IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 February 2024, accepted 8 May 2024, date of publication 13 May 2024, date of current version 21 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3400624

SURVEY

Era of Sentinel Tech: Charting Hardware Security Landscapes Through Post-Silicon Innovation, Threat Mitigation and Future Trajectories

MAMIDIPAKA B. R. SRINIVAS AND KONGUVEL ELANGO, (Senior Member, IEEE)
School of Electronics Engineering, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu 632014, India

Corresponding author: Konguvel Elango (konguvel.e@vit.ac.in)

This work was supported by the Vellore Institute of Technology, Vellore, Tamil Nadu, India.

ABSTRACT To meet the demanding requirements of VLSI design, including improved speed, reduced power consumption, and compact architectures, various IP cores from trusted and untrusted platforms are often integrated into a single System-on-Chip (SoC). However, this convergence poses a significant security challenge, as adversaries can exploit it to extract unauthorized information, compromise system performance, and obtain secret keys. Meanwhile, traditional CMOS features have limitations in addressing hardware vulnerabilities and security threats, so promising post-silicon technologies offer potential solutions. Beyond-CMOS technologies offer avenues to fortify hardware security through distinct physical properties and nontraditional computing paradigms. These advancements bolster authentication processes, enhance key generation mechanisms, ensure hardware integrity and fortify resilience against side-channel attacks, hardware Trojans and quantum-resistant cryptography in securing hardware systems. This article provides a detailed review of hardware security, encompassing the identification and mitigation of threats, the implementation of robust countermeasures, the utilization of innovative primitives, countermeasures, various methodologies and distinct features offered by emerging technologies to resist hardware threats. Moreover, strategies to address challenges, explore future directions, and outline plans for achieving further research outcomes have been put forth in this field.

INDEX TERMS Dual precharge logic (DPL), fault injection attacks (FIA), hardware wallets (HW), negative capacitance FET (NCFET), measurement-to-disclosure (MTD), spintronics, sense amplifier-based logic (SABL), tamper resistance, temporal majority voting (TMV).

I. INTRODUCTION

Cyber-attacks have become increasingly sophisticated and persistent, targeting both software and hardware vulnerabilities. The evolving threat landscape in the modern life of digitization necessitates the adoption of hardware security measures. Attackers aim to compromise systems and gain unauthorised access to private information. The threats connected to the major US healthcare data breaches disclosed during the COVID outbreak [1]. This highlights the critical role of hardware security in mitigating such threats. Moreover, the modern design landscape exhibits a growing dependence on various components including, architectures, intellectual property, and hardware accelerators embedded in SoCs to enhance the performance of the system. This reliance further amplifies the need for robust hardware security measures. With the proliferation of Internet of Things (IoT) devices and interconnected systems, hardware security becomes particularly vital. These devices are extensively deployed in sectors such as critical infrastructure, healthcare, financial transactions and transportation, where the security and integrity of the hardware are of utmost importance. Thus, safeguarding these devices against tampering, unauthorised access, and potential disruptions is crucial, underscoring the necessity of hardware security.

With the rapid proliferation of IoT devices, ensuring security has become imperative. The inherent vulnerabilities in IoT systems necessitate powerful security protocols to protect

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed M. Elmisery.

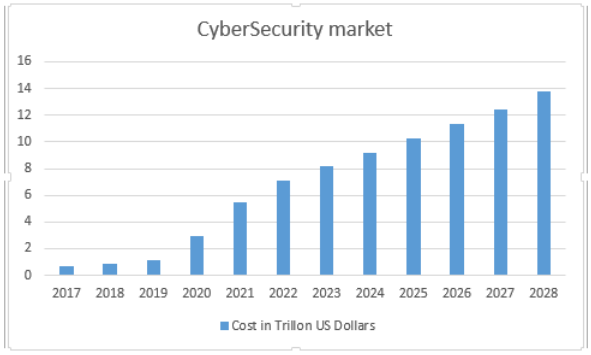

FIGURE 1. Forecast of the cyber security market.

against potential threats and breaches. Therefore, prioritizing ultra-low power consumption and high-speed capabilities, and addressing security concerns has become an essential requirement for IoT devices and systems [2], [3], [4]. In modern times, there has been a significant rise in economic losses resulting from the escalation of cyberspace, hardware assaults and breaches in information and communication systems. The increasing frequency and sophistication of these assaults pose a significant peril to the integrity and security of critical platforms. Consequently, mitigating and preventing cyber and hardware breaches has become a pressing concern for organizations operating in information and communication domains, aiming to safeguard their assets, reputation, and financial stability [5], [6]. Hardware breaches can have significantly more severe consequences compared to cyber security attacks, primarily because software inherently relies presuming that the hardware below isn't compromised. While cyber security attacks can cause disruptions and compromise software systems, hardware breaches have the potential to undermine the foundation on which software operates. This fundamental reliance on uncompromised hardware makes it crucial to prioritize hardware security as any compromise can lead to widespread vulnerabilities throughout the software ecosystem. Therefore, the damaging impact of hardware breaches stems from their ability to undermine the trust and integrity of the underlying hardware, thereby posing significant challenges for ensuring the security and reliability of software systems [7], [8], [9], [10], [11]. As a result, numerous polls have revealed the expense of cyber security as shown in Figure. 1 [12].

It's important to note that attackers continually evolve their techniques, and new attack vectors may emerge over time and weaken the effective performance and efficiency of hardware systems. The various security attacks impact hardware/software such as Hardware Trojans, supply chain attacks, side-channel attacks, physical tampering, hardware key loggers, electromagnetic and photonic attacks, Direct memory access attacks (DMAA), Hardware Interceptions, Fault injection attacks, malicious firmware, Hardware based crypto-attacks, Bus snooping, counterfeiting of IC, machine learning models are some examples of hardware-related security attacks.

TABLE 1. List of abbreviations used in this article.

Abbreviation	Description
CAD	Computer Aided Design
CMOS	Complementary Metal Oxide Semiconductor
SoC	System on Chip
VLSI	Very Large Scale Integrated Circuits
IP core	Intellectual property core
DPL	Dual Precharge Logic
FIA	Fault Injection Attacks
HW	Hardware Wallets
HSM	Hardware Secure Models
IoT	Internet Of Things
MTD	Measurement-To-Disclosure
TMV	Temporal Majority Voting
NCFET	Negative Capacitance Field Effect Transistor
SABL	Sense Amplifier Based Logic
DMAA	Direct Memory Access Attacks
TRNGs	True Random Number Generators
PUFs	physical Unclonable Functions
PCM	Phase Change Memory
TFET	Tunnel Field Effect Transistor
RRAM	Resistive random-access memory
CNTFET	Carbon Nanotube FET
STT-MJT	Spin Transfer Torque Magnetic tunnel junction
HyperFET	Hybrid Phase Transition FET
FSC-PCs	Fluorescence Structural Colour Phonotic Crystals
TEEs	Trusted Execution Environments
SRAM	Static random-access memory
NVM	Non-Volatile Memory
OS	Operating System
PUF-SSTFs	PUF-Secure Split Test with functional testing
CSST	Connecticut Secure Split Test
STDs	Spin Torque Diodes
DPA	Differential Power Analysis
SOT	Spin-Orbit Torque
SiNW-FET	Silicon Nanowire-FET
FPGA	Field Programmable Gate Array
PCB	Printed Circuit Board
SAR-ADC	Successive Approximation Register - ADC
CRO-PUF	Configurable Ring Oscillator PUF
RACRO-PUF	Robust Architecture CRO-PUF

In summary, hardware security is essential for protecting data, defending against cyber threats, and ensuring the reliability of systems in real-time applications across industries. It fosters trust, resilience, and compliance with regulations while mitigating risks in the supply chain. By safeguarding against unauthorized access and ensuring regulatory compliance, hardware security enhances the overall security posture of organizations across diverse sectors.

II. LITERATURE REVIEW

Hardware security plays a pivotal role in real-time contexts by safeguarding sensitive data, thwarting cyber attacks, and bolstering the reliability of systems. It provides resilience against sophisticated threats, ensures compliance with regulations, and mitigates risks in the supply chain. Through features like tamper resistance and secure elements, hardware security maintains data confidentiality, integrity, and availability, bolstering organizational security across various sectors.

CMOS circuits, designed for stability and consistency, struggle to generate truly random outputs required for True Random Number Generators (TRNGs). While they

may exhibit some variability due to environmental noise and process variations, this randomness often falls short of cryptographic standards. Additionally, CMOS circuits are ill-suited for Physical Unclonable Functions (PUFs), as they minimize variations to ensure consistent performance, hindering the diversity needed for effective PUF functionality. Moreover, the sensitive nature of CMOS circuitry and the intricate interplay of electrical signals make them susceptible to side-channel attacks, allowing adversaries to exploit vulnerabilities and extract valuable information.

To overcome these limitations the advantages of post-CMOS technologies in hardware security stem from their ability to address the limitations of traditional CMOS technology while also providing opportunities for the development of more robust, resilient, and future-proof security solutions.

