Physically and Algorithmically Secure Logic Locking with Hybrid CMOS/Nanomagnet Logic Circuits

Alexander J. Edwards[1,*], Naimul Hassan[1], Dhritiman Bhattacharya[2], Mustafa M. Shihab[1], Peng Zhou[1], Xuan Hu[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
*{alexander.edwards, joseph.friedman}@utdallas.edu

***Abstract*—The successful logic locking of integrated circuits requires that the system be secure against both algorithmic and physical attacks. In order to provide resilience against imaging techniques that can detect electrical behavior, we recently proposed an approach for physically and algorithmically secure logic locking with strain-protected nanomagnet logic (NML). While this NML system exhibits physical and algorithmic security, the fabrication imprecision, noise-related errors, and slow speed of NML incur a significant security overhead cost. In this paper, we therefore propose a hybrid CMOS/NML logic locking solution in which NML islands provide security within a system primarily composed of CMOS, thereby providing physical and algorithmic security with minimal overhead. In addition to describing this proposed system, we also develop a framework for device/system co-design techniques that consider trade-offs regarding the efficiency and security.**

I. Introduction

Locking locking is an approach to prevent untrusted foundries from reverse engineering and counterfeiting integrated circuits (ICs). The functionality of the locked intellectual property (IP) is obscured by additional gates and logic structures which are enabled by a secret combination of bits known as the obfuscation key. It will only perform the correct function if the correct key is used to unlock the circuit, thus protecting the IP from untrusted foundries and malicious reverse-engineering parties. It is thus safe for the design house to outsource fabrication to an untrusted foundry, activating the chips with the obfuscation key once they have returned.

The design is only as secure as the key, and must therefore be secure against attempts to determine the key through physical and algorithmic attacks. For algorithmic security, the key must strongly encrypt the functionality of the design such that determining the key is NP-hard. While various logic structures have been proposed to impede algorithmic attacks, this algorithmic security is worthless if the key can be revealed through physical attacks. Therefore, the memory elements storing the key must be impervious to physical probing. Furthermore, any transportation of the key must also be invisible to probing.

Engels *et al.* [2] and Rahman *et al.* [3] recently demonstrated that they could reveal the location of an obfuscation key in modern CMOS processes through electrical imaging. Rahman *et. al.* [3] went further and were able to extract the key value through optical probing. Systems which store and transport the key electrically are therefore not secure against physical probing. Even if opaque materials are used to hide the key memory, these can be etched away to reveal the key [3]. Thus, modern CMOS processes are physically insecure, and thus are not secure at all. Similarly, recent proposals for logic locking with non-volatile devices are also vulnerable to physical attacks [4]–[9].

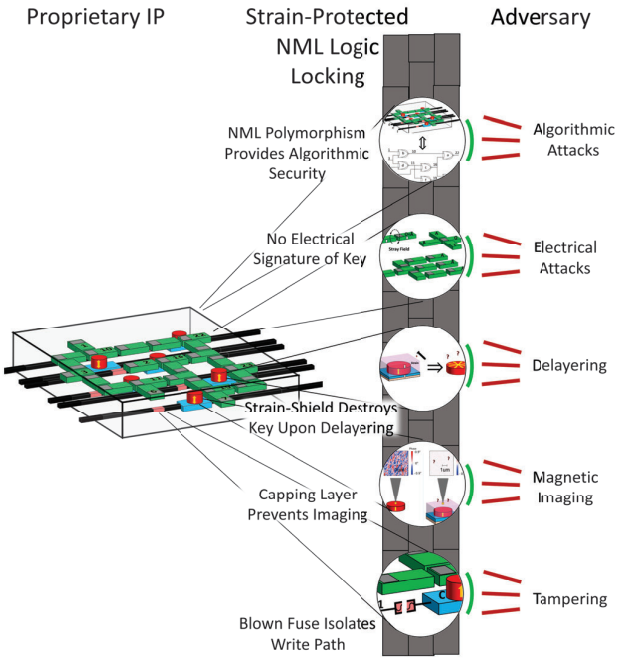

Fig. 1. Security of strain-protected NML. As we demonstrated in [1], NML protected with an opaque strain-inducing shield is secure against all known physical and algorithmic attacks against logic locking.

