Exploring Security Solutions and Vulnerabilities for Embedded Non-Volatile Memories

Zakia Tamanna Tisha
Electrical and Computer Engineering
Auburn University
Auburn, AL, USA
zakia.tisha@auburn.edu

Jeremy Muldavin
Aerocyonics Inc.
RI, USA
jeremy.muldavin@aerocyonics.com

Ujjwal Guin
Electrical and Computer Engineering
Auburn University
Auburn, AL, USA
ujjwal.guin@auburn.edu

2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) | 979-8-3503-5411-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISVLSI61997.2024.00072

***Abstract*—Non-volatile memories (NVMs) have gained prominence in the modern semiconductor industry as they strive to address the requirements of high-performance computing. NVMs have become appealing components in secure systems due to their limited area-energy-runtime budgets and extended data retention capabilities. However, the data retention capability of NVMs, which persists even after power is switched off, also makes them vulnerable to malicious attacks, raising security concerns about their applications. Despite the considerable number of publications on the security applications and vulnerabilities of NVMs separately, few studies have combined these aspects in recent years. During this period, significant developments have occurred in the NVM landscape, including the creation of new hardware security primitives based on NVMs and the emergence of new attacks against them. This paper aims to fill the research gap by providing a comprehensive review of both the security applications and vulnerabilities of embedded NVMs, serving as a valuable resource for researchers new to this area. The paper discusses research trends in NVM-based security primitives such as Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs), as well as logic obfuscation techniques. It also explores the risks and common attacks associated with embedded NVMs and concludes with suggestions for future research directions in the security aspects of this domain.**

***Index Terms*—non-volatile memories, security primitives, PUFs, TRNGs**

I. Introduction

The fundamental limitations associated with shrinking device size and increased process complexity have prompted the emergence of embedded nonvolatile memories (eNVM) with diverse architectures to further increase performance, reduce active and standby power, and provide scalable and programmable hardware accelerators and security features [1]. The era of the Internet of Things (IoT) and cyber-physical systems (CPS) demand data-centric applications with ultra-low power operation, cost-effectiveness, high density, reliability, and extended data storage capabilities. eNVMs ensure persistent data storage for smart devices that operate in remote environments where continuous power supply is unavailable. eNVMs are engineered to preserve data for several years, a stark contrast to volatile memories like dynamic random-access memory (DRAM), which can only maintain data for less than a second. This extended data retention period is particularly advantageous for applications prioritizing data integrity and longevity, such as archival storage, critical system backups, and IoT deployments in remote locations. Moreover, eNVM technologies provide high-density data storage capabilities and are well-suited for low-power applications, seamlessly aligning with the energy-efficient requirements of modern electronics and IoT devices.

Devices with security applications increasingly require the unique properties of eNVMs. Our paper explores the use of eNVM technology to enable security features and the associated risks and vulnerabilities. The first contribution of our paper is examining the technology behind security devices and solutions that utilize eNVMs. Stochastic switching in NVMs acts as a rich entropy source. This, combined with the scalability and reconfigurability of eNVMs, can be leveraged to build novel security primitives like Physically Unclonable Functions (PUFs), True Random Number Generators (TRNGs), etc. [2]. Research is also underway for the application of eNVMs in logic obfuscation techniques. The second contribution offered in our paper is the examination of common attacks and risks associated with eNVMs. The integration of emerging eNVMs into computing systems also raises concerns about the leakage of sensitive information. With the growing popularity of eNVMs, it has become imperative to investigate the risks and vulnerabilities associated with the eNVM technology. Popular attacks targeting eNVMs include side-channel attacks, probing, fault injection, and row-hammer attacks. This paper provides an outline of the research conducted to explore these attacks.

The paper is organized as follows. Section II discusses various types of NVM technologies. Section III elaborates on security applications using eNVMs. Section IV discusses the vulnerabilities and different types of attacks on eNVMs. Section V explores future directions in this domain. Finally, the conclusion is provided in Section VI.

II. Description of NVM technologies

Traditionally, the combination of CMOS-based memories, such as volatile DRAM and SRAM, and nonvolatile flash, have been adequate to meet both the temporary and permanent data storage requirements of multichip systems. The trend towards system-on-chip integration with scalability, reconfigurability, and very low power has driven the development of additional eNVM technologies with new memory and computational architectures. These memory types utilize specific materials that have the ability to maintain a bi-stable state in their electronic characteristics. This distinguishing property enables data retention in eNVMs without a continuous power supply. Until recently, there have been minimal changes to the fundamental technology and cells responsible for retaining

