic anisotropy; physical security; SAT attacks; satisfiability**

I. Introduction

Logic locking is a hardware security method to safeguard the intellectual property (IP) implemented on a digital integrated circuit (IC) from potential threats such as third-party untrusted foundries and reverse engineering entities. The core concept involves concealing the chip's functionality behind a confidential locking key, such that only the IP owners can unlock the chip [1], [2].

The IP designer introduces alterations to the logic, adding additional key inputs to the circuit's functionality, as depicted in Fig. 1. The altered circuit will only execute the correct logical tasks when the correct locking key is stored in designated on-chip non-volatile memory. The IP owner then sends the locked chip layout to a potentially untrusted foundry, withholding any key-related information. Upon receipt of the physical chips, the IP owner unlocks the chips with the key and subsequently releases the chips to the unsecured public market. The design's security against illicit reverse-engineering relies on maintaining the key's secrecy, as it is never disclosed to the public or an untrusted foundry

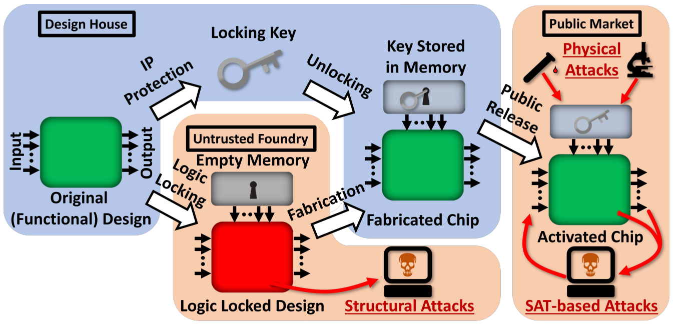


Fig. 1. The logic locking challenge. A chip is protected from an untrusted foundry by splitting the design such that the foundry does not have access to the locking key that unlocks the chip after fabrication. An attacker wanting to replicate the design must have both the layout and the key. As it is generally assumed that the layout is not secure, security of the IP depends on the security of the locking key stored in on-chip memory against various physical, SAT-based, or structural attacks that aim to reveal the key.

Since the chip's operational details are concealed from the foundry, the primary security concern shifts to whether the key maintains confidentiality. In the commercial market, end-users have access to unlocked chip samples containing the key stored in non-volatile memory. This makes the key vulnerable to exposure through invasive techniques [3], [4], moreover, there is the risk of potential discovery via Boolean satisfiability (SAT)-based attacks by analyzing the chip's input-output patterns [2], [5], [6]. Section II provides a detailed examination of these threats to logic locking.

Logic locking must be secure against physical, SAT-based, and structural attacks aimed at uncovering the hidden key. To fortify the system against SAT-based attacks, it is imperative to strongly lock the original logic function relative to the key by introducing additional key-controlled logic gates [1], [7] or polymorphic gates with reprogrammable function [8]–[10]. The strength of the locking can be increased by utilizing longer keys, increasing the polymorphism, and incorporating additional logic circuits specially designed to confound SAT-based attacks [11], [12], though incorporation of these structures can create vulnerabilities to structural attacks which glean designer intent based on how locking hardware is inserted [13]–[15].

The memory components containing the key should be non-volatile, ensuring the key's persistence throughout the chip's operational life. To thwart the discovery of the key through physical probing, it is essential that both the non-volatile memory and the key's internal transport be impervious to physical probing. Additionally, the memory should be tamper-resistant to prevent any unauthorized entities from compromising the chip's functionality by writing an incorrect key [4].

Recent studies by Engels *et al.* [3] and Rahman *et al.* [4] have cast doubt on the effectiveness of logic locking in defending against physical attacks. Both teams pinpointed the locking-key-storing registers, and Rahman *et al.* successfully extracted locking key values through optical probing [4], as detailed in Section II-E. In logic locking [1], security research has primarily revolved around the contest between SAT-based attacks [2], [5], [6] and locking algorithms [11], [12], [16]–[18], often assuming that reading the key from on-chip non-volatile memory was not viable, thus neglecting the potential for physical attacks on the key. While directly imaging secure memory contents is typically challenging, probing during delivery of the key to the locked gates can reveal the key [4]. Moreover, countermeasures designed to add additional material layers to hinder probing [4] may be susceptible to delayering (Section II-D). Regardless of how robustly the key hides chip functionality, a key that can be extracted by physical attacks is not secure at all.

Non-volatile logic in emerging technologies may be particularly useful for logic locking. A number of proposals incorporate polymorphism into non-volatile emerging technology logic gates, though they often do not utilize non-volatility for key storage [8]–[10], opening potential physical vulnerabilities, as outlined in Sections II-C and II-E. In [19], memristors are used to store the locking key; however, probing the circuit's *electrical activity* can expose the key through side-channels (Section II-C), and imaging attacks (Section II-E) can reveal the non-volatile memory. In another approach detailed in [20], polymorphic "all-spin logic" (ASL) gates are employed to thwart power-side-channel attacks [21], though the key remains vulnerable to magnetic imaging (Section II-F) and spin-based electrical side-channel attacks (Section II-C).

To address the above limitations and security challenges, this paper presents the following contributions, recapitulating and extending our prior research in [22], [23]:

- Locking with NML Polymorphism: We leverage polymorphism to lock nanomagnet logic (NML) circuits. This method involves storing the locking key within non-volatile nanomagnets such that the key is never transported, effectively thwarting any attempt to discover the key through physical probing of circuit dynamics [22].

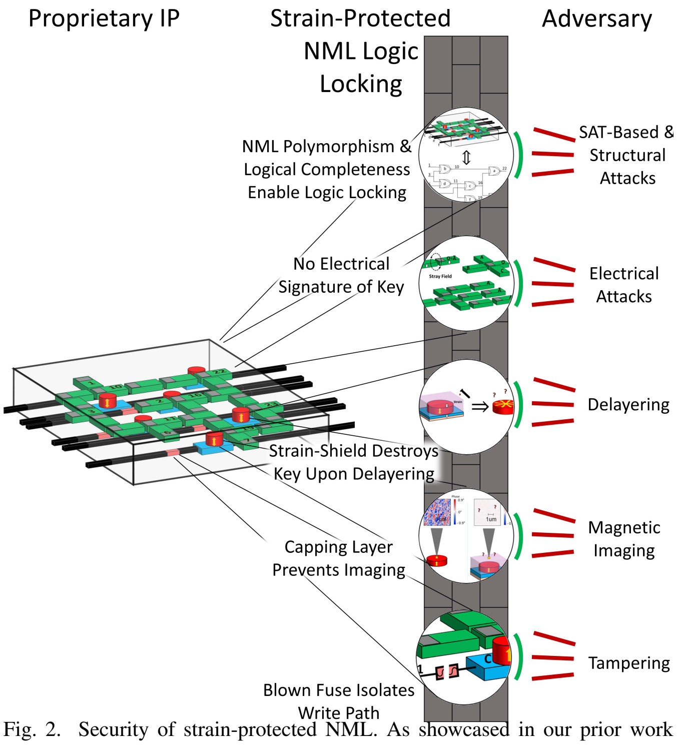

Proprietary IP
Strain-Protected NML Logic Locking
Adversary
NML Polymorphism & Logical Completeness Enable Logic Locking
No Electrical Signature of Key
Stray Field
Strain-Shield Destroys Key Upon Delayering
Capping Layer Prevents Imaging
Blown Fuse Isolates Write Path
SAT-Based & Structural Attacks
Electrical Attacks
Delayering
Magnetic Imaging
Tampering

Fig. 2. Security of strain-protected NML. As showcased in our prior work [22], NML circuits shielded with an opaque strain-inducing capping layer have proven to be resilient against all known physical attacks while retaining the same level of security as CMOS against SAT-based and structural attacks.

- Tamper-Proof Spin-Orbit Torque Programming: The key-bit storing nanomagnets are programmed through spin-orbit torque to unlock the IC, and, by burning fuses in the process, prevent post-activation tampering [22].
- Shielding Against Physical Probing: Non-volatile nanomagnets housing the locking key are safeguarded against physical probing by a strain shield; an attempted delayering of the shield induces the self-destruction of the key. [22]
- Preventing Magnetic Imaging: Through experimental validation, we confirm that the use of shielding materials effectively prevents magnetic imaging of the locking key [22].
- Security Against All Known Threats: We demonstrate that the proposed scheme is secure against all known physical threats and is as secure as CMOS against SAT-based and structural attacks as shown in Fig. 2 [22].
- Hybrid CMOS/NML Logic Locking: We propose a hybrid CMOS/NML logic locking scheme that combines the speed and reliability of CMOS with the security of NML. This scheme selectively locks circuitry using small "islands" of NML logic [23].
- Inherited Physical Security: We prove that a complete hybrid CMOS/NML logic system inherits the physical security of logic-locked NML [23].
- Resilience to SAT-based Attacks: We demonstrate that the hybrid CMOS/NML logic locking scheme can be secured against SAT-based attacks, including physically enhanced attacks with full CMOS visibility (novel).

To the best of our knowledge, this work introduces the first logic locking scheme that is resilient against physical threats while retaining the same security against SAT-based and structural attacks that is provided by CMOS, addressing an essential need in secure circuit design.