We recently proposed the first logic locking system that is secure against both physical and algorithmic attacks [1]. As illustrated in Fig. 1, this system leverages the rich behavior available with spintronics to enable nanomagnet logic (NML) to provide secure logic locking. However, the speed and reliability drawbacks of NML [10]–[13] impede the development of large-scale systems composed solely of NML. This paper therefore proposes that this NML hardware security can be best leveraged in a hybrid CMOS/NML system in which islands of NML provide hardware security in a system that is primarily composed of CMOS circuitry.

978-3-9819263-6-1/DATE22/©2022 EDAA

II. Attacks on Logic Locking

A logic locked design comprises a locked layout and the obfuscation key. The locked layout is provided to untrusted foundries or may be revealed through imaging. We therefore assume that the attacker has access to the layout and can attempt algorithmic and physical attacks on the key.

A. Algorithmic Attacks

The algorithmic satisfiability (SAT) attack is based on a Boolean satisfiability engine and requires access to the locked netlist of the chip and an unlocked chip, both of which will be available to the hacker. The satisfiability engine efficiently trims the possible key values based on strategic input combinations. No chip is secure against a SAT attack if enough time is available; the security of a logic locking scheme is characterized by the time it takes to obtain the key.

B. Side-Channel Attacks

Side-channel attacks observe information beyond the digital input-output behavior, such as power, timing, magnetic, radio, etc. Any obfuscation key which is applied electrically is subject to side-channel attacks, regardless of where the key is stored; this is a significant impediment to logic locking.

C. Electrical Imaging Attacks

Imaging can be used to reveal the electrical activity of an obfuscated chip; if the obfuscation key is stored or transported electrically, it may be revealed through imaging. Rahman *et. al.* created an activity map of a design and were able to reveal the obfuscation key [3]. A large number of technologies are vulnerable to electrical imaging, including CMOS and polymorphic gates with non-volatile devices [4]–[7].

D. Material Delayering Attacks

Material delayering involves removing protective or non-critical layers of a chip in order to enable probing and direct observation of the key bits in a logic-locked system.

E. Magnetic Imaging Attacks

There are two primary categories of magnetic probing:

- stray field detection (*e.g.*, magnetic force microscopy), where the stray field is detected by a magnetic probe.
- active probing (*e.g.*, magneto-optic Kerr effect), where the magnetic state is tracked by reflected light.

Both types of probing can reveal the polarity of a magnet; magnetic imaging can reveal the key bits in [8].

III. Logic Locking with Strain-Protected NML

We previously proposed a logic locking scheme based on NML that is secure against all known algorithmic and physical attacks [1]. The keys are stored in non-volatile nanomagnets and the computation is entirely magnetic, preventing electrical detection of the keys and solving a previously insurmountable challenge to logic locking. Furthermore, the nanomagnets are protected against delayering and magnetic imaging attacks with a strain-inducing opaque shield which must remain intact to prevent self-destruction of the obfuscation key.

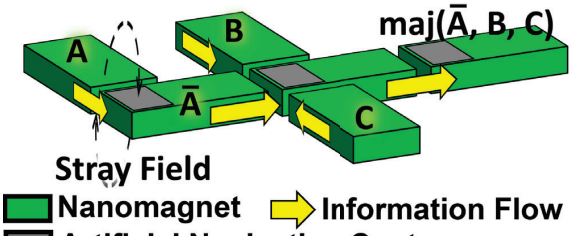

Fig. 2. NML majority gate and signal propagation. The stray fields from nanomagnets $\bar{A}$, B, and C influence the center magnet equally, thus performing the majority function.