2159-3477/24/$31.00 ©2024 IEEE
DOI 10.1109/ISVLSI61997.2024.00072

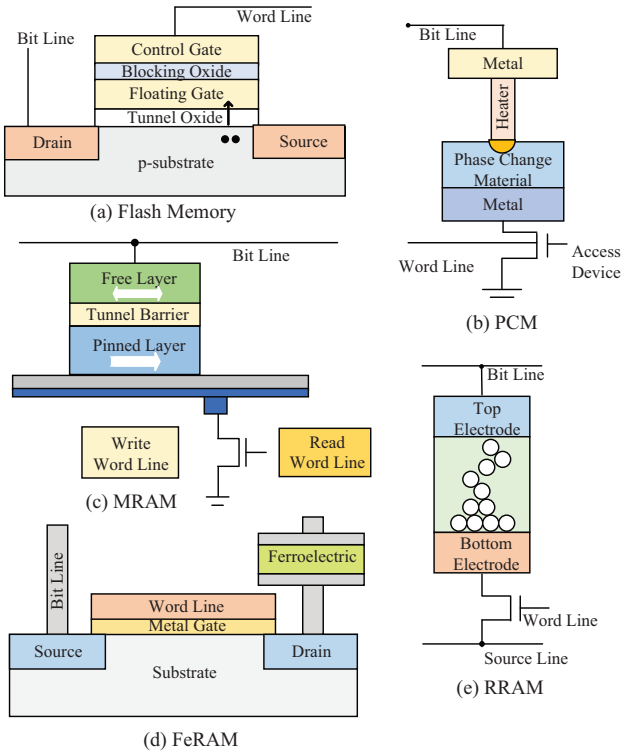

Figure 1: Bitcell diagram of a (a) Flash Memory [3], (b) PCM [4], (c) MRAM, (d) FeRAM [5], (e) RRAM [6].

data when power is off. Currently, floating gate or oxide-nitride-oxide trapped charge (ONO) cell structures are the predominant core technologies in the majority of eNVM devices [7]. This paper explores five types of nonvolatile memory technologies, including flash memory, ferroelectric random-access memory (FeRAM), magnetic random-access memory (MRAM), phase-change memory (PCM), and resistive random-access memory (RRAM).

• **Flash Memory:** A nonvolatile device based on Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) technology [8] and shown in Figure 1(a), Flash memory has revolutionized electronic devices. It utilizes floating gate memory for information storage and tunneling current for programming and erasing. Charge injection or removal from the floating gate enables state retention even after power removal. Flash memory is extensively used in medical diagnostic systems, digital cameras, and mobile phones due to its non-volatility, magnetic immunity, and compatibility with current CMOS processes. However, scaling may face limitations due to tunnel oxide constraints and the cost of integration [5].

• **Phase Change Memory (PCM):** PCM is a type of non-volatile RAM characterized by a simple capacitor-like structure (shown in Figure 1(b)), with a thin chalcogenide semiconductor film sandwiched between electrodes, facilitating easy miniaturization [9]. These devices boast long cycle life, low programming energy, and excellent scaling characteristics. Chalcogenide phase-change materials, commonly containing elements from group 6 of the periodic table and further expandable to additional material systems by doping, are prominent in PCM, with GeSbTe alloys, especially the GST pseudobinary composition, showing high promise. Operating on the principle of phase change from amorphous to crystalline or vice versa, PCM undergoes this transition at a relatively low temperature of around 600°C, driven by energy from Joule heat generated by current passing through the PCM cell. The resistivity of chalcogenide material varies between the crystal and amorphous phases, allowing data storage based on resistivity changes.

• **Magnetic Random Access Memory (MRAM):** Combining spintronic devices with silicon-based microelectronics, MRAM offers nonvolatility and high density, ideal for solid-state disk applications [10], [11]. Memory cells in MRAM consist of two magnetic storage elements stacked with a thin insulating tunnel barrier between them as shown in Figure 1(c). The magnetic tunnel effect allows electrons to tunnel, resulting in low-resistance 'ON' states with parallel magnetic moments. Writing and erasing are achieved by passing a current through the write line, creating a magnetic field [5]. Spin transfer torque MRAM (STT-MRAM) addresses high operating current issues by manipulating magnetization direction in the free layer using spin-polarized current between layers. This technology promises low-current, cost-effective MRAM devices where magnetic interference can be mitigated [9].

• **Ferroelectric Random Access Memory (FeRAM):** It is a type of NVM that consists of a capacitor and transistor structure (see Figure 1(d)). FeRAM provides not just non-volatility but also offers fast memory access similar to DRAM [12]. One of FeRAM's key features is its extremely low power consumption, which is unmatched by other NVM technologies like Flash. This low power requirement allows FeRAM to operate at voltages less than 2V, a significant advantage over Flash, which requires over 20V for write or erase operations. The most used ferroelectric material for FeRAMs is lead zirconate titanate (PZT) [5]. FeRAM also offers fast writing speeds and a high number of rewrites, making it suitable for high-density and processing in-memory applications. These memories come in various cell types, such as capacitor, transistor, and chain cell, with the transistor type being better for high-density uses. However, this type of FeRAM has issues with data retention, not lasting 10 years in practical applications [9].