II. Threats Against Logic Locking

A logic-locked IC design comprises a secured layout and a confidential locking key. The untrusted third-party foundry is granted access to the locked layout for the purpose of IC production. To counterfeit the IC, a reverse engineer must uncover both the locking key – as well as the physical layout, if the foundry is not involved in the attack. The following attacks have the potential to unlock a logic-locked IC.

A. Satisfiability Attacks

The SAT attack is a strong, non-invasive method for uncovering the on-chip stored key [2], [5] and is often utilized to evaluate new logic locking methods [2], [9], [24]. SAT-based attacks, as depicted in Fig. 3, need an unlocked IC (the oracle) and the locked circuit netlist to systematically narrow down the search space for the key. SAT attacks efficiently narrow down the key search space by studying input-output patterns of the netlist and comparing them to the unlocked chip's output; SAT attacks quickly remove incorrect key-bit candidates and swiftly reduce the space of possible correct key-bits.

The inclusion of advanced logic locking circuit structures can bolster the security against SAT attacks, making decryption within a realistic time-frame significantly more challenging. Assuming a locked chip allows infinite attempts of input combinations, no logic locking scheme is perfectly impervious to SAT-based decryption, and logic locking techniques are therefore gauged by the time needed to reveal the correct key.

B. Structural Attacks

Structural attacks are non-invasive attacks that aim to find the locking key by identifying added locking logic through analysis of circuit structure. Unlike the SAT-based attack, structural attacks do not require an oracle, though they still require the locked netlist. Some structural attacks use fault analysis [13], pattern recognition machine learning [14], or statistical analysis [15] to identify designer or EDA tool intent and thereby reveal locking structures.

C. Side-Channel Attack

By-products of circuit operation such as power consumption, voltage drop, and electromagnetic radiation can be used to glean the locking key [25] – such an analysis is referred to as a side channel attack. Consequently, any key that is *electrically* applied to a logic-locked circuit is at risk of side-channel attacks [1], [7], irrespective of whether the key is stored in a non-volatile manner. This vulnerability is of particular concern for CMOS logic-locked circuits and polymorphic gates designed with non-volatile technologies [8]–[10].

For instance, in the context of non-volatile memristors storing the locking key as described in [19], side-channel attacks can expose the key during its electrical readout. Similarly, despite the uniform electrical power consumption across various polarities of ASL nanomagnets [20], [21], the ASL clock connections can be utilized to electrically measure the non-local resistance between adjacent nanomagnets [26]. Specifically, the relative magnetic alignment of two ASL nanomagnets influences their non-local resistance, presenting a potential electrical side-channel that could potentially reveal the nanomagnet polarities storing the locking key.

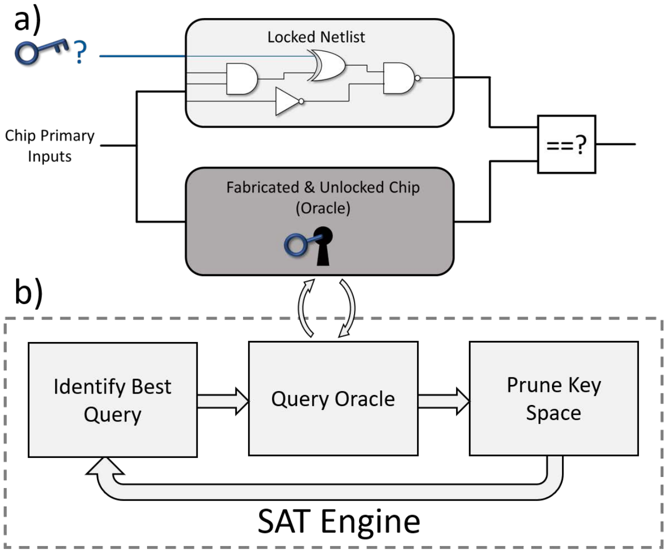


Fig. 3. SAT attack model. a) The attacker has access to the locked netlist and an unlocked fabricated chip – the oracle. The attacker strategically queries the oracle to prune the number of potential locking keys. For example, in the illustrated circuit, a primary input query of 110 will sensitize the key bit to the output to be discovered by the attacker. b) A SAT engine is used to find the best queries to ask the oracle in order to find the correct key in the shortest possible amount of time.

D. Material Delayering

Delayering, the process of removing material layers from an IC, plays a pivotal role in invasive reverse engineering: it permits the physical imaging of a locked layout or the direct probing of a locking key stored in the memory unit. State-of-the-art reverse engineering facilities employ various methods, such as etching and polishing, to access vital material layers that are usually inaccessible [27]. This attack is frequently employed to enable the imaging attacks detailed in Sections II-E through II-G.

E. Imaging Attack on Electrical Properties & Behavior

Various imaging techniques can be employed to probe the electrical characteristics of a circuit, and therefore the locking key. For example, advanced optical instruments are capable of examining an IC and tracking the electrical signals passing through specific nodes over time [28]. In a similar vein, Rahman *et al.*, building on the methodology outlined in [28], utilized electro-optical frequency mapping (EOFM) to create an activity map for a logic-locked design implemented on an FPGA. This map was then used to reveal the key [4]. It's important to note that any logic-locked system with an electrical signature of the locking key is susceptible to electrical imaging attacks.

Imaging techniques can expose the locking key in the case of logic-locked CMOS designs [1], [7] and polymorphic gates that incorporate non-volatile components [8]–[10] if the key is electrically applied to the locked gates. Similarly, the locking key stored in non-volatile memristors [19] can be revealed when used electrically for logic operations. In short, no logic locking scheme that involves the electrical transportation or utilization of the key is immune to imaging attacks, irrespective of the use of non-volatile elements.

F. Imaging Attack on Magnetic Properties & Behavior

Magnetic attacks have not previously received significant attention as conventional computing systems do not incorporate magnetism in a manner that makes them vulnerable to such attacks. However, the secure system introduced here relies on magnetism, necessitating a careful evaluation of the potential for magnetic imaging attacks. These magnetic probing techniques can be categorized into two main groups: (i) those that detect stray magnetic fields, and (ii) those that leverage the interactions between electrons, X-rays, or light and the magnetization of the sample.

The first category of imaging methods includes magnetic force microscopy (MFM), where the stray magnetic field from the sample interacts with an oscillating magnetic tip, inducing changes in frequency and phase. The second category, exemplified by the magneto-optic Kerr effect (MOKE), relies on encoded magnetic information in the light reflected from the sample's surface. In both techniques, the probing process can be obstructed by a thick, opaque shield. Nevertheless, the removal of this shield overcomes the protection against imaging; this approach can be utilized to expose the locking key stored within the polymorphic ASL gates described in [20].

G. Imaging Attack on Physical Layout

Both the physical layout and the locking key are required to successfully counterfeit a logic-locked circuit; the physical layout is also needed to create the netlist used in launching the SAT attack. Imaging attacks can uncover the layout through imaging techniques such as scanning electron microscopy [29].

H. Untrusted Foundry Attacks

To produce the locked IC, untrusted foundries require access to the physical layout. These foundries possess sophisticated tools capable of executing SAT-based, structural, or physical attacks to obtain the locking key, rendering them a particularly dangerous threat against the locked chip.

III. Strain-Protected Nanomagnet Logic Locking

Nanomagnet logic is characterized by its energy-efficient nature, performing logical operations by leveraging dipolar coupling between nanomagnets [30]. In this research, we propose the concept of polymorphism within NML to establish a robust logic locking approach, newly resilient all known physical attacks while retaining the security against SAT-based attacks provided by conventional techniques. The non-volatility of nanomagnets with strain-induced perpendicular magnetic anisotropy (PMA) presents a secure memory solution, effectively shielding the locking key from electrical or magnetic imaging, thereby overcoming a fundamental challenge in logic locking. Additionally, we employ fuses in the spin-orbit torque (SOT) programming path to prevent any unauthorized tampering with the non-volatile memory where the key is securely stored. This novel approach significantly enhances the appeal of NML, which has traditionally faced limitations related to operational speed [31].

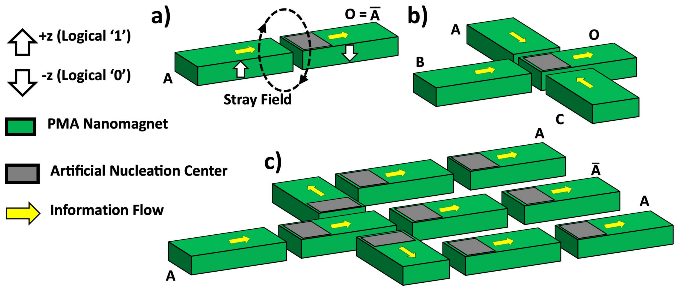


Fig. 4. (a) An inverter implemented using NML, with input denoted as A and output O. (b) A three-input NML minority gate producing an output labeled as O based on the inputs A, B, and C. (c) NML signals are propagated to various connected components via fan-out.

Here, we propose a method involving strain to safeguard nanomagnets against imaging and delayering; this method can be applied to both NML and ASL polymorphic gates [20] to protect against magnetic imaging, as discussed in Section II-F. A similar strategy could also be explored with recently proposed nanomagnetic computing devices such as the magnetoelectric spin-orbit (MESO) logic [32]. However, it is important to note that ASL and MESO gates may still exhibit vulnerability to spin-based electrical side-channel analyses, as detailed in Section II-C. In contrast, NML distinguishes itself from ASL and MESO by not requiring electrical interfaces to nanomagnets during computation, thus mitigating the risk of electrical side-channel attacks aimed at revealing the key.