The road map to security devices with the unique features of post-silicon devices has been discussed, along with the most recent design strategies used by designers to address security threats, vulnerabilities, and their solutions [13], [14], [15], [16]. Security experts have been working incredibly hard to create unique hardware security techniques for all various types of above-listed attacks [17], [18], [19], [20], [21], [22].

Addressing the challenges inherent to CMOS technology, only a handful of review papers have explored selective hardware primitives, with little focus on resilience against machine and deep learning models. For the first time, this article delves into recent advancements in device modelling, leveraging improved security features, resistance to emerging threats, and enhanced performance. The overall related works is summarized in Table 2. The aim is to offer state-of-the-art countermeasures for threats against hardware security, paving the way for the development of more robust, resilient, and future-proof security solutions.

The primary contribution of this paper lies in its exploration of recent advancements in hardware security primitives, particularly focusing on enhanced device characteristics such as RRAM, STT-MJT, NCFET etc. For instance, leveraging RRAM, a TRNG has been engineered to mitigate vulnerabilities to hardware attacks while enhancing throughput and reducing power consumption compared to conventional devices [161] and so forth. Building upon the foundation laid by previous research, the article introduces novel enhancements to security primitives, further fortifying their resilience against machine learning attacks. By shedding light on the symbiotic relationship between hardware security primitives and machine learning attacks, the article contributes to advancing the field's understanding of robust security solutions in the era of evolving cyber threats. Moreover, the article paves the way for the development of more secure and efficient hardware implementations, with implications spanning across various domains, including cybersecurity, IoT and beyond.

The presentation of the article is structured as follows. Firstly, We present a quick explanation of the essential hardware security properties in Section III. Then the distinct qualities and most recent developments in post-silicon technology in section IV. Next describes the hardware security measures that are regularly employed to counter security threats along with current developments to mitigate hardware threats and vulnerabilities with next-generation computing devices which have been listed in Section V. Section VI highlights the recent advancements of machine learning in hardware security. Additionally, some contemporary challenges and prospects in the mentioned areas have been highlighted in Section VII. Section VIII emphasizes an overview and discussion of security modules based on post-silicon devices. Section IX with future research directions. At last, section X ended with the conclusion of this article.

III. COMMON HARDWARE SECURITY FEATURES

For data processing in electronics to be vulnerable to numerous risks and vulnerabilities, it is necessary to have confidentiality, integrity, availability, isolation, reliability, constant time, and quantitative security features in designing Hardware Wallets (HW), and Hardware Secure Models (HSM). Common hardware security properties refer to the key aspects or goals that are typically desired and pursued when designing and implementing secure hardware systems. These properties aim to protect against various threats and vulnerabilities. These security attributes also lay out significant constraints to the verification tools for design. These features aim to help hardware designers and CAD tool developers reduce the time and cost of developing secure products by taking into account the latest advancements in terms of hardware security [13], [23]. Here are some common hardware security properties:

A. TAMPER RESISTANCE

Tamper resistance is a fundamental hardware security property that aims to avoid unauthorized physical permission to the device and protect it from tampering or reverse engineering. Tamper-resistant hardware employs techniques such as secure enclosures, anti-tamper coatings, sensors, and meshing to detect and respond to tampering attempts, including opening the casing or probing the device. One of the various kinds of security enclosures the forward integrity model is followed by a logging system with tamper-evident, which safeguards the integrity of logging data collected in former times [24]. Attackers may have the ability to alter the historical logging data produced, Yet the tamper-evident system will identify any breach in integrity. Several instances of tamper-evident systems developed with various technologies and applications are discussed [25], [26], [27]. For instance, in anti-tampering coatings, the spray coating technique produced Fluorescence-Structural Colour Photonic Crystals (FSC-PCs) in a limited period by chemically joining fluorescent molecules to colloidal particles, a two-sided security card with different information displayed on each side depending on the amount of light. Data encryption and reading are both possible during the light-switching process,

TABLE 2. Overview of the proposed work with respect to previous works in Beyond-CMOS for hardware security.

year & Ref	Post-CMOS technologies discussed	Hardware Primitives Discussed	Methodology	Research Gap	Future Research
2016 [337]	Nano Electro Mechanical Systems (NEMS) and Carbon Nanotube (CNT)	Hardware Trojans,Side channel Attack Analysis,Camouflaging	The methodology addresses IC vulnerabilities, resilience against hardware Trojans, power-based side-channel attacks, and IP reverse-engineering via camouflaging on emerging technologies.	Not Discussed	Future research may validate findings with IC measurements, characterize emerging devices, and develop methods for consistent device traits amid process variations, bolstering resilience against security threats. .
2017 [338]	PCM,Graphene,CNTs	PUFs,TRNGs,Design for Anti-Tamper, Anti-Counterfiet, Anti-Reverse Engineer	The methodology explores features and security applications of emerging nanoscale devices (PCM, graphene, CNTs), addressing challenges, limitations, and providing a roadmap. It also highlights open questions and future research in nanoscale security.	Not Discussed	paper suggests overcoming manufacturing challenges, ensuring security against attacks and data leaks, and promoting multidisciplinary collaboration for informed device design. .
2019 [339]	EmergingFlash,PCM, RRAM,Spintronics	PUFs	The methodology discusses security services for connected devices and IoT, considering architectures with mature and emerging technologies. It emphasizes experimental works with a review of security and performance metrics.	The paper identifies gaps in resilience to probing attacks, calls for more experimental research to address evaluation challenges and model various attacks, and advocates for large-scale NVM-based PUFs fully integrated with CMOS circuits, resistant to noninvasive attacks.	Not Discussed .
2021 [13]	(i) spintronics, (ii) memristors, (iii) CNT (iv) nanowires and (v) 3D and 2.5D integration.	Reverse Engineering,Tampering,Theft of IP, Hardware Trojans,Physical Attacks, Data Security, PUFs,TRNGs,Logic Locking,Split Manufacturing, Camouflaging and Root of Trust	The methodology surveys hardware security, assesses emerging technologies, explores their role in improving security, highlights challenges, and evaluates their alignment with hardware security needs	Integrating security early for emerging technologies in CMOS integration promotion.Identifying weak links in hybrid security scheme implementations	Not Discussed .
2021 [14]	Not Discussed	Reverse Engineering,Tampering, Theft of IP, Hardware Trojans, Physical Attacks, Data Security, PUFs,TRNGs, Side Channel Attacks(Timing,EM,Power,Phonotics), Logic Locking, Split Manufacturing, Camouflaging and Root of Trust	The methodology covers protection techniques, design tools for detecting hardware vulnerabilities, and the importance of understanding hardware security threats. It discusses the need for better design tools, common security properties, hardware attacks, security mechanisms, and secure hardware design tools from academia and industry.	Security in hardware design needs improvement, with better tools, standardized models, and effective metrics necessary. Integrating security alongside traditional parameters presents promising but challenging research directions.	Integrate security into IoT/CPS systematically, develop tools for balancing security with other parameters, ensure sensor/actuator security, address COTS component security, secure AI/ML techniques, and establish accessible security metrics. .
2021 [15]	TFET,PCM,CNTFET, STT_MJT,RRAM, HyperFET	PUFs,TRNGs, Side Channel Analysis(EM,Power,Phonotics), Hardware Obfuscations	The methodology discusses nanoelectronic device principles, CMOS challenges, emerging nanotechnologies' benefits, and analyzes post-CMOS device performance in countermeasures.	The paper identifies gaps in device models, circuit availability, metrics for security assessment, engineers' knowledge, and post-CMOS device security study. It also discusses challenges and benefits of post-CMOS devices for hardware security.	The paper recommends researching integrated device architectures to optimize beyond-CMOS device benefits, focusing on improving tunneling efficiency in TFETs. It highlights the potential of NC-TFET and PC-TFET for lower energy consumption and steeper subthreshold swing without leakage degradation. .
2023 [340]	Not Discussed	Power analysis attack on AES designs	The methodology entails researching countermeasures to mitigate AES vulnerabilities against side-channel attacks, particularly focusing on power analysis in IoT devices. It involves examining security metrics and design overheads of countermeasures employing hiding or masking techniques, with a prerequisite understanding of AES algorithm and Galois field theory. The study is specifically scoped to address power analysis attacks targeting IoT devices secured with AES encryption.	Research Gap not identified	Future research should prioritize strengthening AES designs against evolving threats such as EM-based attacks, leakage power analysis attacks, and frequency-domain CPA. Additionally, there's a necessity to investigate methods for reducing design overheads without compromising security levels in countermeasure designs.
2023 [341]	Not Discussed	Microarchitectural Side-Channel Threats	The article encompass presenting a comprehensive overview of microarchitecture security research efforts, introducing a classification scheme for recent research, providing extensive coverage of published works from the past five years, and identifying areas of active and less-explored research. Additionally, the paper aids in the security-oriented architectural process by categorizing relevant primary studies into Metrics, Modeling, and Assessment; Design flow and Synthesis; Verification; and Miscellaneous.	The research identified gaps in consolidating current microarchitecture security research and in comparing studies due to methodological variations. Additionally, it highlighted the need for improved security in trusted computing mechanisms like Intel SGX without sacrificing performance and emphasized the ongoing challenge of balancing system performance and security amidst methodological limitations in systematic mapping studies.	Identified gaps include outdated efforts in compiling microarchitecture security research and challenges in comparing works due to diverse methodologies. There's a need for enhanced security in trusted computing mechanisms like Intel SGX with minimal performance impacts. Ongoing research emphasizes the challenge of balancing system performance and security. Methodological hurdles in mapping studies underscore the need for improvement in study quality and scope.
2023 [342]	Not Discussed	only on Arbiter-PUFs	The methodology includes implementing the fundamental Arbiter PUF design on ZedBoard to assess its performance under various response lengths. Furthermore, it involves scrutinizing the design, components, attributes, and susceptibilities to machine-learning attacks.	The research identified gaps in consolidating current microarchitecture security research and in comparing studies due to methodological variations. Additionally, it highlighted the need for improved security in trusted computing mechanisms like Intel SGX without sacrificing performance and emphasized the ongoing challenge of balancing system performance and security amidst methodological limitations in systematic mapping studies.	Future research directions in PUF technology may involve investigating Composite PUFs, combining RO PUFs and APUFs, creating digitized variants of APUFs such as Mem-APUF, and exploring composite PUF configurations like LP-PUF.
Proposed Work	TFET,PCM,CNTFET, STT-MJT, Silicon Nanowire, Memristors,NCFET, HyperFET	TRNGs, PUFs(Ring Oscillator,Arbiter, Strong,Weak, Memory based PUFs),Side Channel Analysis(Power, EM,Timing),Hardware Trojan and IP protection(Hardware Water marking, Logic Obfuscation, Split Manufacturing)	The methodology covers nanoelectronic device principles, emerging nanotechnologies' benefits, recent advancements in device level, and analyzes post-CMOS device performance in countermeasures. It includes protection techniques, highlights an understanding of hardware security threats, and discusses common security properties, attacks, and mechanisms. Additionally, it explores hardware primitives resilient to machine and deep learning models in TRNG, PUFs, and side-channel attacks.	Discussed in "Challenges and opportunities in hardware security using emerging devices" section	Discussed in "Future research direction section" .