• **Resistive Random Access Memory (RRAM):** RRAM is a device with a simple metal–insulator–metal structure, where the insulator is typically an oxide of elements like Hafnium, Tantalum, or Titanium. Other materials, such as chalcogenides and 2D materials like hexagonal boron nitride, have also been used and shown in Figure 1(e). RRAMs can have a single metal-insulator-metal layer or a multilayered structure, offering improved uniformity in device parameters. These devices switch between high and low resistance states, representing 1 and 0 bits. The resistive switching is achieved through SET and RESET operations, forming or rupturing conducting paths inside the insulator [13].

III. Embedded NVMs for Security

eNVMs are crucial components in secure systems due to their capability to retain data even when there is no power. These advanced memory solutions play a role in constructing

secure architectures that are resistant to tampering and provide durability for a broad spectrum of applications, such as cryptographic key storage and secure boot processes. Furthermore, their superior scalability, reconfigurability, low-cost local computing, and rich source of entropy make them great candidates for security primitives like physically unclonable functions and true random number generators [2]. In security applications, STT-MRAM and RRAM-based eNVMs are widely utilized. The inherent randomness in RRAM-based security systems is crucial for applications such as PUFs and TRNGs.

• **Physically Unclonable Functions (PUFs):** PUFs harness residual manufacturing process variations to generate unique and unclonable device signatures [14]. By generating on-demand keys, PUFs eliminate the need to store keys in non-volatile memory during deployment, enhancing device resistance against physical attacks. These individualized keys allow for unique device identification and authentication. Memory-based PUFs, among various architectures, generate unclonable signatures without requiring hardware modifications [15], [16]. Considerable research has been conducted on RRAM PUFs [17], [18], MRAM PUFs [19], [20], PCM PUFs [21], [22], and Flash memory PUFs [23].

The majority of PUF demonstrations involve the comparison of resistances among selected cells [24]. In addition, randomness was also induced by applying a near-threshold voltage to RRAM, causing certain cells to flip while others remain unchanged [25], [26]. Geometry-based STT-MRAM PUFs [20], [27] operate through a two-step process, initially placing cells in an unstable polarization state and subsequently allowing them to settle into stable states. Due to the geometric variations in magnetic tunnel junctions (MTJ), each array of cells settles into a unique set of values, which can be conventionally read out to establish a memory PUF. Other STT-MRAM PUFs rely on comparing cell resistances in the anti-parallel state [19], [28]–[30]. Zhang et al. [29] assessed the feasibility and quality of NVM PUFs based on STT-MRAM, PCM, and RRAM. The study demonstrated that, compared to traditional memory PUFs, eNVM-based PUFs offer higher density, enabling more efficient chip area utilization for an equivalent number of bits. However, the reliability of certain eNVMs, such as RRAM-based PUFs, could potentially be influenced by reading instability and retention loss in RRAMs. Retention loss in RRAMs could additionally impact the stability of PUF generated IDs [31].

• **True Random Number Generators (TRNG):** True Random Number Generators (TRNGs) have become integral in secure data handling systems and information security. They are crucial in generating parameters for public key cryptosystems (e.g., ECC, RSA), session keys, and many other applications. TRNGs, in contrast to pseudo-random number generators (PRNGs), derive random numbers from unpredictable physical processes, ensuring superior statistical characteristics. While PRNGs are deterministically repeatable and commonly used in simulation and testing, TRNGs offer heightened unpredictability, making them particularly suitable for applications in highly secure systems [32].

Extensive research on TRNGs has been conducted across various domains of non-volatile memories - spintronic devices [33]–[35], FeRAMS [36], etc. MRAM-based TRNGs have gained attention due to their ability to produce high-quality random numbers and robustness [37]–[39]. Researchers have employed partial programming and program disturb characteristics to implement flash-based TRNGs [23], [40]. Piccinini et al. [41] demonstrated the promising use of amorphous PCM arrays for implementing a TRNG in their research. Much research has been especially dedicated to TRNGs based on resistive memories [42]–[45]. The TRNGs based on RRAM exhibit a high entropy source, making them relatively robust and suitable for integration in high-density scenarios. However, practical applications are still hindered by throughput limitations [46]. While aging effects in eNVMs do not compromise the randomness of TRNGs, they may lead to device degradation over time due to continuous cycling. Similarly, aging influences switching-time variability in resistive eNVM devices. It alters the threshold voltage distribution in NOR flash, which could impact device performance or the consistency of TRNG output across the lifespan [47].

Table I: Summary of security solutions based on eNVMs.

	PUF	**TRNG**	**Obfuscation/ Locking**
PCM	[22]	[41]	–
RRAM	[17], [18]	[42], [43], [46]	–
MRAM	[19], [20]	[33], [35], [39]	[49]
FLASH	[23], [51]	[23], [40]	–
FeRAM	[52]	[36]	–

• **Obfuscation and Locking:** The hardware security community has actively addressed the persistent threat of IP piracy stemming from the horizontal integration of semiconductor design, manufacturing, and testing. With the growing complexity of chip design and manufacturing processes, many design houses find it practically infeasible to produce chips independently. This vulnerability in the semiconductor supply chain opens the door for untrusted entities to exploit and pirate design details, leading to irreparable damage. In response to this challenge, logic locking techniques [48] have been proposed as a countermeasure against IP piracy, involving the obfuscation of circuit designs through the use of secret keys.