A. Background on Nanomagnet Logic

NML uses the magnetic orientation of bistable nanomagnets to represent binary logic values. Nanomagnets may be fabricated with either in-plane magnetic anisotropy or PMA, although this work focuses on PMA due to the security advantages outlined in Section III-D. In NML, binary '0' and '1' signals are represented by the bistable magnetic polarity. NML logic is conducted through the dipolar coupling between adjacent nanomagnets. For instance, in the NML inverter gate depicted in Fig. 4(a), as the artificial nucleation center (ANC) of the output nanomagnet has reduced anisotropy, it is susceptible to the stray magnetic field of the input nanomagnet. The ANC therefore switches state to be opposite that of the input nanomagnet. Subsequently, the magnetic orientation change within the ANC propagates through the rest of the output nanomagnet via magnetic domain wall motion.

Fig. 4(b) shows a three-input NML minority gate. As indicated in Table I, the output nanomagnet's magnetization is the inverse of the majority of the input nanomagnets. Fan-out within NML circuits can be accomplished using an arrangement of nanomagnets akin to the configuration shown in Fig. 4(c). The operational speed of NML circuits is contingent upon the velocity at which domain walls move through the magnets, as discussed in [31].

Both the switching at the ANC and the propagation of domain walls are facilitated by an alternating z-directed clocking magnetic field. This clocking method, when coupled with PMA, serves to mitigate the impact of errors [33] that can affect in-plane NML due to imprecise fabrication [34]. While various other clocking techniques have been proposed that offer energy efficiency advantages, they involve electrical contacts to nanomagnets similar to ASL and are therefore vulnerable to side-channel attacks (as described in Section II-C). This paper thus exclusively explores clocking through the application of an alternating magnetic field.

B. Logic Locking with Nanomagnet Logic Polymorphism

We propose a logic locking concept based on polymorphic NML gates. Polymorphism within NML is achieved by configuring the polarity of specific input nanomagnets using bits from the locking key. The fan-in and fan-out nanomagnets contain ANCs to execute and chain logical operations. In contrast, ANC-free, hard-coded non-volatile nanomagnets store the key bits throughout the chip's operational life.

Fig. 5 illustrates a polymorphic adaptation of the three-input minority gate depicted in Fig. 4(b), with input C serving as the hard-coded nanomagnet. Programming the polarity of input C to -z(+z)-direction results in the polymorphic gate executing the logical NAND (NOR) operation on inputs A and B, and then propagating the output to nanomagnet O. Moreover, an AND/OR polymorphic gate can be achieved by concatenating the inverter from 4(a) to the output of the NAND/NOR gate. NAND or NOR gates in the netlist may therefore be replaced with polymorphic NAND/NOR gates with no area, energy, or delay overhead, a unique feature of NML.

While NAND/NOR polymorphism is the cheapest way to lock NML, any other logic locking technique is applicable to NML due to the fact that NML is logically complete. As shown in Fig. 6(a), a key bit may be used as a logical input to any gate. This enables the NML polymorphic BUF/INV gate of 6(b), which is equivalent to the XOR insertion commonly used in CMOS logic locking [1]; the relative gate overhead of various gate implementations is analyzed in Section VI-B. It should also be noted that as novel logic locking approaches are developed to thwart constantly evolving SAT-based or structural attacks, they can be directly adapted to NML to exploit the unique physical security of NML.

TABLE I
NML NAND/NOR POLYMORPHISM

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

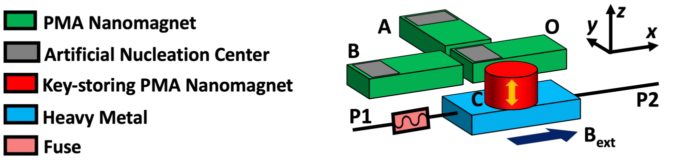


Fig. 5. A polymorphic NAND/NOR gate comprising input nanomagnets A and B, output nanomagnet O, and a programmable non-volatile nanomagnet C, storing a single bit of the locking key. The locking key bit is programmed into nanomagnet C via SOT with a fuse on the programming path to prevent tampering.

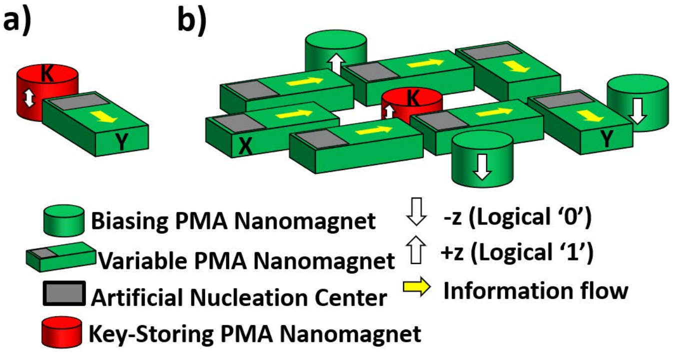


Fig. 6. (a) Key bit logical input. (b) A polymorphic BUF/INV gate comprising input nanomagnet X, output nanomagnet Y, and a programmable non-volatile nanomagnet K that stores a single bit of the locking key. This gate computes $Y = XOR(X, K)$. Inserting this polymorphic gate in NML is therefore logically equivalent to XOR gate insertion in CMOS.

C. Spin-Orbit Torque Programming of Nanomagnet Keys

Nanomagnets can be hard-coded to store the key bits using SOT. In the polymorphic gate shown in Fig. 5, the hard-coded nanomagnet is situated above a heavy metal layer, linked to the electrical current path P1-P2 through a fuse that acts as a wire during programming. The IP designer can configure the nanomagnets by passing an electrical current through the heavy metal layer. SOT current in the $+x$ $(-x)$ direction causes spins to orient in the $+y$ $(-y)$ direction [35]. The current is progressively increased until the fuse burns out, breaking the electrical path and halting current flow. Throughout this process, an applied $+x$-directed magnetization prompts the nanomagnet's polarity to settle in the $+z$ $(-z)$ orientation once the current is withdrawn [35]. This protocol guards against unauthorized parties attempting to reprogram the locking key, preventing the chip from being compromised as well as non-invasive attacks reliant on key modification. Consequently, the fixed, key-storing nanomagnets remain robust against tampering.

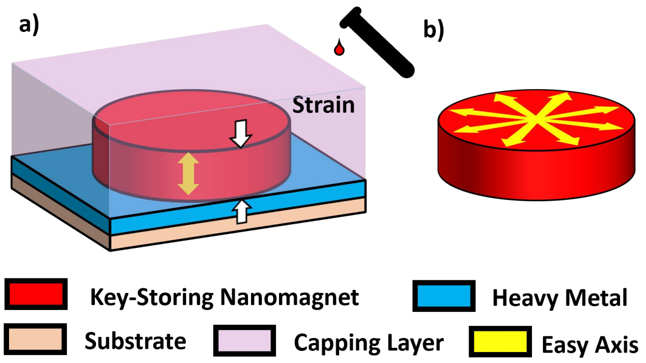


Fig. 7. (a) The strain caused by the capping layer and substrate induces PMA in the nanomagnet. (b) The substrate and/or capping layer is etched, removing strain, resulting in isotropic in-plane easy magnetization orientation. The arrows indicate the direction of the easy axes.

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

To thwart attempts at uncovering the locking key through proximity or visibility-based imaging techniques, we employ an opaque "strain shield" that envelops the nanomagnets. This shield induces anisotropy in the nanomagnets, causing the self-destruction of the hard-coded key bits when delayering is attempted. Our proposal involves inducing the PMA of the hard-coded nanomagnets by means of strain originating from the materials surrounding them, including the substrate, heavy metal, and capping layer, as illustrated in Fig. 7. Experimental evidence has shown that interfacial anisotropy can emerge in magnetic/non-magnetic multilayers due to strain, and the strength of this anisotropy is dependent on the thickness of the non-magnetic layer [36].

In the event of an attacker's attempt to etch the strain shield encompassing a hard-coded nanomagnet, the magnetic polarity will transition from PMA to isotropic in-plane easy magnetization, effectively erasing the locking key bit stored within the nanomagnet. Additionally, it has been observed that etching the surrounding layer causes degradation in magnetic properties long before reaching the magnet [37]. By altering the anisotropy in this manner, delayering of the strain shield from any direction will result in the destruction of the locking key, effectively preventing the key's discovery through magnetic imaging attacks.

E. Overview of Complete Secure System

Fig. 8 presents an illustration of a secured circuit, using the ISCAS'85 benchmark c17 as an example, to showcase the comprehensive security concept [38]. The figure depicts six hard-coded nanomagnets, where locking key bits are written via SOT currents through the heavy metal regions, configuring each minority gate to operate as either a NAND or NOR function. It should mentioned that, as described in Section III-B, NML is not limited to NAND/NOR polymorphism and is amenable to other logic locking techniques and structures including XOR [1], SARLock [11], redaction [39], TTLock [16], and any future techniques as hardware security continues to mature. To ensure that any attempts to delayer near the hard-coded nanomagnets trigger the self-destruction of the key bits, the entire circuit is enveloped by a strain shield. Additionally, while the passive self-destruction scheme is sufficient for physical security, active key-destruction mechanisms (akin to [16], [40]) may also be incorporated to increase SAT-based attack cost.