A. Background on Nanomagnet Logic

In NML [14], binary values are encoded in the magnetization of a nanomagnet. As illustrated in Fig. 2, information is transmitted between neighboring magnets via magnetostatic interactions. Switching is assisted by artificial nucleation centers (ANCs), enabling unidirectional signal propagation. The resulting magnetization switch propagates through the next magnet via domain wall motion assisted by an alternating clocking magnetic field. This enables directed, regenerative, synchronous information propagation throughout the logic system. The system has natural inverters with the magnetization flipping at each magnet, and majority (or minority) gates may be implemented by having multiple input magnets influence the ANC of a single output magnet.

B. Tamper-Proof Logic Locking with NML Polymorphism

As described in [1], we proposed NML logic locking based on the polymorphism of a majority gate. That is, if input C of a majority gate is fixed, the functionality of the majority gate is simplified to $O = A + B$ for $C = 1$ and $O = A * B$ for $C = 0$. As the inputs to NML gates are non-volatile nanomagnets, this input C may be programmed with one bit of an obfuscation key to control the polymorphic two-input gate.

To prevent tampering with the obfuscation key after it is programmed, we proposed in [1] the fuse-protected spin-orbit torque writing mechanism of Fig. 3. To program input C to a particular state, a current pulse is applied in the presence of a magnetic field; eventually the fuse will blow due to I^2R

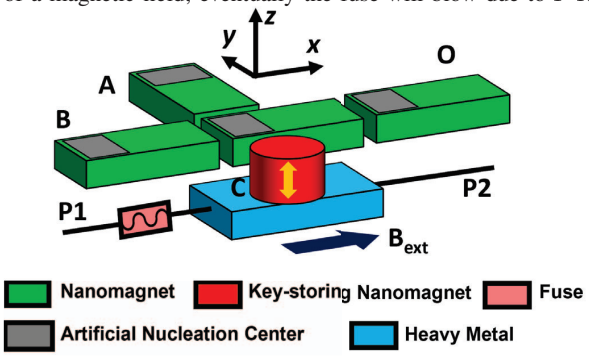

Fig. 3. Two-input polymorphic NML gate with tamper-proof programming of obfuscation key magnet C.

heating, halting the current flow and causing the nanomagnet to relax to the non-volatile key state. Thus, the obfuscation key can be deterministically written only once, and may not be altered after programming.

C. Protection Against Delayering with a Strain Shield

As the magnetization of nanomagnets in conventional NML systems can be readily probed through magnetic imaging techniques, our previous proposal for physically and algorithmically secure logic locking [1] includes an opaque anisotropy-inducing "strain shield" that prevents imaging (Fig. 4). In the absence of this strain shield, the key magnets have in-plane magnetic anisotropy; as they are circular, their negligible anisotropy prevents the storage of information. The strain shield, however, produces bulk strain on the nanomagnets that induces perpendicular magnetic anisotropy (PMA) and enables the nanomagnets to store an obfuscation key in a non-volatile manner. If delayering is performed in an attempt to perform magnetic imaging of the obfuscation key, the nanomagnets will return to an isotropic in-plane orientation, destroying the obfuscation key.

IV. Security of Strain-Protected NML

The logic locking scheme with NML polymorphism is free of electrical signatures, and the imaging-resistant strain shield makes this system secure against all known attacks to logic locking [1]. While the circuit layout may be extracted, it is useless without the undetectable obfuscation key.

A. Security Against Algorithmic Attacks

We demonstrated algorithmic security in [1] by performing the SAT attack on benchmark circuits locked with NML polymorphic gates. The results are similar to those conventionally observed with CMOS, with the solver timing out on five of the circuits after twelve unsuccessful hours.

B. Security Against Side-Channel Attacks

After blowing the fuses of the tamper-proof NML circuit, there is no electrical interface to the key nanomagnets and therefore no electrical side-channels to exploit. Regarding timing, an attacker may attempt to discern timing differences with different inputs; however, the clocking field causes all outputs to be synchronized as long as at least one magnet is used to buffer each output. Thus, there are no side-channels available to launch an attack on the chip.