which can be used to present completely distinct information. The FSC-PCs, which have a quick and easy construction procedure and special optical characteristics, have enormous potential for data display and anti-counterfeiting [28]. The method makes use of temperature readings for evaluation, where it is desirable to lessen reliance on external measuring apparatus to facilitate the integration of embedded testing and activity monitoring. Over the lifespan of a chip. As a first step toward achieving HT detection through on-chip power monitoring with a focus on temperature-based analysis, a completely differential temperature sensor was introduced in this paper [29]. A temperature sensor designed with full differential configuration that uses chopper stabilized amplification was developed by modifying the input currents in the differential configuration of BJT being utilized as temperature sensors, the suggested two-stage trans-impedance there has been a modification to the amplifier architecture built utilizing a chopping technique to mitigate flicker noise, the signal-to-noise ratio has greatly improved, according to simulation data [30].

B. SECURE KEY STORAGE

Secure key storage is critical for cryptographic operations and maintaining the confidentiality and integrity of sensitive data. Hardware security properties often include mechanisms for securely generating, storing and managing cryptographic keys within the hardware device. These mechanisms can involve dedicated secure elements, hardware-based key storage, or Trusted Execution Environments (TEEs) that provide secure isolation for key management. Farha et al. [31] have made experiments and improvements of SRAM-PUF, and the use of PUF to secure Zig Bee devices. The authors have demonstrated the efficacy of SRAM-PUF in safeguarding keying materials of Zig Bee devices, Whether through the generation of secret keys or the secure storage of secret keys in the NVM of the local device, with no requirement for the installation of additional equipment. The proposed HSM in [32] eliminates by storing cryptographic keys and the susceptibility to attacks against these stored keys is eliminated. The HSM generates the cryptographic key from sub-components exhibiting similar to multi-factor authentication, where each factor is an independent authenticator. The proposed scheme improves security by integrating physical security into digital security. In other words, as long as either the crypto provider device stays secure or the human aspect is maintained component stays protected, maintaining the integrity of the system security. The authors in [33] implemented a secure monitor for isolation and capability management, which provides data-flow isolation and control-flow isolation to protect a COLONY's data within the context of memory and CPU and prevent untrusted system software preventing the circumvention or incomplete execution of COLONY's code. The paper also assigns capabilities to each instance of COLONY to access essential system-level semantics, do not protect keys from extraction when the key is at rest and stored in an inactive state. However, the work produced by Han et al. [34] provided uses with multiple security features, such as Intel SGX and HSM commands, to set up a secure channel and restrict to regulating key attributes of keys within an HSM to control key usage. ScaleTrust also applies authenticated encryption to all keys during transmission, which prevents sensitive data leakage and defends against active attacks manipulating data messages. Additionally, Scale Trust guarantees encryption for all keys between the enclave and the HSM, which makes it resistant to eavesdropping.

C. SIDE-CHANNEL ATTACK RESISTANCE

Side-channel attacks leverage unintended information leakage during cryptographic operations, such as power consumption, electromagnetic emissions, or timing measurements. Hardware security properties aim to mitigate side-channel attacks by implementing countermeasures such as power analysis resistance, electromagnetic shielding, randomization techniques, and constant-time algorithms to eliminate or minimize the leakage of sensitive information. The proposed technique from the paper [35] uses an on-demand current equalizer modulating the equalization current to obscure information about current leakage of the Advanced Encryption Standards (AES) engine. Additionally, the on-demand current equalizer is proposed to incorporate a randomization operation to further enhance the Power Side Channel Attacks (PSCA) resistance of the cryptographic engine, unlike former works that enable the randomization process in the Integrated Voltage Regulator (IVR). This approach can add additional obfuscation to the current profile of the encryption engine to enhance its PSCA resistance without incurring any performance penalty.

D. HARDWARE AUTHENTICATION

Hardware authentication properties focus on verifying the authenticity and integrity of the hardware device itself. These properties often involve hardware-based secure elements or secure boot processes that ensure only trusted and authorized hardware components are used and that the device hasn't been tampered with or modified. The method in the paper [33] involves modifying the boot loader to load a secure monitor instead of a secure OS. The secure monitor initiates the protected environment and loads a secure OS to memory. The secure OS initiates the secure environment and shifts to the normal environment to execute a kernel loader. The kernel loader initiates the loading of a non-secure operating system and executes it. Upon loading each binary image, the loader computes the checksum to ensure the integrity of the image. The booting order remains static, with the secure OS running first to initialize the platform. The three properties that are enforced require that the boot loader is loaded from a tamper-resistant ROM, the secure OS is loaded and initialized before the non-secure OS, and every time a loader loads a binary

image, it computes the checksum to verify the integrity of the image.

E. PHYSICAL UNCLONABILITY

Physical Unclonability is a property that leverages unique physical characteristics or manufacturing variations in the hardware to provide device identity and protection against cloning or counterfeiting. As semiconductor industry's globalization has produced a convoluted supply chain comprising numerous contract manufacturers in various nations. Outsourced Semiconductor Assembly and Test (OSAT) facilities are now producing counterfeit semiconductors, overbuilding chips from foundries and other security-related issues. Hardware security properties can include measures such as incorporating PUFs or other hardware-based techniques to ensure each device has a unique identity that cannot be easily replicated. So the PUF-SSTF scheme incorporates PUFs to generate random numbers that are used to scramble the test response and generate functional keys. PUFs are used to generate an enormous number of legitimate functional keys for a millions of IoT nodes, which makes it difficult for attackers to clone or counterfeit the ICs. The PUF-based SSTF scheme is a reliable solution for the identity management of IoT devices post-deployment in the field. The security analysis for PUF-SSTF covers both test response locking and functional keys across recognized benchmark circuits, and the results obtained are comparable with the CSST scheme [36].

F. SECURE COMMUNICATION INTERFACES

Hardware security properties encompass secure communication interfaces, including encryption, authentication, and secure protocols for data transfer. These properties focus on protecting data integrity and confidentiality during communication between hardware devices or with external systems, in many cores with shared memory, the Gossip-Network on chip (Gossip-NoC), Reinbrecht et al. [37] employ Secure Zones (SZs) as the defence strategy. The traffic monitors added by the authors enable the Gossip-NoC routers to switch from XY to YX when they see unusual activity. Additionally, Grammatakakis et al. [38] secure the system from unwanted access to shared memories by utilizing firewalls inside the Network Interfaces (NIs). Only specific memory locations are permitted access thanks to the firewall configuration. Attack attempts are recorded by the NI and sent to the Security Event Correlation (SEC) agent, a thread on the host CPU. The Network-On-Chip (NoC) and firewall are installed in the programmable logic on a Zed board with an ARM Cortex A9 (host CPU) in use by the authors. The SEC oversees the protective measures [39].