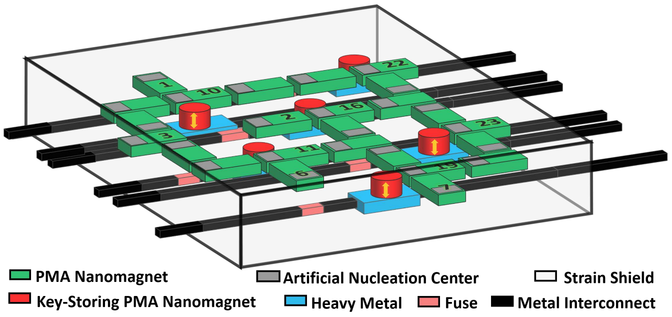


Fig. 8. A physically secure logic-locked c17 circuit including a designated programming port for IP owners. The numbered nanomagnets correspond with the c17 net numbering.

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

The combination of NML gate polymorphism and the strain-mediated self-destruction mechanism serves as a robust defense for the proposed logic locking scheme, effectively safeguarding it against physical, SAT-based, and structural attacks aimed at revealing the locking key. While adversaries may uncover the physical layout of a logic-locked design, the locking key must remain hidden to prevent unauthorized replication and tampering of unlocked ICs.

A. Satisfiablity Attacks

As explained in Section III-B, any locking technique developed for CMOS (*e.g.*, XOR insertion [1], LUT insertion [41], redaction [39], etc.) may be directly adapted to NML; as NML is logically complete, the two logic families are equivalent from the perspective of SAT-based attacks [2], [5]. NML can therefore retain identical security against SAT-based attacks as CMOS.

As NAND/NOR polymorphism comes at no overhead cost in NML (Sections III-B and VI-B), we explored the strength of the NAND/NOR polymorphism by conducting SAT attacks on ISCAS'85 benchmark circuits [38] that were locked with polymorphic NAND/NOR gates. As described in more detail in Supplementary Note 1, Supplementary Figure 1, and Supplementary Table I, circuits c2670, c3540, c5315, c6288, and c7552 successfully resisted a sustained 48-hour SAT attack performed with the attack engine of Subramanyan *et al.* [2]. This resistance is similar to that provided by XOR-insertion, demonstrating the potential for NAND/NOR polymorphism to complement traditional locking techniques and help minimize the overhead cost of using heterogeneous technologies.

B. Structural Attacks

As described in Section IV-A, as NML is logically complete, there is no difference between NML and CMOS from the

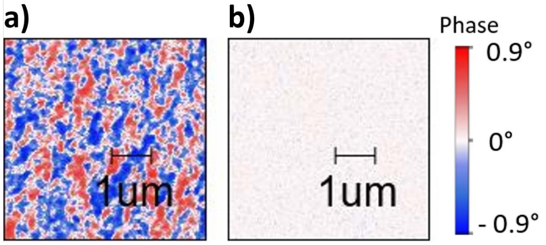


Fig. 9. MFM was employed to image in-plane magnetic domains, with two scenarios depicted: (a) without a 100 nm capping layer and (b) with the capping layer. Notably, the introduction of the capping layer led to the disappearance of phase contrast, leaving behind a signal characterized by random noise.

perspective of a structural attack [13]–[15] – which only operates on gate-level information. NML can therefore achieve, at minimum, the same level of security against structural attacks as CMOS by mimicking security-aware post-synthesis gate choices made for CMOS. Further evaluation of the security against structural attacks is beyond the scope of this work.

C. Side-Channel Attack

Upon programming the hard-coded nanomagnets and burning the fuses, the unlocked NML circuits that are made available to the public include no electrical activity. As the key is never transported or converted to an electrical signal, the locking key is completely devoid of any electrical signature. Consequently, there are no available side-channels from which to launch an attack aimed at revealing the key.

D. Material Delayering

As outlined in Section III-D, any effort to remove the strain shield encompassing the nanomagnets induces a transition in anisotropy from PMA to an in-plane easy magnetization state. This shift leads to a random in-plane magnetization orientation, thereby destroying the locking key. Moreover, the etching procedure deteriorates the magnetic characteristics of the nanomagnets, ultimately culminating in the total destruction of the IC.

E. Imaging Attack on Electrical Properties & Behavior

Imaging attacks targeting electrical properties or behavior are infeasible in the context of NML because NML operates based on magnetic interactions rather than electrical interactions.

F. Imaging Attack on Magnetic Properties & Behavior

Efforts to delayer the system would result in the destruction of the locking keys contained within the nanomagnets. Therefore, any attempt to execute an imaging attack on the magnetic properties or behavior must be conducted through the strain shield surrounding the nanomagnets. However, detecting magnetization via stray magnetic fields demands close proximity to the nanomagnet, and electron, X-ray, or optical imaging methods require a transparent path between the source and the nanomagnet.

To illustrate the security of strain-protected logic locking with NML against magnetic imaging attacks, MFM was employed to image magnetic domains in a Co(15nm)/Ti(5nm)/Substrate film. An extra 100 nm Ti capping layer was deposited atop half of the film. When MFM was used to image the Co without the capping layer, in-plane magnetic domains were clearly observable, as depicted in Fig. 9(a). As illustrated in Fig. 9(b), when scanning over the region with the capping layer, the phase contrast vanished, indicating that the MFM became unable to discern the magnetization directions, illustrating that when the capping is present, magnetic imaging cannot reveal the perpendicularly stored magnetic state. In-plane domains revealed during delayering will have states that are independent from the information formerly stored in the nanomagnets. Additionally, this experiment demonstrates that NML will not inductively interfere with nearby routing or CMOS logic, which could otherwise be used to launch a side channel attack on the NML.

G. Imaging Attack on Physical Layout

After material delayering, a reverse engineer can employ methods like scanning electron microscopy or other probing techniques to capture the physical layout of the logic-locked design. Nevertheless, it is vital to note that this locked physical layout remains secure and resistant to unauthorized reproduction due to the security of the locking key, which in the proposed scheme is robust against all known attacks.

H. Untrusted Foundry Attacks

During the manufacturing process, the third-party foundry is furnished with both the physical layout and the netlist of the logic-locked design. However, it is crucial to emphasize that counterfeiting the functional design remains an insurmountable challenge in the absence of access to the secure locking key.

I. Complete Security

Logic locking with NML is therefore secure against the known physical attacks and can adapt all locking techniques from CMOS for security against the known SAT-based and structural attacks. The programmability and logical completeness of NML enable the use of existing locking techniques to secure a chip against SAT-based and structural attacks, while the strain-induced PMA ensures the physical security of the key. Attempts to reveal the key by probing the magnetizations of the key-storing nanomagnets are thwarted by the opaqueness and thickness of the strain-inducing capping layer, the delayering of which causes self-destruction of the locking key through strain relaxation.

The unique physical security provided by NML thus results from the fact that the ability of a nanomagnet to represent a bit of information is entirely dependent on the presence of a separate material layer which can be repurposed to block imaging attacks. To the best of the authors' knowledge, this information representation dependence does not exist in non-magnetic technologies. For instance, in CMOS, information is represented as the presence or absence of electrical charge on a wire. As the presence or absence of a material layer will not change the fundamental nature of a wire to store charge, there is high chance that even active shielding mechanisms in CMOS may be cleverly delayered to reveal the still-present key through imaging. This is not the case in NML, as delayering of the shield will immediately, passively, and intrinsically destroy the information storage of the nanomagnet, thereby destroying the key information itself. By exploiting the unique physics of nanomagnet logic and strain-dependent magnetic anisotropy, the proposed method provides an intriguing solution to secure an locking key from physical attacks, opening new pathways for logic locking.

V. Secure Hybrid CMOS/NML Circuits

While strain-protected NML offers complete hardware security against the known physical, SAT-based, and structural attacks, the development of an exclusively NML-based computing system faces obstacles due to NML's subpar speed and reliability, as evidenced by [42]–[45]. To address this, we propose the integration of logic-locked NML islands within a predominantly CMOS-based computing system, aiming to leverage the security benefits of NML while maintaining the speed and reliability characteristic of CMOS. This approach is depicted in Fig. 10.

It should be noted that the hybrid logic locking methodology presented in the remainder of this work is technology agnostic and may be equally applied to any physically secure emerging technology. Though the strain-protected NML approach described above is the first such physically secure emerging technology, future technologies may be able to similarly leverage the secure hybrid approach described below.

A. Nanomagnet Logic Islands

As described in Section III-A, the design of large-scale computing systems solely comprising NML faces challenges intrinsic to the magnetic phenomena [44], [46]:

- the clock speed is constrained by the inherently slow nature of magnetic switching and magnetic domain wall motion and
- thermal noise, misalignment, and fabrication imperfections result in switching errors reducing circuit reliability.

Hence, to realize secure *large-scale* computing systems, we advocate for hybrid systems in which one or more NML circuits is integrated within a predominantly CMOS-based computing system. NML can be integrated with CMOS in a manner analogous to MRAM [47], which has similar materials stacks and has recently been integrated into competitive CMOS processes. These NML islands hide the system's functionality, as the locking key bits, stored in nanomagnets within these islands, substantially influence the system's logical behavior. Consequently, the design of hybrid CMOS/NML systems involves a balance between security and computational efficiency, which governs the optimal number, size, and placement of NML islands within the CMOS system.