This research area remains relatively unexplored within the community, particularly in terms of integrating eNVM-based designs. The research work by Divyanshu et al. explores various emerging structures based on 2T/3T MTJ for potential applications in logic locking [49]. Additionally, magnetic skyrmion-based locking solutions were proposed by Guin et al. [50]. Table I shows the summary of studies for security primitives and solutions based on eNVMs.

IV. Security Risks Posed by Embedded NVMs

The integration of emerging eNVMs in contemporary computing systems raises significant concerns about the potential leakage of sensitive information to adversaries. Typically, confidential data like secret keys, login credentials, and credit card information undergo encryption and are stored in hard drives, such as magnetic disks or flash storage. Subsequently, this encrypted data is decrypted on-the-fly and loaded into volatile memories, such as SRAM-based caches, in close proximity to the processor. Historically, precautions were not necessary

as SRAMs and DRAMs lose their content after powering down. However, implementing encryption at the cache level becomes exceedingly challenging. If cache memories become non-volatile, there is a risk of adversaries gaining access to all sensitive information in its raw form. Consequently, addressing data safety concerns in higher memory stack levels while sustaining optimal performance poses a significant challenge.

• **Side-channel attacks:** Side-channel attack (SCA) poses a serious security threat to cryptographic chips used in secure systems. Unlike attacks that target the algorithm itself, SCAs focus on exploiting vulnerabilities in the physical implementation of cryptographic algorithms. NVMs exhibit asymmetric and high read/write currents, where the currents for writing and reading data '1' and data '0' differ, making them prone to SCAs [53]. Various research works have shown that eNVM technologies such as MRAM, FeRAM, PCM, and RRAM can be susceptible to SCAs. Chakraborty et al. [54] demonstrated the vulnerability of MTJ-based implementations of cryptosystems to differential side-channel attacks, in which the adversary leverages multiple traces to extract the secret key. The authors of [55] demonstrated SCA attacks exploiting the seasoning effect in PCM, which is the change in behavior of PCM cells as a function of operational cycles. The vulnerability of IMC architectures implemented using RRAM to SCA was showcased in the study conducted by [56]. FeRAM is also susceptible to SCAs. SCAs compromise the security of data transmitted over communication networks using FeRAMs. Enan et al. [57] studied the effect of SCAs on FeRAMs with noise.

• **Probing:** A probing attack is an invasive technique employed by directly probing a signal wire to extract information from a chip using micro or nanoprobes. During a probing attack, an adversary accesses the internal wires and connections of a targeted device to extract sensitive information. Various emerging physical probing methods can be used to gain unauthorized access or compromise the integrity of stored information in an eNVM device. STT-MRAM cells usually consist of magnetic and non-magnetic layers, placing the magnetic free layer near the middle of the device stack. This deep positioning makes it hard to directly probe the magnetic free layer non-destructively using magneto-optical current imaging (MOCI). Nonetheless, adversaries could potentially address this challenge by taking a cross-sectional image or removing stack layers until they expose the data storage layer. FeRAM may face security risks from scanning microwave impedance microscopy (sMIM) and scanning capacitance microscopy (SCM), which are capable of detecting changes in capacitance and resistance, respectively. Another potential attack method on FeRAM is electron beam-induced resistance change (EBIRCH), where changes in resistance can be measured using tools like electron beam-induced current (EBIC) or electron beam-absorbed current (EBAC) and EBIRCH. PCM could be at risk from conductive atomic force microscopy (CAFM) because it can detect the current state of the material, which varies between amorphous and crystalline states. To execute such an attack, one might need to remove layers until the active layer is exposed. RRAM employing HfO_2 is not susceptible to MOCI due to the absence of ferromagnetic properties. However, if NiO material with ferromagnetic properties is used, RRAM could be vulnerable to MOCI [58].

Table II: Summary of risks associated with eNVMs.

	Side-channel attacks	Probing	Fault injection	Row-hammer
PCM	[55]	[58], [62]	–	–
RRAM	[56]	[58]	[59]	[63]
MRAM	[54], [64]	[58]	[60]	[65], [66]
FLASH	–	–	[61], [67]	–
FeRAM	[57]	[58]	–	–

• **Fault injection attacks:** The supply noise in eNVMs, caused by high and asymmetric write currents, can be exploited for fault injection attacks. By writing a specific data pattern, the attacker can create deterministic supply noise. This noise can then propagate to the memory space of the victim-user, leading to read/write operation failures. In [59], Khan et al. conducted a fault injection experiment on RRAM-based last-level cache (LLC). The high write current of RRAM can lead to supply noise, such as voltage droop and ground bounce. Their study showed that supply noise induced by high write current can transmit to the neighboring banks and affect parallel read/write operation. By manipulating the read/write data patterns, the attacker can influence the magnitude of the supply noise and thus execute a fault injection attack. Note that STT-MRAM is also vulnerable to these attacks because of their significant write/read current usage and extended write latency. Nair et al. [60] also conducted fault modeling on STT-MRAM at the layout level at various voltage and temperature corners. In [61], the researchers applied optical fault injection to extract information stored in Flash memories.