G. SECURE DEBUGGING AND TESTING

Secure debugging and testing properties involve mechanisms that protect against unauthorized access, tampering, or exploitation during the development, testing, and maintenance phases. Hardware security properties may include secure access control, encrypted debug interfaces, and secure testing processes to prevent unauthorized individuals from accessing sensitive areas of the hardware or injecting malicious code during debugging or testing. The great controllability and observability that the JTAG standard, also known as IEEE 1149.1, offers for ICs makes it useful for debugging and testing. It provides good observability and controllability for users to access the Test Data Registers (TDRs) and Boundary-Scan Cells (BSCs) through the Test Access Port (TAP). As a result, users can test and debug ICs using a variety of techniques, including post-silicon debugging, chip reconfiguration, verification, power management, and clock control [40].

H. SECURE BOOT AND FIRMWARE INTEGRITY

Secure boot and firmware integrity properties aim to ensure that the device starts up with trusted and unmodified firmware or software. These properties include measures such as secure boot processes, firmware encryption, digital signatures, and secure firmware update mechanisms to protect against unauthorized modifications or the installation of malicious firmware. For embedded devices, firmware encryption can stop the firmware from being read to copy the device into a fake or to steal the creator's intellectual property. Additionally, the integrity is protected to prevent an attacker from maliciously altering the firmware. In [41] illustrates a cryptographic concept for implementing Secure Boot capabilities using the inherent features of a particular hardware device.

In, summary FSC-PCs promise improved tamper resistance, while fully differential temperature sensors show potential for detecting hardware Trojans. ScaleTrust's secure key storage addresses insider threats and scalability, focusing on optimization and advanced encryption. Additionally, lightweight power side-channel attack protection utilizes on-demand current equalizers for enhanced key resistance. Trusted execution environments like COLONY ensure hardware authentication, while integrating PUFs enhances IoT semiconductor security. Future efforts focus on optimization and advanced designs for stronger security and resilience. These are some of the common hardware security properties that help mitigate various threats and vulnerabilities. Implementing these properties contributes to building robust and secure hardware systems that can withstand attacks and protect sensitive data and functionality.

IV. UNIQUE CHARACTERISTICS AND MOST RECENT ADVANCEMENTS IN POST-SILICON TECHNOLOGY

A. TUNNEL FIELD EFFECT TRANSISTOR (TFETS)

Everyone is indeed required with low-power application devices and inexpensive transistors are essential for the technological world of today. A 3 nm MOSFET nanoelectronic device has just been created by investigators. Even though MOSFET reduces size and power consumption, there are still

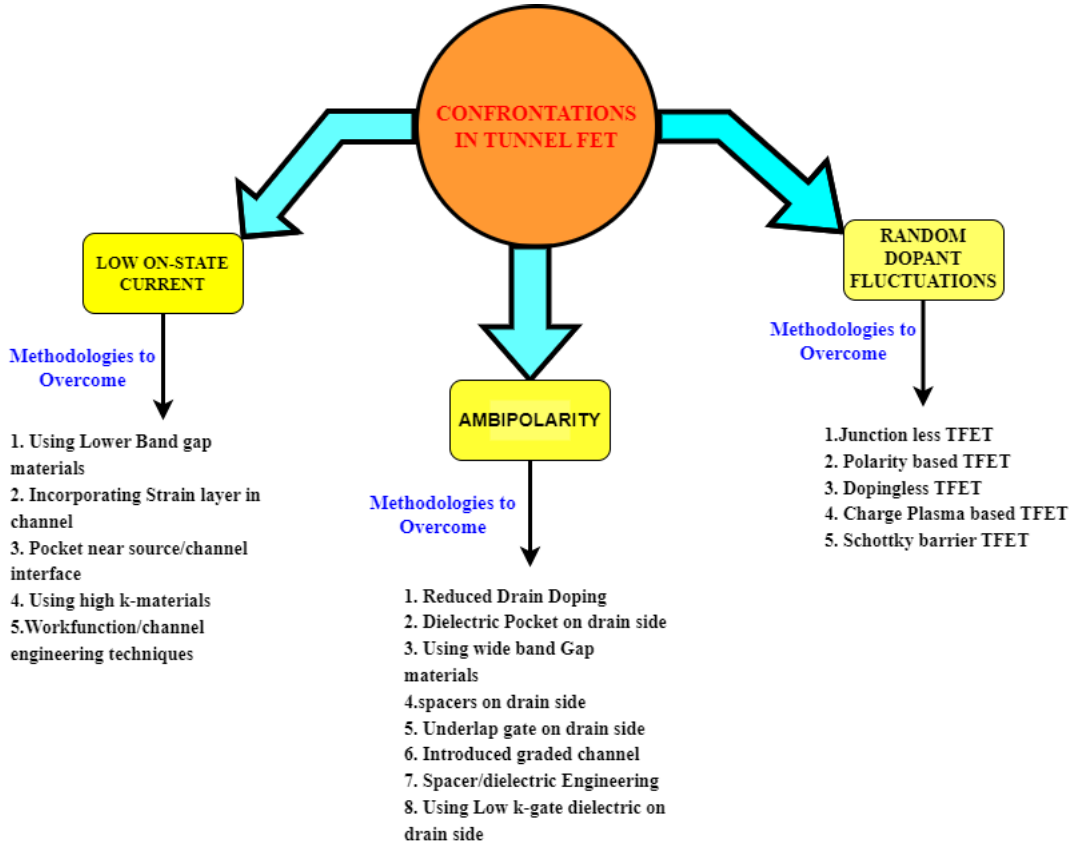

FIGURE 2. Confrontations and possible solutions.

certain problems because of Short Channel Effects (SCEs) like a hot electron, channel length modulation, leakage current, off-state current, threshold voltage roll-off, sub-threshold slope is more than 60mv/dec, impact Ionization, Drain Induced Barrier Lowering (DIBL), and some other processes. Energy efficient TFETs are regarded as a promising technology for future generation circuit devices and hardware security applications in contrast to the conventional MOSFET with impeccable characteristics. Having a low sub-threshold swing $<$ 60mv/dec of an established limit, which implies that they can more quickly transition between the current on and off phases, is advantageous for low-power hardware security applications because it permits operation that is both energy-efficient and has a sufficient level of performance. Because the I_{on} and I_{off} currents weren't improved simultaneously, our various classic heterojunction TFETs couldn't fulfil the demands for the better performance of TFETs, but with a Near Broken-Gap Heterojunction (NBGH) at the source/channel interface, a linearly graded channel component and a novel Graded-Channel Heterojunction TFET (GCH-TFET) [42] is presented to aid in the use of IOT applications [43] and still there are many engineering techniques used for various applications in all ways.. Comparing TFETs to traditional CMOS transistors surpasses the restrictions imposed by the CMOS transistor, Because of this reason it has gained interest among researchers. The quantum tunnelling process in the TFETs, namely band-to-band tunnelling (BTBT) across the source-channel interface, which decreases the short-channel effects and improves the Subthreshold Slope (SS) lower than 60mv/dec [44], [45]. Inspite of the advantages mentioned above TFET also have drawbacks such as low-on current, ambipolar conduction, and random doping fluctuations. Many researchers have proposed several techniques to overcome these shortcomings in TFETs. The possible challenges and solutions for these particular drawbacks are shown in Figure.2 [46], [56]. The other side of TFET also has some special characteristics that may make them less vulnerable to specific side-channel attacks, in the work demonstrated with the TFET SABL makes it less susceptible to static power side-channel intrusions [47] and it can be used in the neuromorphic computing like Spiking Neural Networks (SNNs) based on TFET neurons are presented for pattern recognition applications, showcasing its great advantage on energy effectiveness [48]. Still, TFET can be explored to the strong hardware secure designs because of its peculiar characteristics like side-channel attacks counter measures [49], hardware primitives like physical unclonable methodologies [50], true random number generators [51], hardware obfuscations [52] and hardware Trojans [53], [54], [55].

Emerging hardware technologies like TFETs and spin-based devices offer improved hardware security over CMOS. TFETs resist side-channel attacks and reduce power consumption, though facing challenges in low ON-state current and complexity. Similarly, TFET-based current mode logic (CML) reduces power consumption and resists attacks like DPA, but encounters fabrication complexity and scalability issues. Spin-based devices provide non-volatile data integrity but are vulnerable to magnetic field manipulation. Future research aims to optimize TFET and spin-based device designs and develop encryption techniques to enhance system security in IoT and other applications.