In the hybrid system, well-chosen subcircuits within a normally-CMOS netlist are chosen to be fabricated instead with logic-locked NML. Ideally, these chosen subcircuits should have minimal effect on timing, but they should be on critical datapaths such that locking a few of them results in locking of the whole chip. Two categories of subcircuits typically fulfill these requirements: combinational subcircuits that are not part of the critical timing path and deeply pipelined sequential subcircuits. As detailed in Sections V-B and V-C, NML can function as either combinational or sequential logic, permitting both structures to be locked with physically-secure NML.

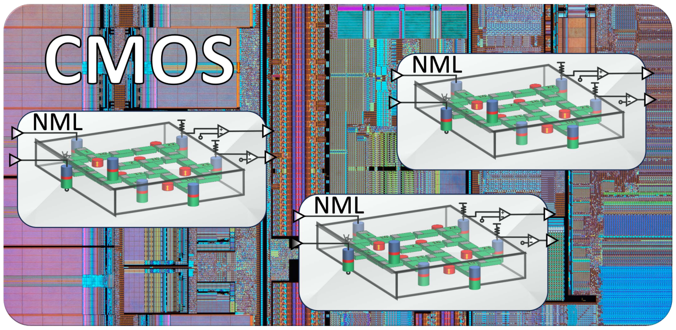


Fig. 10. Proposed hybrid CMOS/NML system. While CMOS demonstrates superior speed and robustness compared to NML, it remains vulnerable to physical attacks. This concept suggests strategically substituting select CMOS blocks with secure NML blocks to bolster security with minimal impact on system efficiency.

As increased size and complexity of an NML circuit increases NML delay and soft error rate, smaller blocks should be chosen to implement with logic-locked NML islands in order to minimize overhead. The optimization of efficient and secure hybrid CMOS/NML systems entails intricate tradeoffs in device/system co-design that involve the efficiency and security of NML islands, contingent on their size, as well as co-design considerations related to the optimal placement of these islands.

B. Inputs to NML Islands

Inputs to the NML islands can be written using spin-transfer torque, converting electrical inputs into magnetic orientation. As depicted on the left side of Fig. 11, this process involves applying CMOS vdd across a magnetic tunnel junction (MTJ) to write the magnetic orientation [47]. The interplay of the current direction within the device and the magnetization of the fixed ferromagnet layer (shown in blue) determines the resulting orientation of the free ferromagnet layer (depicted in green). Dipolar coupling from the MTJ free layer governs the magnetization of the NML input magnet, facilitating the propagation of magnetic signals within the NML circuit.

The NML input method is versatile, suitable for deployment in both combinational and sequential logic circuits, owing to its capacity to clock the input current through a tri-state buffer. This method not only conserves energy but also avoids the occurrence of glitches. Consequently, NML islands can function as replacements for both combinational and sequential blocks. In combinational blocks, the NML's propagation delay is directly related to the clocking magnetic field's period. In

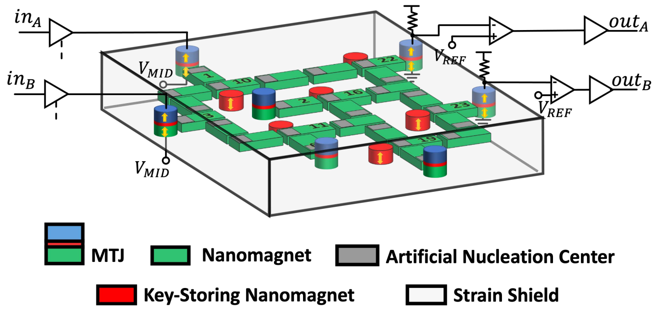


Fig. 11. Input signals from the conventional CMOS system are transmitted to the secure NML logic circuit through spin-transfer torque on the left. On the right side, output signals from the NML system are directed back to the CMOS system via the combination of an MTJ and a voltage divider.

sequential circuits, the NML's clocking magnetic field must be synchronized with the overall CMOS system clock.

C. Outputs from NML Islands

The NML island outputs can be accessed using MTJs, which exhibit resistance variations based on the orientation of the free-layer magnetization. As depicted in the right side of Fig. 11, this resistance can be detected using a voltage divider, and if required, a thresholding amplifier can be employed for level-shifting purposes. Energy efficiency can be achieved by sending a read current through the device only when results are ready for retrieval.

Much like the NML input circuit, the NML output circuit is versatile and can work with both combinational and sequential logic. In combinational blocks, a continuous read voltage application produces an output voltage that constantly reflects the output nanomagnet state, and a small read voltage applied only after the output has stabilized would reduce power consumption. In sequential blocks, a clocked read voltage is utilized, and a latch at the output maintains the signal between read cycles. In both scenarios, the NML island seamlessly integrates into a conventional CMOS system with minimal read-out circuitry, ensuring proper functionality.

VI. Security & Efficiency of Hybrid CMOS/NML

Incorporating secure NML into a conventional CMOS system necessitates a co-design approach that simultaneously addresses timing, overhead, robustness, and security aspects.

A. Timing Considerations

The hybrid CMOS/NML approach integrates the security advantages of strain-protected NML with the speed and reliability of CMOS. In terms of timing, optimal combinational blocks for NML security islands are those characterized by substantial parallelism, enabling the computation of critical functions without extensive gate depth. These functions exert minimal influence on the overall system timing, making them well-suited for NML security islands. In the context of NML, combinational propagation delay is determined by the maximum circuit depth (measured in nanomagnets) multiplied by the clock frequency, which is constrained by the propagation speed of magnetic domain walls.

In the case of pipelined sequential blocks, the NML circuits exhibit natural pipelining due to the alternating magnetic clocking field necessary for NML signal propagation. Consequently, these blocks can achieve substantial parallelism and high throughput, although they may encounter noticeable latencies.

In some circuit architectures, key value can affect output arrival time; this is a potential exploit if the output nanomagnet state is visible to the attacker. For these architectures, the MTJ read voltage should only be applied after the output is guaranteed to have settled as described in Section V-C, thereby ensuring that these possible timing deltas are not available to the physically insecure electrical sub-system.

B. Logic Locking Overhead

The most efficient gate implementations in NML differ slightly from those in CMOS, as depicted in Supplementary Table II. For instance, whereas a minority gate (*i.e.*, polymorphic NAND/NOR) costs twelve transistors in CMOS (the equivalent of three NAND2 gates), NAND/NOR replacement in NML is cost-free as all NAND and NOR gates are already built from minority gates. NAND/NOR polymorphism, while not seriously explored for CMOS locking, should therefore be emphasized in NML locking. Additionally, as NML is non-volatile, key-bits are stored in key-storing nanomagnets that do not require non-local nonvolatile memory for key storage; in contrast, CMOS approaches require significant memory use for key storage. XOR gates in NML may be constructed from three minority gates, as depicted in Fig. 6, or using twelve transistors in CMOS. As there is no known tri-state functionality in NML, NML cannot take advantage of the conventional optimizations for multiplexers (MUXs) and lookup tables (LUTs), which use full or half transmission gates (TGs), respectively. For all other logic, NML and CMOS are equivalent in terms of gate overhead.

C. Power, Performance, & Area Overhead

As summarized in Section IV-I, NML provides physical security not available in any other technology. However, as NML has reduced efficiency relative to CMOS, NML should be integrated into large-scale CMOS systems with small NML islands while maintaining security against SAT-based attacks.

As summarized in Table II, NML [48] has high overhead compared with modern CMOS [49]. Note that while NML switching is lower energy than CMOS by two orders of magnitude (including losses from clocking circuitry) [48],

TABLE II
PPA Overhead of a Single Gate and Switching Event

	Area (μm^2)	Energy (aJ)	Delay (ps)	EDP (aJps)
NML [48] (2014)	0.04	2.8	20,000	56,000
CMOS [49] (proj. 2025)	0.034	490	0.96	470

the low gate clock frequency of NML (50 MHz) seriously degrades performance, leading to an energy-delay-product (EDP) increase of 100x.

Programming, island input and readout, and island replication incur additional overhead. For key programming, each key bit requires a fuse and a wire. Programming paths should be connected to a memory-addressable current driver to minimize overhead. Each island input requires a tri-state buffer consuming conventional STT-MRAM write energy as low as 12 μJ [50], and each island output requires a tri-state buffer and sense-amp. Island replication consumes triple (or quintuple for 5-1 replication) the area and energy of a single island without additional delay. The CMOS voter is a single majority gate. Input, output, and voting logic consume negligible delay compared with the NML.

D. Robustness Considerations

The non-negligible error rate of NML presents challenges for robustness. To mitigate against soft NML errors, redundant error-correction schemes should be employed. Creating error correcting codes in NML requires additional NML hardware, and information about the locking key may be revealed in the layout of the additional hardware. However, if NML islands are duplicated to correct errors, no new information about the locking key will be included in the chip layout. Therefore, an error correction scheme where an odd number of duplicated NML islands feed into a shared CMOS voter will be the most secure method for mitigating the soft error rate of NML.