• **Row-hammer attacks:** The Row-hammer attack exploits electromagnetic interference to intentionally flip specific bits in DRAM memories by repetitively accessing particular rows. These deliberate bit-flips contravene a fundamental principle of secure and reliable computing systems: memory isolation, which maintains a strict separation of application memory to prevent unauthorized changes in its internal state. Few studies have investigated the impact of Row-hammer on eNVMs such as STT-MRAM. The reduced thermal barrier in STT-MRAM could result in retention failures and make the bits sensitive to stray magnetic fields and thermal noise. Researchers in [65] investigated the effects of Row-hammer attacks on STT-MRAM using high write current. The effects of this attack on STT-MRAM are not as severe as DRAM, but it can create different types of failures and affect more bit cells. At the same time, Row-hammer attacks can result in retention problems and read disturb issues if read operations are conducted while cells experience disturbed current due to ground bounce. Another adverse effect of this attack is introducing the possibility of read/write failures. The authors of [63] introduced a Row-hammer attack in RRAM crossbars resulting from thermal crosstalk between memory cells in their study. Table II shows the summary of security attacks and vulnerabilities posed by eNVMs.

V. Future Directions

Future research in eNVM technologies can focus on addressing key challenges related to cell-level and device-level reliability, variability, yield, and highly smooth structure

design [1]. One challenge hindering the widespread adoption of eNVMs is the need to lower the cost per bit, which involves enhancing the density of array cells. Many new memory devices use chalcogenide compounds and Ir/Ta-based metal electrodes, which pose challenges for process integration. Research can help optimize processes such as patterning/etching, deposition, and annealing to seamlessly use these compounds [68]. STT-MRAM devices require a reduction of about half the switching current to meet the endurance requirements for last-level cache utilization. This reduction is crucial to ensure that memory cells can handle the repeated write operations needed in these applications [69].

Several challenges remain for implementing eNVM-based security primitives in IoT and integrated systems. These challenges include optimizing devices for high-frequency operation (greater than 1 Gbit/s), low energy consumption per bit, and high endurance (at least 10^{16} cycles). Ensuring compatibility with CMOS technology is crucial for easy integration. Additionally, eNVM devices that form the entropy source for cryptographic roots should be engineered to enhance their stochastic behavior, which is typically undesirable in-memory applications. Research can focus on TRNG schemes that do not require post-processing algorithms or entropy-tracking feedback loops, enabling a more efficient design in terms of area and energy [70].

As the adoption of eNVMs in electronic devices increases, there is a growing need to assess their vulnerability to various security threats. It is important to explore vulnerabilities in devices and beyond, such as potential fault injection from eNVM peripherals. System-level features like wear-leveling could also be exploited for attacks. The security community should consider new attack vectors beyond denial of service and fault injection. Areas such as information leakage in eNVMs require more attention due to the many ways they can be exploited for data leakage. A multi-layered approach is required to enhance eNVM security against physical attacks. One can integrate nanopyramid structures and protective shields at the device level to protect against optical attacks. Material-based approaches like antiferromagnetic materials and superconductors can also be explored. Additionally, carbon nanotube resistance sensors can be integrated for real-time tamper detection [58]. However, one of the most important aspects of mitigating eNVM attacks is developing efficient detection methods. Future research approaches can explore new device engineering techniques that reduce vulnerabilities without adding significant overhead.

VI. Conclusion

This paper explores the security aspects of non-volatile memories in a rapidly expanding electronics industry. eNVMs have gained popularity in secure systems due to their energy efficiency and data retention capabilities. While the security applications and vulnerabilities of eNVMs have been studied individually, this paper provides a comprehensive review of both aspects. The discussion on security primitives like PUFs and TRNGs reveals promising developments in leveraging the properties of eNVMs for secure systems. Additionally, exploring common attacks on embedded eNVMs underscores the need for robust security measures. Looking ahead, future research can focus on enhancing the security of eNVM-based systems. This includes addressing emerging threats and developing more effective security primitives.

References

[1] W. Banerjee, "Challenges and Applications of Emerging Nonvolatile Memory Devices," *Electronics*, no. 6, 2020.

[2] M. R. Mahmoodi, D. B. Strukov, and O. Kavehei, "Experimental Demonstrations of Security Primitives With Nonvolatile Memories," *Transactions on Electron Devices*, no. 12, pp. 5050–5059, 2019.

[3] E. I. Vatajelu, H. Aziza, and C. Zambelli, "Nonvolatile memories: Present and future challenges," in *Int. Design and Test Symposium*, pp. 61–66, 2014.