B. HYBRID PHASE TRANSITION FET (HYPERFET)

The testability, dependability, and safeguarding of electronic systems are critical challenges for the protection of human life with the rapid growth of advanced computing technologies in all electronic domains. But for the past few decades, power has become a significant barrier for very large integrated circuits. The scaling of CMOS technologies in the past allowed for the payment of functionality increases in chips by lowering the supply voltage and lowering transistor capacitance. This opens it for the researchers to find new paradigms, new physics and new mechanisms to overcome the limitations of conventional CMOS this helps to evolve with a new emerging technology called HyperFET. The working functionality of this device starts with the novel operation i.e. the strong electron-electron interactions present, transition metal oxide materials can exhibit a variety of phases with vastly different electrical, magnetic, structural, and thermal properties. Electronic controls that allow for reversible control of these phase transitions may lead to whole new devices with capabilities beyond those of current semiconductor technology. At approximately 670 °, a metal-insulator transition (MIT) takes place in the transition metal oxide material VO_2. By connecting VO_2 to the source of traditional CMOS devices, hyperFET devices have recently been shown. These HyperFET showed a sharp switching slope that was below the ambient temperature Boltzmann switching limit of 60 mV/dec [57], [58], [59]. This new evolution of functionality opens the applications in domains like low-power digital applications [60], [61], [62], neuromorphic computing, coupled oscillators [63], hardware security applications [64] shown in Figure.3.

It is observed and demonstrated that CMOS technologies are found to have various disadvantages in terms of power density and energy resources because of technology scaling, given the impossibility of obtaining lower threshold voltages without causing significant leakage currents. So, an alternative emerging device has shown to overcome that limitations of the traditional transistor, called HyperFET. It contains the Phase Transition Material (PTM) connected to the source terminal of FET as shown in Figure. 4. The PTM will result in the sudden high impedance (insulator) - low impedance (metal) transitions to increase the I_{on} current and to reduce I_{off} current which helps to decrease the SS. In the insulating phase in the absence of electrical stimulation, PTMs often stabilize. The current flowing through the PTM grows linearly as a voltage (V_{gs}) is applied, as demonstrated by the I - V curve in Figure. 5.

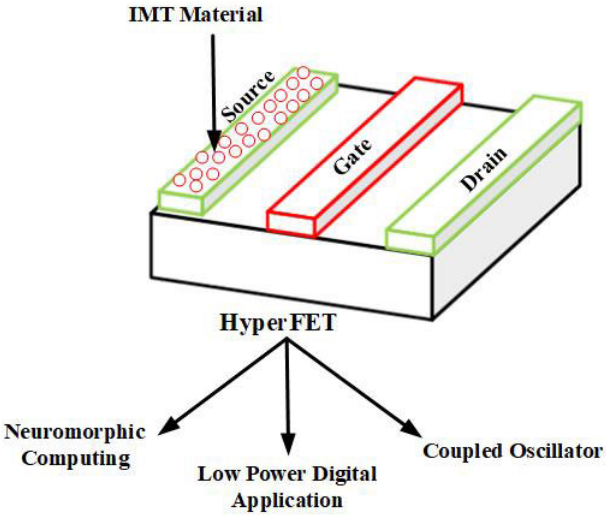

FIGURE 3. Cross-sectional view of HyperFET and its applications.

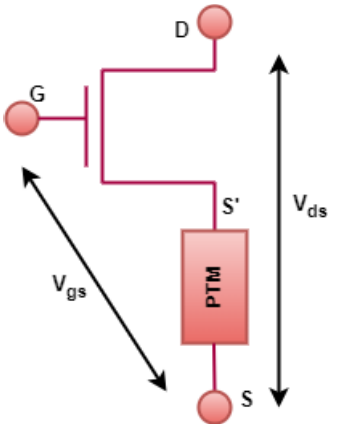

FIGURE 4. HyperFET [60], [61], [62], [63], [64], [65].

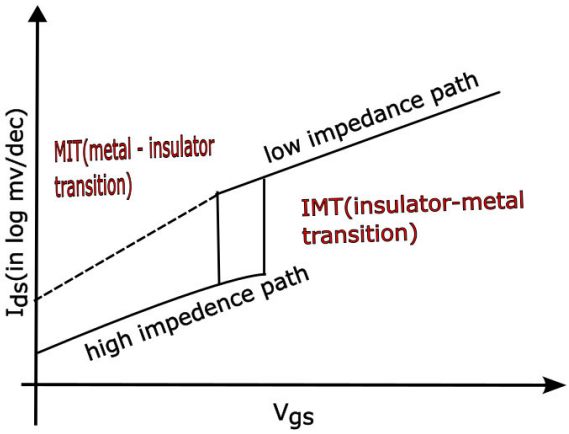

FIGURE 5. General I -V characteristics [60], [61], [62], [63], [64], [65].

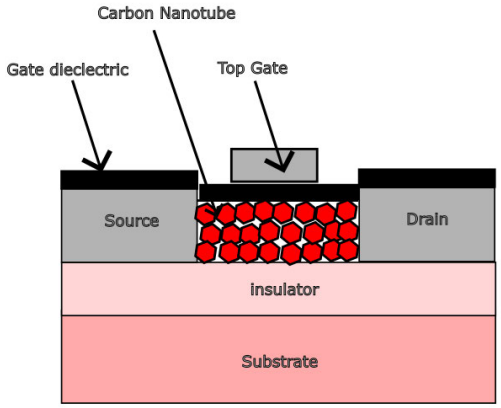

FIGURE 6. General I -V characteristics [60], [61], [62], [63], [64], [65].

HyperFET circuits reduce power consumption and enhance hardware security, but novel materials and design approaches may introduce vulnerabilities. Challenges persist in balancing performance and security for wearable and IoT applications. PTM modulated HyperFETs offer higher ON current and steep sub-threshold curves, requiring meticulous parameter optimization. Similarly, AlGaN/GaN phaseFETs with ALD VO_2 resistors provide ultralow leakage and steep sub-Boltzmann switching but face fabrication complexity and compatibility issues. Despite potential advantages, emerging devices like HyperFETs encounter limitations in maturity, cost, and compatibility.

C. CARBON NANOTUBE FET (CNTFET)

The area and power-delay-product (PDP) for CNTFETs have undergone significant improvements over MOS devices, which renders them enticing to MOS competitors. Carbon atoms compose the internal structure of hollow shapes and cylindrical nanotubes that are referred to as CNTs in a hexagonal lattice configuration. Conceptually, they resemble graphene sheets rolled into tubes, where graphene constitutes a monolayer of carbon atoms organized in a two-dimensional honeycomb pattern. CNTs exhibit varying diameters and lengths and are categorized mainly as Single-Walled Carbon Nanotubes (SWCNTs), featuring a solitary graphene layer, and Multi-Walled Carbon Nanotubes (MWCNTs), which comprise multiple layers of graphene tubes nested akin to Russian nesting dolls. Due to their distinctive structure, CNTs showcase remarkable mechanical, electrical, and thermal attributes, positioning them optimistically across a spectrum of applications encompassing electronics, materials science, and nanotechnology. The cross-sectional view of CNTFETs is shown in Figure. 6. Depending on how the carbon atoms organize themselves, CNTs are likely to be classed into two groups: metallic (m-CNTs) or semiconductor (s-CNTs). The non-zero band gap energy found in s-CNTs can be taken advantage for the production of CNTFETs, which are compatible with adding to silicon MOSFETs fabrication process. The CNT has been grown on a surface and plays out as a channel underneath the control via a gate. Although the CNT region between the source and drain electrodes is fervently doped, the CNT region underneath the gate is undoped. The features of these CNFETs are likely to be the same as CMOS functionality as well as the regular fabrication process. In CNTFET the mobility of charge carriers is the same which helps the voltage transfer characteristics be symmetrical. Apart from that, the diameter of the CNTs can be use for figuring out the threshold voltage of a CNTFET.

$$DCNT = (\frac{\sqrt{3}a_0}{\pi})(\sqrt{n^2 + m^2 + nm}) \quad (1)$$

A CNT's functionality may differentiate between metallic and semiconductors relying on its chirality (n, m). The diameter of CNT can be measured as shown in the above equation (1) where a_0 is the interatomic distance between two carbon atoms. The CNT becomes metallic when n-m = 3K (K ϵ Z) and n = m; otherwise, it seems a semiconductor and can be employed as the channel region of a Nanotube-based device [66]. By the variation in operational characteristics between a metallic source/drain and the CNT, multiple kinds of CNTFETs have since been evolved, all showcasing a high I_{ON}/I_{OFF} ratio [67], [68]. There is no guarantee that perfect alignment of the CNTs during the fabrication process is inevitable. Misaligned CNTs and metallic CNTs provide critical challenges for CNTFET circuits which gives improper functionality to designed circuits. And some other certain inherent variations like CNT-chirality, CNT-diameter, inter-CNT spacing, transistor width, gate pitch, gate-dielectric thickness, gate height, and dopant content [69], [70] These inherent variations in the CNFETs have been taken advantage to the design of hardware security models like TRNGs [72] and PUFs [71]. Since carbon nanotubes possess low off-current tendencies and can serve as the channel connecting both the source and the drain in CNTFETs, they harness less power. Further lessening consumption of power is due to the fact that no current flows across the source back to the drain which employs the design for low-power applications in contrast to the traditional CMOS [73]. This advantage of CNTFET is used in strengthening the side channel attacks [74].