Applying a soft error limit during island assignment applies a direct constraint on NML island size. The probability of computing a correct output in an NML island is a function of the probability that each gate computes the correct output along that data path according to:

$$EC = 1 - (1 - EG)^{D} = D * EG + o(EG^{2}),$$

where EC is the circuit error rate, EG is the gate error rate of NML, and D is the number of NML gates in the fan-in cone of the output of the data path. The reliability of these circuits may be improved by replicating islands of the secure technology and passing their outputs through a voter to correct errors that may occur in one of the islands. Reliability of this scheme follows:

$$EC \approx (D * EG)^{\lceil V/2 \rceil},$$

where V is the degree of the V-to-one voter. Therefore, for a target error rate, EC, we get:

$$D < \frac{EC^{\frac{1}{\lceil V/2 \rceil}}}{EG},$$

bounding the size of the island data path, D. For the case of NML, with gate error rate, EG, of 10^{-8} [51] and a target circuit error rate, EC, of 10^{-12}, with a three-to-one voter, data path size should be limited to 100 gates, and with a five-to-one voter, data path size should be limited to 10,000 gates.

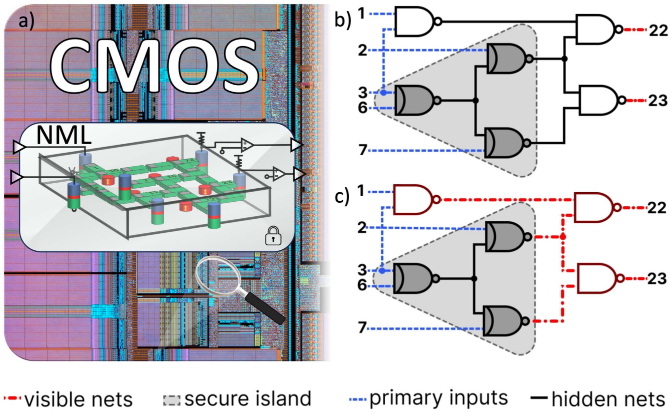


Fig. 12. (a) A key bit-storing NML island locks a circuit region within a larger CMOS system and secures the bit stream from invasive attacks. Though the CMOS/NML interface does not open additional physical exploits, it enables physically-enhanced SAT-based attacks that probe the CMOS logic to gain insight into the functionality of the islands. (b) Conventional SAT attack model. Primary inputs of the oracle are controllable and primary outputs are observable. (c) Physically-enhanced SAT attack model. Primary inputs are controllable, and all nets not hidden within the physically secure islands are observable.

We demonstrate in Section VII that 10,000 gates is sufficient to secure against both conventional and future physically-enhanced SAT attack models.

E. Physical Security

Whereas Section IV proved that strain-protected NML is secure against all known physical attacks, the inclusion of the interface CMOS circuitry may open vulnerabilities in the hybrid CMOS/NML methodology. At the inputs of secure NML islands, the only security concern lies in the interface between the physically insecure CMOS environment and the secure NML environment. Given that the ANCs and the clocking field ensure that data cannot flow in a reverse direction towards the circuit inputs, the introduction of a buffer magnet after the inputs prevents any potential key information from being detectable at the input interface. The electrical interface will therefore only contain information about the input and output signals to that island. Thus, even if an attacker has visibility into the CMOS portion of the chip, no new information about the locking key will be revealed through imaging of the NML/CMOS interfaces.

F. Security Against SAT-Based Attacks

As the polymorphism of an NML island is limited by the size of the island, and thereby its reliability, security of the hybrid NML/CMOS logic locking scheme against SAT-based attacks must be carefully evaluated. Additionally, as it is possible to image electrical signals in CMOS, a realistic attack model must account for the possibility that an attacker can image the CMOS portion of the chip to glean information about the key stored in the physically secure emerging technology. As depicted in Fig. 12(a), this physically-enhanced SAT attack model assumes that the attacker has visibility into the CMOS portion of the chip. The attacker is therefore able to observe the effect of the key in CMOS nets downstream from the emerging technology island. In order to sensitize the key to the visible nets, the proper combination of primary inputs

This article has been accepted for publication in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. This is the author's version which has not been fully edi
content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2024.3434362

must be stimulated; finding this combination is NP-hard, still requiring a SAT engine to attack.

In order to benchmark hybrid logic locking against SAT-based attacks, we must therefore evaluate a physically-enhanced variation of the SAT attack in which all nets implemented in CMOS are visible to the attacker. As illustrated in the *conventional* SAT attack model of Fig. 12(b), the SAT engine can only stimulate primary inputs and observe primary outputs of the oracle. In contrast, for the *physically-enhanced* SAT attack model of Fig. 12(c), all nets not completely embedded within a single secure island are treated as primary outputs that the attacker can observe. The SAT engine can then use the information from the visible internal nets to generate the most efficient oracle queries, as in the conventional attack described in Section II-A. As the physically-enhanced attack must match the behavior of all of the visible internal nets in addition to the primary outputs, in some cases, the physically enhanced attack can be slower than the conventional attack – wherein the state of these internal nets are treated as don't-cares. As described in Section VII, our locked hybrid circuits are therefore evaluated with *both* the conventional and physically-enhanced SAT attacks.

As imaging the oracle takes considerably longer than simply querying the chip as in the conventional SAT attack, it is expected that the physically-enhanced attack model incurs additional time overhead. This overhead was not incorporated in our results, and would significantly increase the SAT attack solve times. These solve times are therefore a lower bound, and the physically secure logic locking approach actually provides more security against SAT-based attacks than is indicated by our SAT attack results.

G. Security Against Structural Attacks

Unlike SAT attacks, structural attacks are oracle-less and would therefore not be able to take advantage of the electrical imaging that enables the physically-enhanced attack described in Section VI-F. The only new source of designer intent presented by the hybrid locked system beyond the conventionally available intent addressed in Section IV-B is the choice of whether to implement a specific gate in CMOS or the emerging technology. This information has not been previously available to attackers, and structural attacks have therefore not been developed to account for it; benchmarking the hybrid logic locking system against structural attacks – and developing strategies to mitigate new vulnerabilities that might arise – is therefore reserved for future work, if such attacks become available.

VII. Security of Hybrid CMOS/NML Logic-Locked Circuits against SAT Attacks

To estimate the security of the hybrid CMOS/NML logic locking scheme against SAT attacks, we locked the ISCAS'85 suite of benchmark circuits [38] with NAND/NOR polymorphism and various sizes and quantities of islands. As the physically-enhanced SAT attack can be slower than the conventional SAT attack in some cases (see Section VI-F), we attacked the locked circuits with both attack models. As NML is not limited to NAND/NOR polymorphism for locking, the results described in this section paint a conservative picture of the ability to secure hybrid CMOS/emerging technology systems against traditional and physically-enhanced SAT attacks. Security can be strengthened by using advanced locking techniques developed for CMOS or by modifying locking algorithms that resemble the concept of islands (*e.g.*, maximum fanout free cones [17] or hardware redaction [39]). Furthermore, the results presented in this section are not specific to NML and are directly representative of *any* hybrid CMOS/physically secure emerging technology system.

As described in Section VI-D, islands should be less than 10,000 gates deep in order to match a target error rate of 10^{-12}; we demonstrate below that this depth is sufficient to successfully secure the ISCAS'85 benchmark circuits. The netlists of the benchmark circuits were locked through a naïve island selection algorithm that was used to generate a large number of locked versions of each ISCAS'85 benchmark circuit. The island selection algorithm randomly chooses a seed gate and greedily adds more gates to the island in an attempt to minimize the number of visible nets emerging from the island; more details are provided in Supplementary Note 2 and Algorithms 1-4 in the Supplementary Information. Every NAND and NOR gate within the island was replaced by a polymorphic NAND/NOR gate and key bit.

Benchmark circuits were attacked with both the conventional and physically-enhanced attack models, as described in Sections II-A using an Intel i7-7820X CPU, IV-A, and VI-F. All locked benchmark circuits are available at https://www.utdallas.edu/~joseph.friedman/. By including the physically-enhanced attack model – the most sophisticated to date – we ensure that a locked circuit is able to thwart a physically-enhanced attack that is above and beyond the conventional standard for security against SAT attacks.

A. Security Against Conventional SAT Attack

A large number of locked benchmark circuits successfully resisted a 48-hour conventional SAT attack. In order to consistently secure against the *conventional* SAT attack, islands did not need to be bigger than 500 gates. As depicted in Fig. 13, five of the seven large ISCAS'85 combinational benchmarks were consistently secured against 48-hour conventional attacks, with c1908 resisting an attack for 600 seconds and c5315 resisting for 19 hours.