[4] N. Aswathy and N. Sivamangai, "Future Nonvolatile Memory Technologies: Challenges and Applications," in *Int. Conference on Advances in Computing, Comm., Embedded & Secure Systems*, pp. 308–312, 2021.

[5] J. S. Meena, S. M. Sze, U. Chand, and T.-Y. Tseng, "Overview of emerging nonvolatile memory technologies," *Nanoscale research letters*, pp. 1–33, 2014.

[6] M. N. I. Khan and S. Ghosh, "Comprehensive Study of Security and Privacy of Emerging Non-Volatile Memories," *Journal of low power electronics and applications*, no. 4, p. 36, 2021.

[7] N. Derhacobian, S. C. Hollmer, N. Gilbert, and M. N. Kozicki, "Power and Energy Perspectives of Nonvolatile Memory Technologies," *Proceedings of the IEEE*, no. 2, pp. 283–298, 2010.

[8] R. Bez, E. Camerlenghi, A. Modelli, and A. Visconti, "Introduction to flash memory," *Proceedings of the IEEE*, no. 4, pp. 489–502, 2003.

[9] Y. Fujisaki, "Overview of emerging semiconductor non-volatile memories," *IEICE Electronics Express*, no. 10, pp. 908–925, 2012.

[10] S. Tehrani, J. M. Slaughter, M. Deherrera, B. N. Engel, N. D. Rizzo, J. Salter, M. Durlam, R. W. Dave, J. Janesky, B. Butcher, *et al.*, "Magnetoresistive random access memory using magnetic tunnel junctions," *Proceedings of the IEEE*, no. 5, pp. 703–714, 2003.

[11] M. Le Gallo and A. Sebastian, "An overview of phase-change memory device physics," *Journal of Physics D: Applied Physics*, p. 213002, 2020.

[12] K. Asari, Y. Mitsuyama, T. Onoye, I. Shirakawa, H. Hirano, T. Honda, T. Otsuki, T. Baba, and T. Meng, "FeRAM circuit technology for system on a chip," in *Proceedings of the First NASA/DoD Workshop on Evolvable Hardware*, pp. 193–197, 1999.

[13] V. Gupta, S. Kapur, S. Saurabh, and A. Grover, "Resistive Random Access Memory: A Review of Device Challenges," *IETE Technical Review*, no. 4, pp. 377–390, 2020.

[14] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration Systems*, no. 10, pp. 1200–1205, 2005.

[15] S. Sutar, A. Raha, and V. Raghunathan, "Memory-Based Combination PUFs for Device Authentication in Embedded Systems," *IEEE Transactions on Multi-Scale Computing Systems*, no. 4, pp. 793–810, 2018.

[16] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Proceedings of the 44th annual design automation conference*, pp. 9–14, 2007.

[17] A. Chen, "Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions," *IEEE Electron Device Letters*, no. 2, pp. 138–140, 2014.

[18] A. Mazady, M. T. Rahman, D. Forte, and M. Anwar, "Memristor PUF—A Security Primitive: Theory and Experiment," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, no. 2, pp. 222–229, 2015.

[19] E. I. Vatajelu, G. Di Natale, M. Indaco, and P. Prinetto, "STT MRAM-based PUFs," in *Design, Automation & Test in Eu. Conference & Exhibition*, pp. 872–875, 2015.

[20] J. Das, K. Scott, S. Rajaram, D. Burgett, and S. Bhanja, "MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS," *IEEE Transactions on Nanotechnology*, no. 3, pp. 436–443, 2015.

[21] L. Zhang, Z. H. Kong, and C.-H. Chang, "PCKGen: A Phase Change Memory based cryptographic key generator," in *International Symposium on Circuits and Systems*, pp. 1444–1447, 2013.

[22] N. Noor and H. Silva, "Phase Change Memory for Physical Unclonable Functions," *Applications of Emerging Memory Technology: Beyond Storage*, pp. 59–91, 2020.

[23] Y. Wang, W.-k. Yu, S. Wu, G. Malysa, G. E. Suh, and E. C. Kan, "Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints," in *Symposium on Security & Privacy*, pp. 33–47, 2012.

[24] P.-Y. Chen, R. Fang, R. Liu, C. Chakrabarti, Y. Cao, and S. Yu, "Exploiting resistive cross-point array for compact design of physical unclonable function," in *Int. Symposium on Hardware Oriented Security and Trust*, pp. 26–31, 2015.

[25] P. Koeberl, U. Kocabaş, and A.-R. Sadeghi, "Memristor PUFs: A new generation of memory-based Physically Unclonable Functions," in *Design, Automation & Test in Eu. Conference*, pp. 428–431, 2013.

[26] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, "A write-time based memristive PUF for hardware security applications," in *Int. Conference on Computer-Aided Design*, pp. 830–833, 2013.

[27] J. Das, K. Scott, D. Burgett, S. Rajaram, and S. Bhanja, "A novel geometry based MRAM PUF," in *Int. Conference on Nanotechnology*, pp. 859–863, 2014.