Integrating the Lorenz chaotic system into CNT-PUF designs enhances security against machine learning attacks. However, PUFs based on CNTFETs face challenges such as manufacturing variability and susceptibility to side-channel attacks, requiring robust encryption and key management solutions. Despite offering higher speed and lower power consumption, CNTFET technology presents security risks due to process variations and manufacturing defects, necessitating tailored solutions for enhanced hardware security.

D. SPINTRONICS

Spintronics, short for "spin transport electronics," revolves around the manipulation of electron spin in electronic devices. It expands on traditional electronics by harnessing both electron charge and spin for various applications.

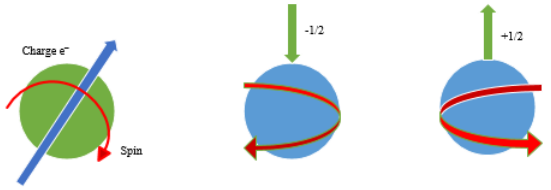

FIGURE 7. Basic orientation and notation of charge used in spintronics.

In spintronics, electron spin a quantum property analogous to intrinsic angular momentum is pivotal. In numerous manners, spintronics diverges in structure compared to CMOS technology to be put to use in a broad spectrum of applications. Firstly Spintronics utilizes spin-polarized currents where electrons possess preferred spin orientations. The spin orientation and its notation are represented in Figure. 7. This polarization can be controlled using magnetic fields. Secondly, materials with efficient spin transport properties are used, enabling the propagation of spin information over extended distances. Thirdly electron spin is manipulated through mechanisms like magnetic fields or spin-orbit interactions, allowing for control and switching between spin states. Fourthly spin-polarized electrons are injected into materials, with changes in spin orientation detected. This forms the basis of data writing and reading in devices. Finally, in the applications comprising ferromagnetic layers separated by an insulating barrier, MTJs serve as non-volatile memory in applications like MRAM, in the recent advancements in response to the von Neumann bottleneck challenge, an innovative approach has been explored replacing conventional computing architectures incorporating sophisticated sensing circuits and autonomous logic processing units by adopting a write-in-memory logic paradigm using memory cells. Nevertheless, this approach faces the drawback of heightened energy consumption for writing compared to the established reading energy consumption. To address this issue, a solution is proposed an ultra-low-power, high-speed In-Memory Computing (IMC) unit founded on field-accelerated spin-orbit torque (SOT) magnetic random access memory (MRAM), leveraging voltage-controlled magnetic anisotropy (VCMA). The study delves into the magnetization dynamics of the device by solving a tailored Landau-Lifshitz-Gilbert equation [83] through a physics-based compact model. This newly suggested MRAM architecture is put to the test for operations pertaining to Boolean logic and a non-volatile full-adder (NVFA), showing its potential to mitigate energy challenges while enabling advanced computing functionalities [75]. Spin FETs blend traditional transistor structures with spin effects, introducing novel logic and memory functions and these generate microwave signals via angular momentum transfer and find use in RF and microwave technologies, the work introduced was a concise electrical model for Spin-Torque Diodes (STDs) utilized as continuous-wave (CW) radio-frequency (RF) detectors. This model integrates the nonlinear resistance of the STD junction by assessing its current-voltage (I-V) behaviour, incorporates the input and output impedance of the STD, and factors in the bandwidth and the impact of spin-torque gain based on RF input power [76]. Leveraging spin for advanced logic gates and qubits, with implications for computing advancements [78]. Spintronics memristors blend the scalability of spin-transfer torque devices with the non-volatile features characteristic of memristors. This combination fulfils the demands of robust data processing that necessitate high-speed, low-power, & scalable quantum computation (QC) [77]. Spintronics offers advantages such as reduced energy consumption, faster data processing, and non-volatile memory. Its transformative potential spans memory devices, processors, sensors, and communication systems, by leveraging electron spin properties for innovation.

1) SPIN TRANSFER TORQUE MAGNETIC TUNNEL JUNCTION (STT-MJT)

STT-MTJ is a specific kind of spintronic technology of that falls under the umbrella of spintronics. It entails employing spin transfer torque for regulating the magnetic moments' orientation upon an MTJ. Two ferromagnetic layers have been separated from one another via an insulating tunnelling wall in an MTJ as shown in Figure.8. The tunnelling current, which is capable of being utilized for interpreting data in binary formats, gets impacted by the relative direction of the magnetic moments within these layers. The magnetic moments can be altered by applying a current with a certain spin polarization, permitting data both to be written and read in memory devices.

STT-MTJ can be understood as a specialized application of spintronics principles, with its primary emphasis on harnessing spin transfer torque to achieve specific functionalities, notably in the domains of memory and storage. Spintronics, however, encompasses a wider spectrum of ideas and mechanisms that go beyond STT-MTJ, encompassing various approaches to spin manipulation, spin-based logic, and more. An STT-MTJ consists of three key components: two magnetic layers divided by a slender insulating layer. These layers are typically made of ferromagnetic materials with distinct magnetic orientations. When an electric current flows through the MTJ structure, it consists of electrons with their individual spins. The spin polarization of these electrons refers to the predominant direction of their spins, either ''up'' or ''down. ''The insulating layer between the two magnetic layers is thin enough to allow a phenomenon called ''spin-dependent tunnelling'' to occur. Electrons with spins aligned parallel to the magnetic layers (e.g., ''up'' in both layers) have a higher probability of tunnelling through the insulating layer than electrons with anti-parallel spins (e.g., ''up'' in one layer and ''down'' in the other). When a current with spin-polarized electrons flows through the MTJ, it applies a torque to the magnetic moments of the two ferromagnetic layers. This torque can cause a change in the relative alignment of their magnetic orientations. The

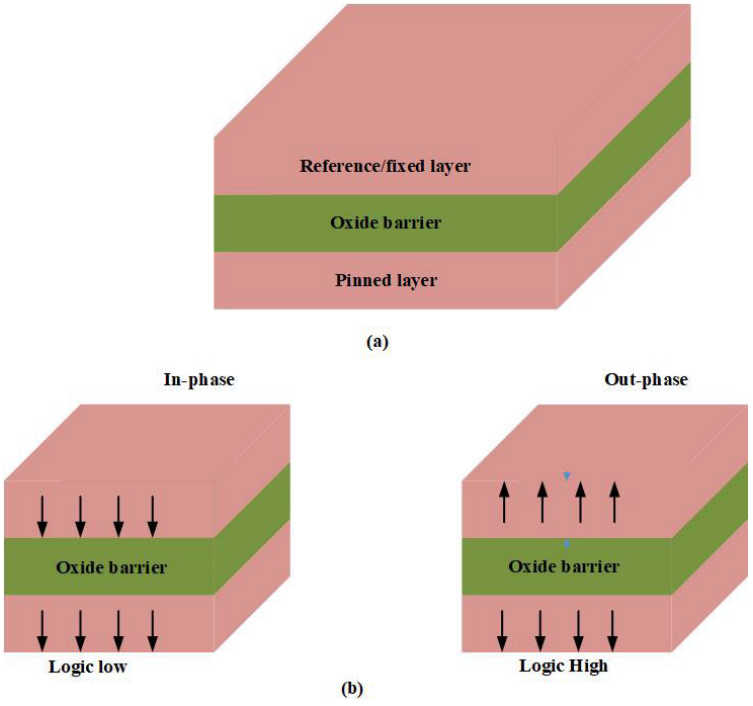

FIGURE 8. STT-MJT a) Device architecture b) Stochastic toggle action.

magnetic layers' relative orientation affects the tunnelling probability of electrons, which, in turn, influences the overall resistance of the MTJ. When the magnetic layers are parallel (low-resistance (R_P) state), it corresponds to one binary value (e.g., "0"). When they are anti-parallel (high-resistance (R_{AP}) state), it corresponds to the opposite binary value (e.g., "1") as shown in Figure.8. STT-MTJ devices can be used for both reading and writing data. To read data, a small current is passed through the device, and the resulting resistance can be measured to determine the stored binary value. To write data, a larger current is applied to change the magnetic state of the MTJ, effectively switching it between the low-resistance (RP) and high-resistance (RAP) states, representing "0" and "1," respectively [79]. STT-MTJ relies on the controlled manipulation of electron spins and their effect on the magnetic layers' relative alignment to store and retrieve binary information. The difference between the resistances is termed as tunnelling magnetic resistance (TMR) is noted as in equation (2)

$$TMR = \frac{R_{AP} - R_P}{R_P} * 100 \tag{2}$$

The read stability of MJT depends upon the TMR ratio as it's more higher the more stable and accurate in reading from MJT [79], [80]. By the inherent physical properties of Utilizing the spin transfer torque mechanism, the MTJ undergoes state transitions when subjected to a bidirectional current (I) surpassing the critical current level (I_{C_0}) [81] where the critical current is given by equation (3),(4).

$$I_{C_0} = 2\alpha \frac{\gamma e}{\mu_B g} E \tag{3}$$

$$E = \frac{\mu_0 M_s H_k V}{2} \tag{4}$$

where E is the Potential Energy Threshold, H_k is the Effective Anisotropy Strength, μ_0 is the Permeability of the Void, M_s is the Full Magnetization, χ is the Relaxation Rate in Magnetism, γ is the Gyromagnetic Momentum, e is the Quantum of Charge, μ_B is the Bohr magneton, V is the volume of the void, k_B is the Boltzmann constant, g is the spin polarization efficiency factor, T is temperature, τ is switching duration, τ_0 is standard time [81].