Compared with the attack time when every NAND, NOR, AND, and OR gate is locked shown in Supplementary Table 1, the attack time achieved by the hybrid logic locking technique is over twice as long for circuits c1355 and c1908. As, relative to the conventional SAT attack, the only difference between these locked circuits is that fewer gates are locked in the hybrid scheme, there exist situations where locking well-chosen portions of logic can provide superior security than if all of the gates are locked. The hybrid locked circuits perform similarly to conventional locking schemes in CMOS with a large proportion of 48-hour timeouts on the larger benchmark

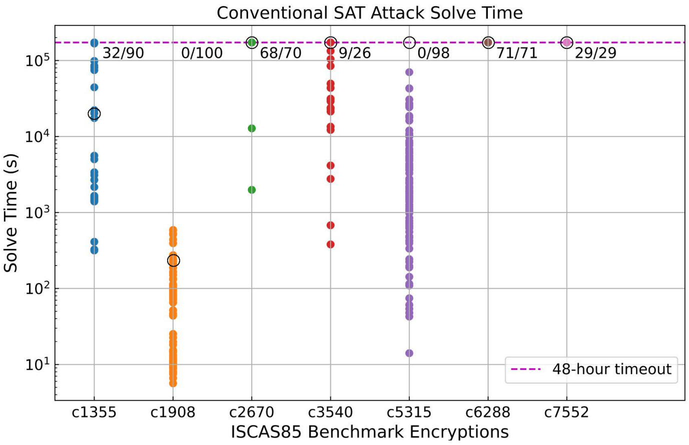


Fig. 13. Conventional SAT attack solve times of various locked ISCAS'85 benchmark circuits with island sizes limited to 500 gates. Locked circuits were successfully able to thwart 48-hour attacks for five of the seven benchmarks, similar to results achieved with conventional CMOS circuits. Black circles represent the solve time when every gate in the circuit was locked with the NAND/NOR polymorphism.

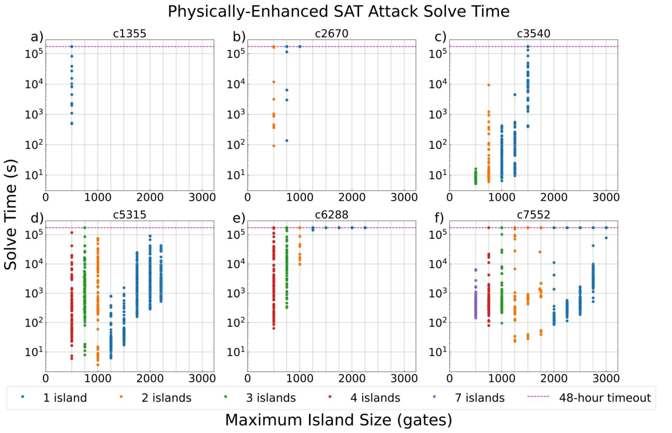


Fig. 14. Physically-enhanced SAT attack solve time for ISCAS'85 benchmark circuit for various maximum island sizes. All benchmarks shown had locked circuits that thwarted a 48-hour attack with small island size, thereby minimizing reliability and performance overhead.

circuits. The hybrid locking scheme can therefore consistently secure ISCAS'85 benchmark circuits under the conventional SAT attack model, even when locked islands are chosen using a naïve stochastic, greedy algorithm.

B. Security Against Physically-Enhanced SAT Attack

As illustrated in Fig. 14, successfully locked circuits achieving a 48-hour timeout were found for all depicted benchmarks despite the extra visibility of the attacker (illustrated in Supplementary Figure 2). While it is easier for the SAT engine to glean the key bits under the physically-enhanced attack model, the fact that the SAT attack times out even with our naïve selection algorithm demonstrates it is possible to secure a hybrid IC under the physically-enhanced attack model that can observe any unlocked net.

While the possible island sizes are constrained by the total number of gates in each circuit, larger islands do not necessarily imply more timeouts. This suggests that fewer large islands are not as effective as many small ones, and therefore, as circuit size scales, many small islands can be sufficient to secure the whole circuit, limiting the performance and delay overhead. Additionally, the sizes of the islands that achieved timeout were well within the limitation resulting from the reliability analysis described in Section VI-D. Security under the physically-enhanced attack model is further emphasized in Fig. 15, which visualizes the ability to achieve 48-hour timeouts across various configurations of island size, quantity of islands, number of key bits, and island I/O size.

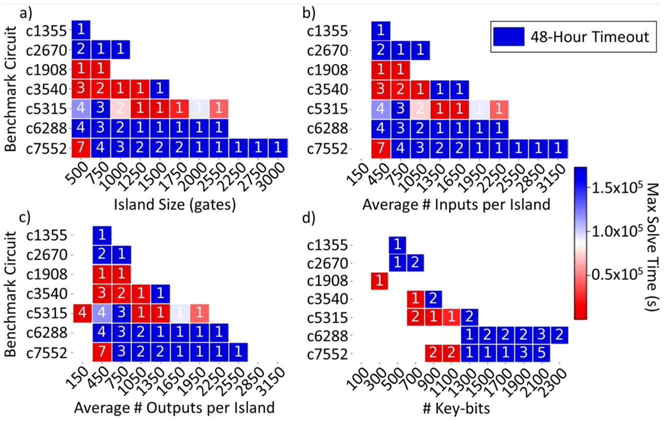


Fig. 15. Correlation heat maps of maximum physically-enhanced SAT attack solve time and (a) island size, (b) average number of island inputs, (c) average number of island outputs, and (d) number of key bits. Number of islands is indicated in white in the bottom right corner of each cell. The heatmaps showcase that a 48-hour timeout can be achieved across various island size and quantity configurations.

Our results demonstrate that it is possible to ensure the security of logic locked circuits under conventional and physically-enhanced SAT attacks. It should be noted here that there may be techniques to speed up the physically-enhanced attack that are not explored here. For instance, logically-independent islands may be attacked in-parallel or sequentially, dividing the problem into much more approachable chunks. This strategy can be countered by locking multiple gates in different islands using the same key bit, creating logical dependencies between islands. If key assignments are well-chosen, any particular island could be solved with a large number of possible key-bit combinations, but finding a key-bit combination that solves all the islands simultaneously will be significantly more difficult, ensuring the attacker must consider the circuit holistically. Security can be further increased through usage of alternate locking techniques (such as XOR insertion [1], LUT insertion [41], redaction [39], etc.) and developing smarter island assignment algorithms (perhaps modified versions of existing algorithms [17], [18]), though a more thorough evaluation of the physically-enhanced model and associated attack strategies and locking techniques is reserved for future work. Our naïve gate selection algorithm is therefore able to lock a circuit such that sufficient security is observed under both attack models. We have therefore demonstrated that the hybrid locking scheme is secure against both the conventional, and a physically-enhanced SAT attack model.

VIII. Conclusions

We have proposed a physically secure logic locking scheme using NML for both solely-spintronic and hybrid CMOS/NML chips. Despite NML's limitations, its distinctive physical security attributes warrant further exploration for manufacturing logic-locked NML chips. The replacement and insertion of well-chosen gates ensures security against SAT-based and structural attacks, and strain-induced PMA guarantees physical security of the key: the opacity and thickness of the strain shield prevent probing of the key-storing nanomagnets' magnetic states, while any attempt at delayering triggers the key's self-destruct mechanism, as magnetizations relax upon removal of the strain. Leveraging the unique physical traits of NML and strain-induced PMA, this approach offers an innovative technique protecting a key against physical attacks, thus paving the way for new avenues in logic locking.

As the speed and robustness drawbacks of NML have impeded its technological development, this work proposes a hybrid CMOS/NML locking scheme such that small "islands" of NML protect the entire chip. This work demonstrates that small islands are sufficient to secure logic-locked circuits against both conventional SAT attacks and physically-enhanced SAT attacks where an attacker has access to all internal electrical signals. Though the emerging technology islands are assigned by a naïve, stochastic algorithm, sufficient security is achieved against both conventional and physically-enhanced SAT attacks to achieve 48-hour attack timeouts. Hybrid logic systems are thus shown to provide security against physical and SAT-based attacks with minimal performance and reliability overhead resulting from the use of NML. As the results presented in Sections VI and VII are technology agnostic, a hybrid logic system with other physically secure emerging technologies can be similarly secured against the known physical attacks and SAT-based attacks.

Acknowledgement

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.*, "A critical view on the real-world security of logic locking," *J. Cryptogr. Eng.*, vol. 12, no. 3, pp. 229–244, 2022.

[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," *IEEE TETC*, 2020.

[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] L. Li and A. Orailoglu, "Piercing logic locking keys through redundancy identification," in *Proc. DATE*, 2019, pp. 540–545.

[14] P. Chakraborty *et al.*, "Sail: Analyzing structural artifacts of logic locking using machine learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3828–3842, 2021.

[15] M. Yasin *et al.*, "Removal attacks on logic locking and camouflaging techniques," *IEEE TETC*, vol. 8, no. 2, pp. 517–532, 2020.

[16] ——, "Ttlock: Tenacious and traceless logic locking," in *Proc. IEEE HOST*, 2017, pp. 166–166.

[17] K. Juretus and I. Savidis, "Increasing the sat attack resiliency of in-cone logic locking," in *Proc. IEEE ISCAS*, 2019, pp. 1–5.

[18] M. Yasin *et al.*, "On improving the security of logic locking," *IEEE TCAD*, vol. 35, no. 9, pp. 1411–1424, 2016.

[19] A. Rezaei *et al.*, "Hybrid memristor-CMOS obfuscation against untrusted foundries," in *Proc. IEEE ISVLSI*, 2019, pp. 535–540.

[20] Q. Alasad *et al.*, "Leveraging all-spin logic to improve hardware security," in *Proc. GLSVLSI*, 2017, pp. 491–494.

[21] ——, "Resilient and secure hardware devices using ASL," *ACM JETC*, vol. 17, no. 2, 2021.