C. Security Against Electrical Imaging Attacks

As the NML system operates entirely via magnetic interactions, imaging of electrical phenomena is not possible.

D. Security Against Material Delayering Attacks

As described in Section III-C any attempted delayering of the strain shield to observe the magnetic state of the key-storing nanomagnets will cause the PMA of the nanomagnet to be removed. As the magnet is circular, this will cause the magnet to move to a random in-plane state, thereby destroying the stored obfuscation key bit. Therefore, this NML system is secure against delayering.

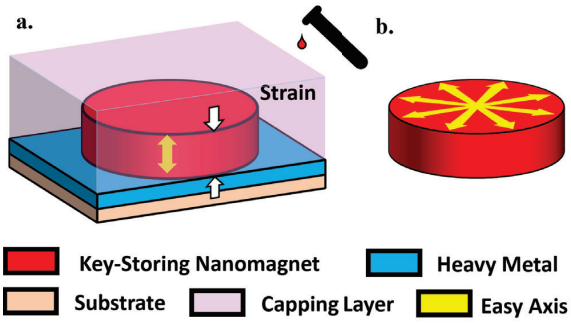

Fig. 4. Strain-induced magnetic anisotropy. (a) The strain shield is manufactured with a material that induces PMA in the nanomagnets such that (b) if the shield is removed through some invasive technique, the nanomagnet will return to an isotropic in-plane magnetization with random orientation, thereby destroying any information that was stored in it.

E. Security Against Magnetic Imaging Attacks

The opacity of the strain shield prevents active imaging, and its thickness prevents stray field imaging. To demonstrate this, we manufactured a small Co(15nm)/Ti(5nm)/Substrate film and observed distinct magnetic domains using MFM [1]. We then manufactured an additional 100 nm Ti capping layer atop the film and were no longer able to observe any magnetic domains. This strain-protected NML system is thus secure against magnetic imaging attacks.

V. Secure Hybrid CMOS/NML Circuits

While strain-protected NML provides physical and algorithmic hardware security [1], the development of a solely-NML computing system is impeded by the poor speed and reliability of NML [10]–[13]. As illustrated in Fig. 5, we therefore propose that hybrid CMOS/NML computing systems be developed that leverage the security of NML obfuscation islands in a system primarily composed of CMOS.

A. Nanomagnet Logic Islands

The development of large-scale computing systems comprised solely of NML is challenged by issues inherent to the underlying magnetic phenomena [13], [15]:

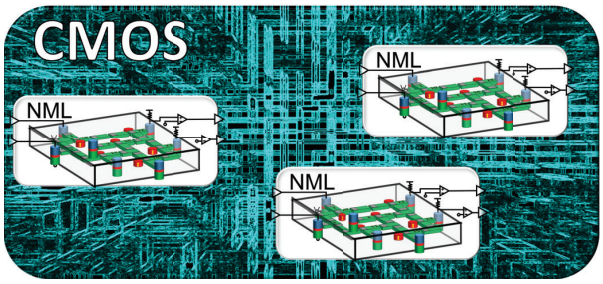

Fig. 5. Hybrid CMOS/NML proposal. CMOS is superior to NML in terms of speed and robustness, but is vulnerable to physical attacks. We therefore propose that CMOS blocks be strategically substituted with secure NML blocks to provide security with minimal efficiency overhead.

- magnetic switching and magnetic domain wall motion are slow processes, thereby limiting the clock speed.
- thermal noise, misalignment, and fabrication issues lead to switching errors that degrade circuit reliability.

Therefore, in order to create *large-scale* computing systems that are physically and algorithmically secure, we propose hybrid systems in which one or more NML circuits is integrated with CMOS circuits that comprise the majority of the computing system. These NML obfuscation islands lock the functionality of the system as a whole, as the nanomagnet obfuscation keys within these islands significantly impact the logical behavior of the entire system. Therefore, hybrid CMOS/NML system design is characterized by trade-offs between security and computational efficiency that dictate the optimal quantity, size, and location of NML obfuscation islands within the CMOS system.