The probability function of stochastic switching behaviour is represented in terms of current (I), critical current(I_c), Δ is temperature factor and time (T) as equation (5):

$$p(1,t) = 1 - exp(\frac{-t}{\tau_0} exp[-\Delta(1 - \frac{I}{I_c})^2]) \tag{5}$$

The time it takes to transition between the two operational modes is expressed as shown below in equation (6):

$$\tau = \tau_0 exp(\frac{E}{K_B T}(1 - \frac{I}{I_{C_0}})) \qquad (I > I_{C_0}) \tag{6}$$

In STT-MTJ devices, it's because of important inherent variations to consider that can be leveraged for security enhancements. These variations can add an extra layer of protection against unauthorized access and tampering like random variability, write and read noise, bit errors, temperature sensitivity, process variability, magnetic field

sensitivity, write, read, retention variability etc can make them more resilient and resistant to a broad spectrum of attacks, including physical tampering, side-channel attacks, and unauthorized access attempts. In the paper a novel neuromorphic spin-based TRNG that relies on the stochastic characteristics exhibited by MTJs operating in the sub-critical current regime. In the proposed design, effectively mitigates the influence of process variations through the incorporation of a neuromorphic architecture and the integration of an embedded XNOR operation. Moreover, the TRNG proposal delivers impressive advantages, including high throughput, reduced energy consumption per random data bit, as well as decreased power dissipation and area overhead when juxtaposed with state-of-the-art spin-based TRNGs, all attributed to its streamlined and efficient structure [72]. 2T/3T MTJs serve as a vital component in logic locking when seamlessly integrated into the circuit. They play a pivotal role in generating a key combination that is indispensable for ensuring the correct operation of the circuit. As discussed in paper [19], logic locking is a strategic method that introduces novel key inputs and logic elements into the circuit, causing it to exhibit erroneous behaviour until the precise key combination is furnished. In the context of MTJ-based logic locking, these MTJ structures are instrumental in constructing this crucial key combination. These structures are meticulously engineered to be sensitive to specific key parameters, necessitating precise parameter configuration to enable the circuit to function correctly. This approach is versatile, finding utility in both combinational and sequential logic-locking scenarios. So this offers enhanced security coverage across a broader range of threats when contrasted with alternative obfuscation techniques like IC camouflaging and split manufacturing. To mitigate the risk of side-channel attacks, the authors in paper [47] suggest the adoption of SABL gates, which have demonstrated superior resistance to Differential Power Analysis (DPA) when compared to traditional CMOS gates. Additionally, the proposed TFET SABL gates further bolster DPA resilience by reducing data dependencies on device power consumption. Furthermore, the authors recommend combining logic encryption/locking with these TFET SABL gates to achieve heightened hardware security with exceptionally low energy consumption. Overall, the TFET SABL gates put forth in this proposal exhibit reduced energy consumption and increased DPA resilience, positioning them as a promising choice for secure and energy-efficient cryptographic systems. Within the domain of SOT-assisted MTJ technology, the MTJ resistance functions as a distinctive identifier. This resistance undergoes variation due to diverse process factors, including oxide layer thickness and TMR ratio, resulting in resistance discrepancies among individual devices. To authenticate a device, a designated challenge is applied, enabling the measurement of MTJ resistance and the derivation of a device-specific response. This distinct response operates as the device's unique signature, meticulously archived as a challenge-response pair within a database for authentication purposes. The response's uniqueness stems from the inherent, unpredictable process variations inherent to device manufacturing, rendering the replication or prediction of this response a challenging endeavour this feature stands as a crucial requirement for PUF's, establishing SOT-assisted MTJ as a strong candidate for PUF implementation [20].

The spin-orbit torque MRAM unit offers security advantages over CMOS but requires further research to address integration challenges and vulnerabilities. Spintronic devices like spin-torque diodes and memristors show promise but need improvements in parameter extraction accuracy and scalability. A compact model of magnetic tunnel junctions aims to enhance reliability and security by addressing fabrication errors and stochastic behaviour. Despite fabrication complexity, spintronic random number generators offer secure solutions with lower power consumption, emphasizing the importance of managing process-induced variations for reliable security features.

E. MEMRISTORS

Memristors, often referred to as ''memory resistors,'' belong to a class of two-terminal non-volatile memory devices known for their distinctive response to electrical current. Their primary function revolves around the capability to retain and modify a resistance state, achieved by applying voltage or current. This intrinsic feature empowers memristors to store data in the form of resistance levels. These versatile devices can function as both switches and digital memory elements, representing binary data (0's and 1's) through their high and low resistance states, making them ideal for digital memory tasks. Furthermore, memristors possess the ability to adapt their resistance in response to input signal frequency and timing, a critical attribute for applications in neuromorphic computing and machine learning. In accordance with the voltage that is given to an initial memristor device, it could be possible to choose whether to deploy analogue or digital functionality in a memristor component, which typically displays a progressive change in current proportionate to the amount of cumulative electrical input. The typical diagram of a memristor and its characteristics are shown in Figure.9. A diffusive memristor represents a distinct category of memristors by the authors from the paper [84], relying on the migration of metal ions to modify its resistance. This process yields stable yet volatile characteristics and intrinsically unpredictable behaviour. When exposed to voltage pulses of varying amplitudes, the memristor's current response exhibits a random distribution spanning different ranges. This built-in randomness is effectively harnessed to develop a bonafide random number generator (RNG), specifically intended for hardware security applications. The modulation of the reference voltage (V_{ref}) holds a central role in shaping the unpredictability of the TRNG's output bits. This control is exercised by governing the likelihood of observing ''0'' or ''1'' in the binary outputs. When V_{ref} experiences an increase, the probability

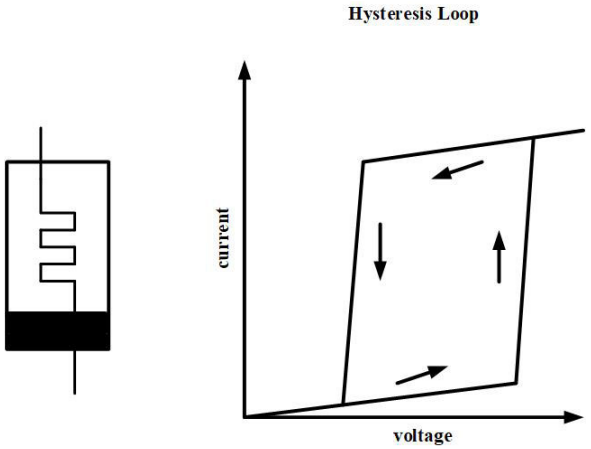

FIGURE 9. Memristor's device architecture and its hysteresis characteristics.

of obtaining ''1'' diminishes, while the odds of acquiring ''0'' rise. Precision in adjusting V_{ref} enables a refined regulation of output probabilities, converging them toward the 50% mark, thereby amplifying control over the TRNG's randomness. This adaptable V_{ref} setting can be fine-tuned to suit various practical applications, including applications in neural networks or random number generation. By maintaining output probabilities in proximity to 50%, the TRNG adeptly generates a stream of random numbers at a speed of 2 kilobits per second, consistently meeting the rigorous standards set by NIST verification tests. Consequently, the adjustment of V_{ref} stands as a critical determinant in the management of the TRNG's output bit randomness [84]. Memristive memories possess the ability to generate stochastic bit-streams directly within memory, thereby addressing a longstanding challenge in the cost-effective design of stochastic computing systems. This innovation eliminates the requirement for an extra analogue-to-digital conversion step when processing analogue inputs. As a result, memristive memories offer the potential to significantly reduce the cost of bit-stream generation while simultaneously bolstering the resilience of Stochastic Computing systems against soft errors [85]. The proposed memristor cell, utilizing a monolayer AlO_x film, demonstrates a unique capability of exhibiting both analogue and digital resistive switching behaviour. This cell can effectively replicate typical synapse functionalities, including Spike Time-Dependent Plasticity (STDP) and Long-term Potentiation/Depression (LTP/LTD) in various operational modes. In its digital component, featuring High and Low resistive states (HRS/LRS), the cell demonstrates variable levels of accuracy with different power consumption profiles. Specifically, it achieves approximately 82% and 94% accuracy in the Modified National Institute of Standards and Technology (MNIST) recognition task. These findings underscore the potential of the proposed memristor cell for the development of energy-efficient, practical, and mixed-precision neuromorphic computing systems, leveraging AlOx monolayer memristors as a foundational technology [86]. In addition to its role in memory technology, memristors find diverse applications in neuromorphic computing [89], hardware security(TRNGs [84] and PUFs [87], [88]), energy-efficient electronics [90], analogue computing, sensor technology [91], biomedical applications, quantum computing, cognitive computing, internet of things (IoT) and Materials Science.