[28] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM," in *Int. symposium on circuits & systems*, pp. 2169–2172, 2014.

[29] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Feasibility study of emerging non-volatile memory based physical unclonable functions," in *Int. Memory Workshop*, pp. 1–4, 2014.

[30] K. Shamsi and Y. Jin, "Security of emerging non-volatile memories: Attacks and defenses," in *VLSI Test Symposium*, pp. 1–4, 2016.

[31] A. Chen, "A review of emerging non-volatile memory (NVM) technologies and applications," *Solid-State Electronics*, pp. 25–38, 2016.

[32] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A Survey on True Random Number Generators Based on Chaos," *Discrete Dynamics in Nature and Society*, pp. 1–10, 2019.

[33] A. Fukushima, T. Seki, K. Yakushiji, H. Kubota, H. Imamura, S. Yuasa, and K. Ando, "Spin dice: A scalable truly random number generator based on spintronics," *Applied Physics Express*, no. 8, p. 083001, 2014.

[34] Y. Liu, Z. Wang, Z. Li, X. Wang, and W. Zhao, "A spin orbit torque based true random number generator with real-time optimization," in *18th International Conference on Nanotechnology*, pp. 1–4, 2018.

[35] Y. Qu, J. Han, B. F. Cockburn, W. Pedrycz, Y. Zhang, and W. Zhao, "A true random number generator based on parallel STT-MTJs," in *Design, Automation & Test in Eu. Conference & Exhibition*, pp. 606–609, 2017.

[36] M. I. Rashid, F. Ferdaus, B. B. Talukder, P. Henny, A. N. Beal, and M. T. Rahman, "True Random Number Generation Using Latency Variations of FRAM," *IEEE Transactions on VLSI Systems*, no. 1, pp. 14–23, 2020.

[37] W. H. Choi, Y. Lv, J. Kim, A. Deshpande, G. Kang, J.-P. Wang, and C. H. Kim, "A Magnetic Tunnel Junction based True Random Number Generator with conditional perturb and real-time output probability tracking," in *International Electron Devices Meeting*, pp. 12–5, 2014.

[38] M. N. I. Khan, C. Y. Cheng, S. H. Lin, A. Ash-Saki, and S. Ghosh, "A Morphable Physically Unclonable Function and True Random Number Generator using a Commercial Magnetic Memory," *Journal of Low Power Electronics and Applications*, no. 1, p. 5, 2021.

[39] E. I. Vatajelu, G. Di Natale, and P. Prinetto, "Security primitives (PUF and TRNG) with STT-MRAM," in *VLSI Test Symposium*, pp. 1–4, 2016.

[40] B. Ray and A. Milenković, "True Random Number Generation Using Read Noise of Flash Memory Cells," *IEEE transactions on electron devices*, no. 3, pp. 963–969, 2018.

[41] E. Piccinini, R. Brunetti, and M. Rudan, "Self-Heating Phase-Change Memory-Array Demonstrator for True Random Number Generation," *IEEE Transactions on Electron Devices*, no. 5, pp. 2185–2192, 2017.

[42] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A Contact-Resistive Random-Access-Memory-Based True Random Number Generator," *IEEE Electron Device Letters*, pp. 1108–1110, 2012.

[43] J. Yang, Y. Lin, Y. Fu, X. Xue, and B. Chen, "A small area and low power true random number generator using write speed variation of oxidebased RRAM for IoT security application," in *Int. symposium on circuits and systems*, pp. 1–4, 2017.

[44] Z. Wei, Y. Katoh, S. Ogasahara, Y. Yoshimoto, K. Kawai, Y. Ikeda, K. Eriguchi, K. Ohmori, and S. Yoneda, "True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM," in *Int. Electron Devices Meeting*, pp. 4–8, 2016.

[45] R. Govindaraj, S. Ghosh, and S. Katkoori, "CSRO-Based Reconfigurable True Random Number Generator Using RRAM," *IEEE Transactions on VLSI Systems*, no. 12, pp. 2661–2670, 2018.

[46] G. Rajendran, W. Banerjee, A. Chattopadhyay, and M. M. S. Aly, "Application of Resistive Random Access Memory in Hardware Security: A Review," *Advanced Electronic Materials*, no. 12, p. 2100536, 2021.

[47] S. Chakraborty, A. Garg, and M. Suri, "True Random Number Generation From Commodity NVM Chips," *IEEE Transactions on Electron Devices*, no. 3, pp. 888–894, 2020.

[48] U. Guin, Q. Shi, D. Forte, and M. M. Tehranipoor, "FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs," *ACM Transactions on Design Automation of Electronic Systems*, vol. 21, no. 4, pp. 1–20, 2016.

[49] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Logic Locking Using Emerging 2T/3T Magnetic Tunnel Junctions for Hardware Security," *IEEE Access*, pp. 102386–102395, 2022.