In the hybrid system, well-chosen blocks in a digital design are implemented with secure NML. Fig. 6 depicts a sample IP block diagram, highlighting potential candidates for logic locking with strain-protected NML. Optimally, the blocks selected for NML obfuscation islands will not significantly impact timing, but will still perform a critical function such that the obfuscation of this portion of the circuit obfuscates the entire design. Two types of blocks generally meet these criteria: combinational blocks that do not lie on the critical timing path and pipelined sequential blocks in scheduled systems that complete computation in fewer cycles than the slowest block. As described below in Sections V-B and V-C, secure NML is amenable to both combinational and sequential logic and thus both of these types of blocks are appropriate for strain-protected NML logic locking.

As increased size and complexity of an NML circuit implies increased impacts of the deleterious NML characteristics mentioned above, the ability to provide algorithmic security with small NML islands permits strong algorithmic security with minimal hardware overhead. The optimization of secure and efficient hybrid CMOS/NML systems must therefore consider complex device/system co-design trade-offs regarding the efficiency and security of NML islands as a function of their size, as well as co-design considerations related to the ideal placement of these islands.

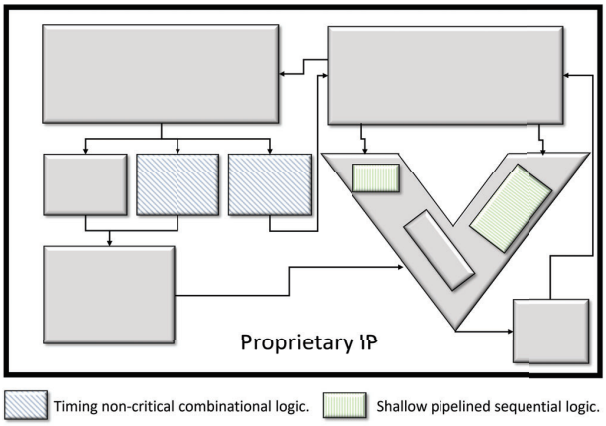

Fig. 6. Sample block diagram of IP. Potential candidates for NML logic locking are highlighted. These include combinational blocks and pipelined sequential blocks that are not on the critical timing path; for example, a pipelined adder may require three cycles of computation whereas a multiplier may require 15. The faster blocks may thus be logic-locked with NML without drastically impacting the processing time or clock frequency.

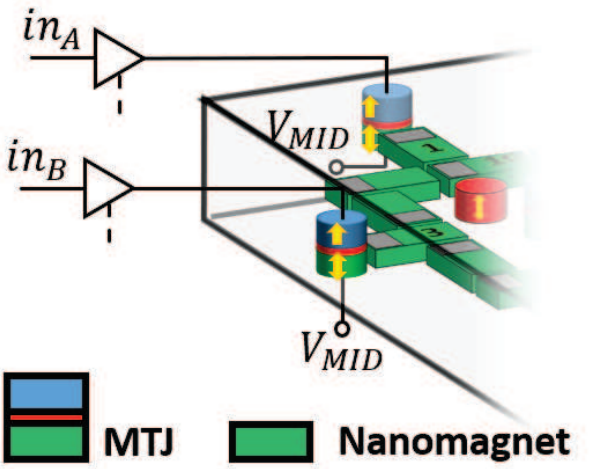

Fig. 7. Signals from the conventional CMOS system are input into the secure NML logic circuit through spin-transfer torque.

B. Inputs to NML Islands

Inputs to the NML islands may be controlled via spin-transfer torque, converting electrical stimuli to magnetic orientation. Fig. 7 illustrates this mechanism, wherein current passing through the magnetic tunnel junction (MTJ) writes its magnetic orientation. The direction of the current through the device, in conjunction with the magnetization of the fixed ferromagnet layer (blue), dictates the resultant direction of the free ferromagnet layer (green). Dipolar coupling from the MTJ free layer governs the magnetization of the NML input magnet, allowing signal propagation to the NML circuit.