[22] N. Hassan *et al.*, "Secure logic locking with strain-protected nanomagnet logic," in *Proc. DAC*, 2021.

[23] A. J. Edwards *et al.*, "Physically and algorithmically secure logic locking with hybrid cmos/nanomagnet logic circuits," in *Proc. DATE*, 2022.

[24] A. Rezaei *et al.*, "Rescuing logic encryption in post-sat era by locking & obfuscation," in *Proc. DATE*, 2020, pp. 13–18.

[25] 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.

[26] S. Takahashi and S. Maekawa, "Spin current in metals and superconductors," *JPSJ*, vol. 77, no. 3, pp. 031 009–031 009, 2008.

[27] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proc. DAC*, 2011, pp. 333–338.

[28] 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.

[29] B. Shakya *et al.*, "Covert gates: Protecting integrated circuits with undetectable camouflaging," *IACR TCHES*, pp. 86–118, 2019.

[30] A. Imre *et al.*, "Majority logic gate for magnetic quantum-dot cellular automata," *Science*, vol. 311, no. 5758, pp. 205–208, 2006.

[31] F. Riente *et al.*, "MagCAD: tool for the design of 3-D magnetic circuits," *IEEE JXCDC*, vol. 3, pp. 65–73, 2017.

[32] S. Manipatruni *et al.*, "Scalable energy-efficient magnetoelectric spin–orbit logic," *Nature*, vol. 565, no. 7737, pp. 35–42, 2019.

[33] 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.

[34] D. Carlton *et al.*, "Investigation of defects and errors in nanomagnetic logic circuits," *IEEE TNANO*, vol. 11, no. 4, pp. 760–762, 2012.

[35] 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.

[36] F. den Broeder *et al.*, "Magnetic anisotropy of multilayers," *Journal of Magnetism and Magnetic Materials*, vol. 93, pp. 562–570, 1991.

[37] J. Read *et al.*, "Magnetic degradation of thin film multilayers during ion milling," *APL Materials*, vol. 2, no. 046109, 2014.

[38] "ISCAS'85 Benchmark." [Online]. Available: http://www.pld.ttu.ee/~maksim/benchmarks/iscas85/bench/

[39] P. Mohan *et al.*, "Hardware redaction via designer-directed fine-grained efpga insertion," in *Proc. DATE*, 2021, pp. 1186–1191.

[40] N. Limaye *et al.*, "Thwarting all logic locking attacks: Dishonest oracle with truly random logic locking," *IEEE TCAD*, vol. 40, no. 9, pp. 1740–1753, 2021.

[41] A. Baumgarten *et al.*, "Preventing IC piracy using reconfigurable logic barriers," *IEEE Des. & Test Comp.*, vol. 27, no. 1, pp. 66–75, 2010.

[42] F. M. Spedalieri *et al.*, "Performance of magnetic quantum cellular automata and limitations due to thermal noise," *IEEE TNANO*, vol. 10, no. 3, pp. 537–546, 2011.

[43] D. Carlton *et al.*, "Investigation of defects and errors in nanomagnetic logic circuits," *IEEE TNANO*, vol. 11, no. 4, pp. 760–762, 2012.

[44] M. M. Al-Rashid *et al.*, "Effect of nanomagnet geometry on reliability, energy dissipation, and clock speed in strain-clocked DC-NML," *IEEE TED*, vol. 62, no. 9, pp. 2978–2986, 2015.

[45] M. S. Fashami *et al.*, "Switching of dipole coupled multiferroic nanomagnets in the presence of thermal noise: Reliability of nanomagnetic logic," *IEEE TNANO*, vol. 12, no. 6, 2013.

[46] M. M. Al-Rashid *et al.*, "Dynamic error in strain-induced magnetization reversal of nanomagnets due to incoherent switching and formation of metastable states: a size-dependent study," *IEEE TED*, vol. 63, no. 8, pp. 3307–3313, 2016.

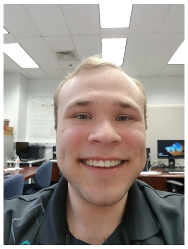
[47] D. C. Worledge *et al.*, "Spin torque switching of perpendicular Ta—CoFeB—MgO-based magnetic tunnel junctions," *Applied Physics Letters*, vol. 98, no. 2, p. 022501, 01 2011.

[48] M. Becherer *et al.*, "Towards on-chip clocking of perpendicular nanomagnetic logic," *Solid-State Electronics*, vol. 102, pp. 46–51, 2014.

[49] *International Roadmap for Devices and Systems (IRDS): More Moore*, 2022.

[50] T. Y. Lee *et al.*, "World-most energy-efficient mram technology for non-volatile ram applications," in *Proc. IEDM*, 2022, pp. 10.7.1–10.7.4.

[51] M. M. Al-Rashid *et al.*, "Effect of nanomagnet geometry on reliability, energy dissipation, and clock speed in strain-clocked DC-NML," *IEEE TED*, vol. 62, no. 9, 2015.



Alexander J. Edwards is a fifth-year Computer Engineering Ph.D. student at The University of Texas at Dallas (UTDallas). He received the B.S. degree in Computer Engineering in 2019 from Oklahoma Christian University. In 2023, he was awarded a Chateaubriand Fellowship for a four-month research visit to Université Paris-Saclay. In 2022, he was awarded the DOE SCGSR Award for a three-month research exchange visit to Sandia National Laboratories.

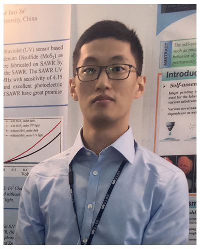
Naimul Hassan received his Ph.D. in Electrical Engineering from the Erik Jonsson School of Engineering & Computer Science at UTDallas in 2023. He received the B.Sc. degree in Electrical and Electronic Engineering in 2016 from Bangladesh University of Engineering and Technology. In 2022, he was awarded a Chateaubriand Fellowship for a four-month research exchange visit to Université Paris-Saclay.

Jared D. Arzate is a junior Electrical Engineering student at The University of Texas at Austin. His current research focus is on physical and algorithmic hardware security with nanomagnet logic. He has been a National Science Foundation (NSF) Research Experiences for Undergraduates (REU) Fellow.

Alexander N. Chin is a senior Computer Science student at UTDallas. His current research focus is on physical and algorithmic hardware security with nanomagnet logic. He has been awarded the UTD Undergraduate Research Scholar Award, and has also been a National Science Foundation (NSF) Research Experiences for Undergraduates (REU) Fellow.

Dhritiman Bhattacharya received his B.Sc. degree in Electrical and Electronic Engineering from the Bangladesh University of Engineering and Technology in 2013 and Ph.D. degree in Mechanical and Nuclear Engineering from Virginia Commonwealth University in 2020. He holds a Postdoctoral Associate position at Georgetown University. His current research interests include design, fabrication and characterization of nanomagnetic devices.

Mustafa M. Shihab received the BS in Electronic and Telecommunication Engineering from the North South University and MS in Electrical Engineering from Auburn University. He received his Ph.D. at UTDallas in 2021. His research interests include computer architecture, reconfigurable computing and their implications in hardware security. He is currently a hardware architect at Intel Corporation.



Peng Zhou received his Ph.D. in Electrical Engineering from the Erik Jonsson School of Engineering & Computer Science at UTDallas in 2023. He received the Bachelor degree in Mechanical Engineering in 2015 from Xiamen University of Technology and the Master degree in Electrical Engineering in 2018 from Xiamen University. His current research focus is on the design of a neuromorphic circuit that performs unsupervised on-chip online learning with STT-MRAM.

Xuan Hu received his Ph.D. in Electrical Engineering from UTDallas in 2021. He also received the B.S. degree in Electrical and Information Engineering in 2013 from Huaqiao University and the M.S. degree in Electrical Engineering in 2015 from Arizona State University. His research has focused on the circuit design and modeling of efficient logic and neuromorphic circuits composed of ambipolar carbon nanotubes, skyrmions, magnetic domain-wall devices, memristors, and multi-gate transistors.

Jayasimha Atulasimha is a Qimonda Professor of Mechanical and Nuclear Engineering with a courtesy appointment in Electrical and Computer Engineering at the Virginia Commonwealth University. He has authored or coauthored ~80 journal publications on magnetostrictive materials, magnetization dynamics, spintronics and nanomagnetic computing. His current research interests include nanomagnetism, spintronics, multiferroics, nanomagnetic memory and neuromorphic computing devices.

Yiorgos Makris received the Diploma degree in computer engineering from the University of Patras in 1995, and the M.S. and Ph.D. degrees in computer engineering from the University of California at San Diego in 1998 and 2001. He joined UTDallas, where he is currently a Professor of electrical and computer engineering, leading the Trusted and RELiable Architectures Research Laboratory, and the Safety, Security and Healthcare Thrust of the Texas Analog Center of Excellence.

Joseph S. Friedman received the B.E. degree from the Thayer School of Engineering at Dartmouth in 2009. He received the M.S. and Ph.D. degrees in Electrical & Computer Engineering from Northwestern University in 2010 and 2014. From 2014 to 2016, he was a CNRS research associate with Université Paris-Saclay. He is an associate professor in the Eric Jonsson School of Electrical & Computer Engineering at UTDallas, a core member of the Computer Engineering program, and director of the NeuroSpinCompute Laboratory.