[50] Y. Zhang, C. Tang, P. Li, and U. Guin, "Camskygate: camouflaged skyrmion gates for protecting ics," in *Proceedings of the 59th Design Automation Conference*, pp. 757–762, 2022.

[51] P. Prabhu, A. Akel, L. M. Grupp, W.-K. S. Yu, G. E. Suh, E. Kan, and S. Swanson, "Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations," in *Trust and Trustworthy Computing: International Conference, Proceedings 4*, pp. 188–201, Springer, 2011.

[52] S. Kim, K. Lee, M.-H. Oh, J.-H. Lee, B.-G. Park, and D. Kwon, "Physical Unclonable Functions Using Ferroelectric Tunnel Junctions," *IEEE Electron Device Letters*, no. 6, pp. 816–819, 2021.

[53] M. N. I. Khan, S. Bhasin, B. Liu, A. Yuan, A. Chattopadhyay, and S. Ghosh, "Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories," *Journal of Low Power Electronics and Applications*, no. 4, p. 38, 2021.

[54] A. Chakraborty, A. Mondal, and A. Srivastava, "Correlation power analysis attack against STT-MRAM based cyptosystems," *Cryptology ePrint Archive*, 2017.

[55] L. Xu, W. Shi, and N. Desalvo, "Seasoning effect based side channel attacks to AES implementation with Phase Change Memory," in *Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy*, pp. 1–8, 2014.

[56] S. S. Ensan, K. Nagarajan, M. N. I. Khan, and S. Ghosh, "SCARE: Side Channel Attack on In-Memory Computing for Reverse Engineering," *Transactions on VLSI Systems*, no. 12, pp. 2040–2051, 2021.

[57] A. Enan and M. I. H. Bhuiyan, "Investigation of Side Channel Leakage of FeRAM Using Discrete Wavelet Transform," in *International Conference on Telecommunications and Photonics*, pp. 1–4, 2019.

[58] L. K. Biswas, M. Shafkat, M. Khan, L. Lavdas, and N. Asadizanjani, "Emerging Nonvolatile Memories—An Assessment of Vulnerability to Probing Attacks," in *ISTFA*, pp. 217–224, 2022.

[59] M. N. I. Khan and S. Ghosh, "Fault injection attacks on emerging non-volatile memory and countermeasures," in *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy*, pp. 1–8, 2018.

[60] S. M. Nair, R. Bishnoi, M. B. Tahoori, G. Tshagharyan, H. Grigoryan, G. Harutyunyan, and Y. Zorian, "Defect injection, Fault Modeling and Test Algorithm Generation Methodology for STT-MRAM," in *International Test Conference*, pp. 1–10, 2018.

[61] F. Cai, G. Bai, H. Liu, and X. Hu, "Optical fault injection attacks for flash memory of smartcards," in *Int. Conference on Electronics Information and Emergency Communication*, pp. 46–50, 2016.

[62] S. Kannan, N. Karimi, O. Sinanoglu, and R. Karri, "Security Vulnerabilities of Emerging Nonvolatile Main Memories and Countermeasures," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, no. 1, pp. 2–15, 2014.

[63] F. Staudigl, H. Al Indari, D. Schön, D. Sisejkovic, F. Merchant, J. M. Joseph, V. Rana, S. Menzel, and R. Leupers, "NeuroHammer: Inducing Bit-Flips in Memristive Crossbar Memories," in *Design, Automation & Test in Europe Conference & Exhibition*, pp. 1181–1184, 2022.

[64] M. N. I. Khan, S. Bhasin, A. Yuan, A. Chattopadhyay, and S. Ghosh, "Side-Channel Attack on STTRAM Based Cache for Cryptographic Application," in *Int. Conference on Computer Design*, pp. 33–40, 2017.

[65] M. N. I. Khan and S. Ghosh, "Analysis of Row Hammer Attack on STTRAM," in *International Conference on Computer Design*, pp. 75–82, 2018.

[66] S. Agarwal, H. Dixit, D. Datta, M. Tran, D. Houssameddine, D. Shum, and F. Benistant, "Rowhammer for Spin Torque based Memory: Problem or not?," in *International Magnetics Conference*, pp. 1–1, 2018.

[67] K. Garb and J. Obermaier, "Temporary Laser Fault Injection into Flash Memory: Calibration, Enhanced Attacks, and Countermeasures," in *Int. Symposium on On-Line Testing & Robust System Design*, pp. 1–7, 2020.

[68] J. Choe, "Memory Technology 2021: Trends & Challenges," in *Int. Conference on Simulation of Semiconductor Processes and Devices*, pp. 111–115, 2021.

[69] M. Si, H.-Y. Cheng, T. Ando, G. Hu, and P. D. Ye, "Overview and outlook of emerging non-volatile memories," *Mrs Bulletin*, no. 10, pp. 946–958, 2021.

[70] R. Carboni and D. Ielmini, "Stochastic Memory Devices for Security and Computing," *Advanced Electronic Materials*, no. 9, p. 1900198, 2019.