This NML input mechanism is amenable to both combinational and sequential logic, as the input current can be clocked with a tri-state buffer to save energy and prevent glitches. Thus, NML islands can replace both combinational and sequential blocks. In combinational blocks, the clocking magnetic field is included in the NML propagation delay; in sequential circuits, the clocking magnetic field of the NML circuit must be considered in relation to the global CMOS system clock.

C. Outputs from NML Islands

The outputs from the NML islands can be read with MTJs, which have a variable resistance depending on the orientation of the free-layer magnetization. As illustrated in Fig. 8, this resistance may be sensed with a voltage divider; if necessary, a thresholding amplifier may be used for level-shifting. Energy may be conserved by only reading the system briefly when a result becomes available.

Like the NML input circuit, the NML output circuit is compatible with both combinational and sequential logic. For combinational blocks, the read voltage may be constantly

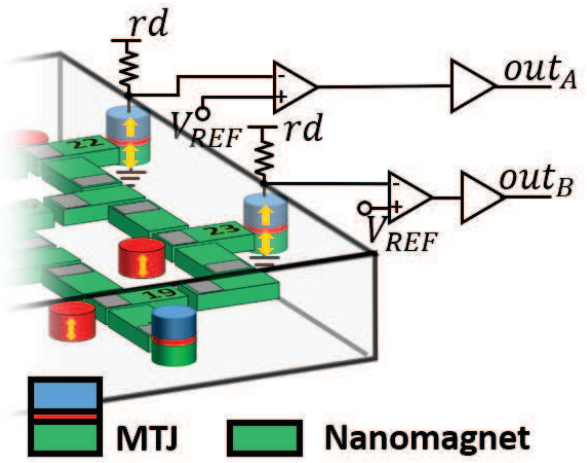

Fig. 8. Output signals from the secure NML system are provided to the conventional CMOS system through an MTJ and voltage divider.

applied, thereby producing an output voltage which represents the output nanomagnet state at all times. In this case, a small read voltage may be used to reduce power consumption. For sequential blocks, the read voltage may be clocked, with a latch at the output to hold the signal between read cycles. In both cases, the NML island can function properly within a conventional CMOS system with minimal read-out circuitry.

VI. Security & Efficiency of Hybrid CMOS/NML

The integration of secure NML within a conventional CMOS system requires co-design that simultaneously considers timing, robustness, and security.

A. Timing Considerations

This hybrid CMOS/NML approach combines the logic locking security of strain-protected NML with the speed and reliability of CMOS. Regarding the timing of combinational blocks chosen for NML security islands, the best combinational blocks are those with heavy parallelism that compute critical functions without a large amount of gate depth. These functions minimally impact the overall system timing, and are therefore highly suitable for NML security islands. In NML, the combinational propagation delay is the maximum depth of the circuit (in terms of the number of nanomagnets) multiplied by the clock frequency, which is limited by the propagation speed of magnetic domain walls.

For pipelined sequential blocks, the NML circuits are naturally pipelined by the alternating magnetic clocking field required for NML signal propagation. These blocks can therefore operate with heavy parallelism and high throughput, but may suffer from large latencies.

There are various methods for decreasing the NML circuit depth, including increasing the number of gate inputs and incorporating multiple nanomagnet layers to avoid large planar routing paths. Though NML suffers from slow speeds, the impact of this slow speed can be mitigated by strategically selecting logic-locked blocks that avoid critical timing paths and optimizing the NML circuits for minimal depth.

B. Robustness Considerations

The non-negligible error rate of NML presents challenges for robustness. To minimize the deleterious impacts of NML errors, shallow blocks can be used with significantly greater reliability.

Another solution is to duplicate the NML circuits to reduce errors caused by fabrication defects. In one approach, three nominally-identical NML circuits can be placed in parallel, with majority voting to circumvent NML switching errors. Alternatively, properly operating circuits may be selected during the testing process, and incorrect circuits isolated with fuses. As the same obfuscation key will be written to each circuit, these approaches do not create new security vulnerabilities. Similar to timing considerations, robustness issues can be minimized by maximizing the quantity of NML security islands and minimizing island depth, thereby gleaning both the security benefits of NML and the speed/robustness benefits of CMOS.

C. Physical Security

As described in [1], the strain-protected NML circuits are physically and algorithmically secure. The only new vulnerabilities that may potentially be presented by this hybrid system are at the interfaces between the CMOS and NML. As described in Sections V-B and V-C, the electrical interface only contains information about the input and output signals to that island. Thus, if electrical imaging is performed, an attacker must still perform an algorithmic attack to decipher the key bits.

At the input to NML security islands, the only potential security risks are at the interface from the physically insecure CMOS environment to the secure NML environment. As the ANCs and the clocking field ensure information does not travel backwards toward the circuit inputs, the inclusion of at least one buffer magnet after the inputs ensures that no information about the key is able to be sensed at the input interface.

At the outputs of the NML security islands, the potential security risks are at the electrical interface at the output of the secure NML environment. As the resultant electrical signal will only reveal information about the output of the NML island, the island remains secure as long as it is algorithmically secure. This interface therefore does not provide any additional exploits to adversaries.

D. Algorithmic Security

The security of hybrid CMOS/NML against algorithmic attacks increases with the number of islands. As depicted in Fig. 9(a), conventional algorithmic attacks occur at the chip interface, in which the outputs are monitored in response to input combinations chosen to isolate and decipher key bits. Similar to conventional logic locking, the computational challenge of deciphering these key bits increases exponentially with the number of islands.

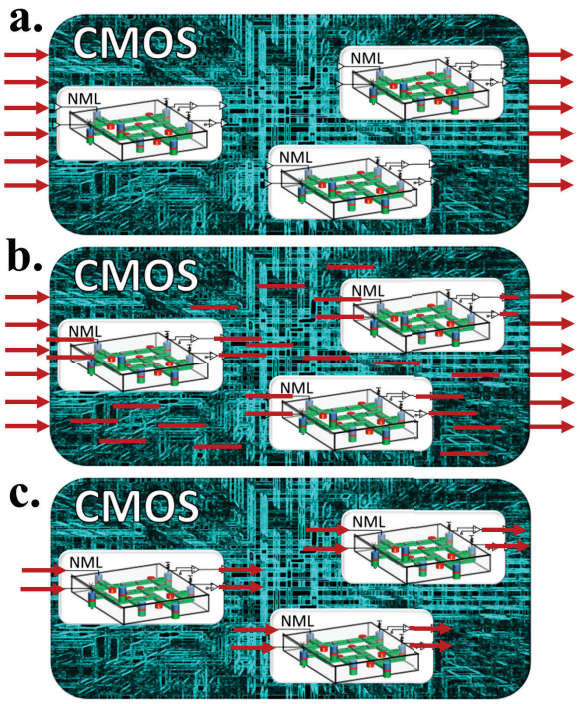

Fig. 9. Levels of algorithmic attacks on hybrid CMOS/NML logic locking. (a) In conventional algorithmic attacks, the attacker must decipher the key with only the input/output combinations. In a conventional SAT attack, the individual NML islands therefore work together to secure the CMOS chip. (b) If the attacker can image the electrical behavior of the chip, they can reduce the number of unknowns through visibility of the NML island interface. However, it remains exceptionally difficult for the attacker to target the individual islands with required stimuli, and the complexity of the attack is not significantly reduced. (c) The only way the complexity of the attack can be reduced is by stimulating individual ports of the NML islands embedded in the CMOS, which is not currently possible.

If an attacker has access to electrical imaging, they will be able to discern the inputs and outputs to the NML islands, as described in Section VI-C. In this case, illustrated in Fig. 9(b), the attacker may be able to isolate obfuscation key bits with a reduced number of targeted stimuli. However, the ability to target an individual island with a specific stimulus is an NP-hard problem; therefore, the required SAT attack remains NP-hard.

In order to attack the NML security islands individually as in Fig. 9(c), it must be possible to physically stimulate individual nets within the circuit structure. This has not been demonstrated in the literature at the scales provided by modern fabrication technologies. If it ever becomes possible, the security of the chip will be equal to the security of the strongest island. To prevent against future attacks against individual islands, each NML island can be made suitably secure individually, resulting in a trade-off between timing, robustness, and security.

More than likely, however, attackers will never have the opportunity to stimulate individual nets. Therefore, the algorithmic security of the collective NML islands can increase with the number of islands. Therefore, hybrid CMOS/NML has the potential to be both physically and algorithmically secure, with minimal circuit efficiency overhead required to provide this security.

VII. Conclusions

This work builds on our previously proposed strain-protected NML logic locking, which was the first logic locking proposal that is secure against all known physical and algorithmic attacks. As the speed and robustness drawbacks of NML have impeded its technological development, we propose here that NML security circuits can be efficiently integrated into modern CMOS technologies in small "islands" such that the security of these islands protects the entire chip. Furthermore, device/system co-design trade-offs have been explored, leading to the conclusion that full-system security can be achieved with minimal efficiency overhead through the use of numerous small NML security islands that are off the critical timing path.

Acknowledgements

The UTD authors 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] N. Hassan *et al.*, "Secure logic locking with strain-protected nanomagnet logic," in *Design Automation Conference*, 2021.
[2] 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.
[3] 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.
[4] F. Parveen *et al.*, "Hybrid polymorphic logic gate with 5-terminal magnetic domain wall motion device," in *Proc. IEEE ISVLSI*, 2017, pp. 152–157.
[5] S. Patnaik *et al.*, "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in *Proc. DATE*, 2018, pp. 97–102.
[6] N. Rangarajan *et al.*, "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," *arXiv:1811.06012*, 2018.
[7] A. Rezaei *et al.*, "Hybrid memristor-CMOS obfuscation against untrusted foundries," in *Proc. IEEE ISVLSI*, 2019, pp. 535–540.
[8] Q. Alasad *et al.*, "Leveraging all-spin logic to improve hardware security," in *Proc. GLSVLSI*, 2017, pp. 491–494.
[9] ——, "Resilient and secure hardware devices using ASL," *ACM JETC*, vol. 17, no. 2, 2021.
[10] M. S. Fashami *et al.*, "Switching of dipole coupled multiferroic nanomagnets in the presence of thermal noise: Reliability of nanomagnetic logic," *IEEE T. Nano.*, vol. 12, no. 6, 2013.
[11] F. M. Spedalieri *et al.*, "Performance of magnetic quantum cellular automata and limitations due to thermal noise," *IEEE Transactions on Nanotechnology*, vol. 10, no. 3, pp. 537–546, 2011.
[12] D. Carlton *et al.*, "Investigation of defects and errors in nanomagnetic logic circuits," *IEEE Transactions on Nanotechnology*, vol. 11, no. 4, pp. 760–762, 2012.
[13] M. M. Al-Rashid *et al.*, "Effect of nanomagnet geometry on reliability, energy dissipation, and clock speed in strain-clocked dc-nml," *IEEE Transactions on Electron Devices*, vol. 62, no. 9, pp. 2978–2986, 2015.
[14] P. Zhou *et al.*, "Multilayer nanomagnet threshold logic," *IEEE Transactions on Electron Devices*, vol. 68, no. 4, pp. 1944–1949, 2021.
[15] 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 Transactions on Electron Devices*, vol. 63, no. 8, pp. 3307–3313, 2016.