The study recommends memristors for hardware security due to their density and power benefits but acknowledges vulnerability to modeling attacks. It suggests transient memristors as a solution, offering intrinsic randomness and advanced security features, with further research required. Additionally, a proposed TRNG using diffusive memristors improves security by leveraging physical stochasticity, needing validation for robustness. Memristor-based neuromorphic systems provide security advantages but require management of challenges like resistance drift and performance overheads.

F. SILICON NANOWIRE FET(SiNW-FET)

Silicon Nanowire Field-Effect Transistors (SiNW-FET) exhibit compelling features that render them appealing for a variety of applications in the realm of nanoelectronic and beyond. These transistors are characterized by their minuscule dimensions, operating at the nanoscale, which facilitates the integration of a multitude of transistors onto a single chip. This capacity fosters the creation of high-density, high-performance electronic circuits. At the core of a SiNW-FET lies an ultra-thin silicon wire, typically boasting a nanometre-scale diameter, often just a few nanometres. This silicon wire functions as the conduit for electrical current. Surrounding the nanowire is an insulating gate dielectric that serves a dual role, it isolates the nanowire from the gate terminal and regulates the flow of current along the wire. The SiNW is further outfitted with source and drain electrodes positioned at its extremities, facilitating the connection to external electrical circuits and enabling the seamless passage of current through the wire, as depicted in Figure.10. The operational principle of SiNW-FET hinges on the application of a gate voltage. When a voltage is provided to the gate terminal (referred to as the gate voltage), it generates an electric field within the gate dielectric. This electric field, depending on the specific type of SiNW (n-type or p-type), either attracts or repels charge carriers electrons or holes within the silicon nanowire channel. By manipulating the gate voltage, SiNW-FET can be toggled between two distinct states the ''on'' state and the ''off'' state. In the ''on'' state, the gate voltage permits the flow of current through the nanowire, effectively activating the transistor. Conversely, in the ''off'' state, the gate voltage obstructs current flow, deactivating the transistor. Owing to their nanoscale dimensions and minimized parasitic capacitance, SiNW-FET exhibits the capability to swiftly transition between on and off states, rendering them well-suited for high-speed electronic applications. Furthermore, SiNW-FET

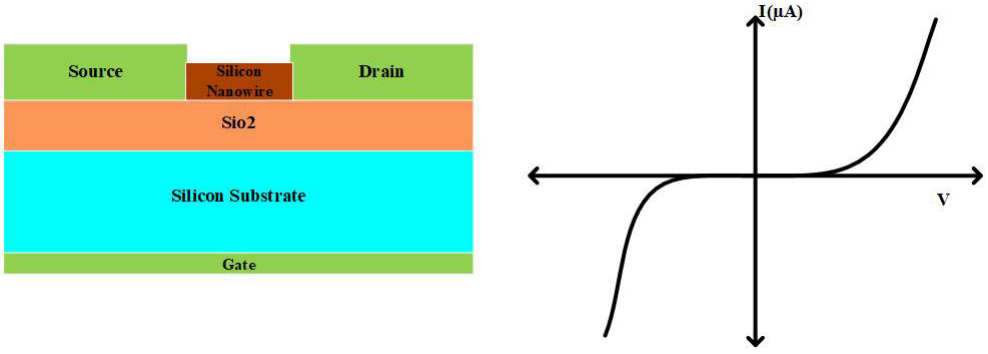

FIGURE 10. Silicon nanowire cross-section view and its general symmetric characteristics.

can serve as amplifiers of electrical signals. By applying a modest input voltage to the gate, these transistors can exert control over a substantially larger current between the sources and drain electrodes, effectively amplifying the input signal. Various types of configurations or structures have been studied in Silicon nanowire FET like double-gate, omegaa-gate, tri-gate and pi-gate and GAA structures, among all structures by virtue of the reality GAA offers better device control, that it boasts a slightly larger band of conduction energy than other gates and has the lowest leakage current of any gate [92]. SiNW-FETs can be harnessed to craft camouflaging gates and polymorphic gates, effectively concealing layouts and netlists, thereby bolstering intellectual property (IP) protection. Moreover, SiNW-FETs serve as a foundation for crafting current/voltage-based circuit protectors that effectively thwart fault injection attacks. These circuit protectors are adept at detecting and preventing the injection of malicious logic into a circuit. Lastly, SiNW FETs can be leveraged to design a lightweight SymFET-based XOR gate, ideal for implementing cryptographic functions that enhance circuit security. In summary, this article highlights that SiNW-FETs offer outstanding efficiency and security, making them a valuable choice for constructing secure hardware circuitry from various studies [93], [94], [95]. TIGFETs have emerged as a top choice for crafting high-security and high-performance cryptographic circuits among the various emerging transistor technologies. Furthermore, it's worth noting that TIGFETs uphold a similar level of security against Side-Channel Attacks (SCA) without any trade-off in power efficiency and additional spatial demands when contrasted with CMOS alternatives [96] and this logic is applied to the AES, the SM4 block cipher algorithm (SM4), and the lightweight cryptographic algorithm PRESENT have been implemented using TIGFET-based CML gates. These implementations have been subjected to a correlation power attack to assess the enhancement in resilience against SCA by Liu et al. [96]. Moreover SiNWFETs are used in wide applications like low power consumption [100], sensor applications [97], reconfigurable logic [98], high-frequency applications [99].

The study underscores security challenges with GAA Nanowire FETs versus CMOS, yet their improved performance offers security potential. Similarly, the dual-gate silicon nanowire FET enhances gate control and reduces parasitic capacitance, bolstering immunity against side-channel attacks. Reconfigurable circuits, like RFETs, offer security through logic locking but face vulnerabilities, stressing the need for robust measures. Silicon nanowire sensors excel in biomarker detection but grapple with integration challenges into CMOS

G. PHASE CHANGE MEMORY (PCM)

Phase Change Memory (PCM) is a non-volatile memory device that uses electrical resistance to alter the phase-change material's transit between its amorphous to crystalline phases to store data. Three essential elements typically make up a PCM cell called as phase change material, heater element and read/write electrode. This phase-changing material is sandwiched between two electrodes, which are frequently made of metals, in a PCM cell. The ''heater'' or just ''write'' electrode is one of these electrodes, and the ''read'' electrode is the other as depicted in fig.11. A particular chalcogenide glass substance, often made of components like germanium, antimony, and tellurium i.e. $Ge_xSb_yTe_z$, is at the core of PCM. This particular substance was picked because of its exceptional capacity to switch quickly and irreversibly between the amorphous form and the crystalline form. These materials have distinct electrical resistance values for each phase that can be used to interpret binary data as logic '0' and '1'. Three different operating modes for the PCM include writing (programming), reading, and erasing (rewriting). When writing the data into a PCM cell, a strong electrical current is run via the heater electrode, which quickly heats up the PCM. By converting the material from low resistance to high resistance during heating, a particular bit value is represented by a change in resistance. A smaller voltage is provided to retrieve the data from the electrode in a PCM cell to read information coming from it. It is possible to ascertain the stored data by measuring the PCM material's resistance. A reduced electrical current is provided

to the heater to erase data, which causes the phase-change material to transform back from high resistance phase to low resistance phase as seen in Figure.11. The Analogue In-memory Computation is a well-known use case for PCM technology, allowing for the efficient storage of a coefficient while also supplying the tools to perform matrix operations inside a memory block. When a voltage x_k is introduced across a PCM device with conductance configured to $w_{j,k}$ and outputs an electrical current $i_{j,k}$ is equal to $w_{j,k} \times x_k$. The conductance is regarded as constant and unaffected by the applied voltage in this presumption this methodology is a well-liked use of PCM technology and in the paper [101] to suggest a universal training strategy for neural networks with PCM-based layers. Within the neural network layers, PCM arrays have been used in numerous applications [102]. The PCM device has DC I-V characteristics of the S-curve type as depicted in Figure. 11 that make it suitable for digital applications using ternary logic, with this feature the implementation of the ternary multipliers and the ternary SRAM circuits, as well as performance comparisons with other current designs, are used to show the benefits of the proposed ternary gates in circuit applications [103]. PCM has been investigated for applications beyond storage-class memory, including its potential use in the Ternary Content Address Memory (TCAM), in the neuromorphic computation and also in the hardware security applications. Because of the inherent variability during both set and reset operations, applying the same programming pulse doesn't consistently yield the same programmed resistance in cells. This variability occurs both from cell to cell and between repeated cycles of the same cell operation [104]. Furthermore, when pulse parameters fall within the midpoint of those typically used for full set or reset operations, there's uncertainty in achieving the High-Resistance State (HRS) or Low-Resistance State (LRS) [105]. These unpredictable and variable programming characteristics can be harnessed to create PUFs. PUFs are hardware devices employed in applications related to cryptographic security, such as authentication and identification, and the generation of digital keys [105], [106], [107], [108], [109], [110].

PCM devices offer high throughput and CMOS compatibility for hardware security but face challenges like voltage-dependent conductances. The study suggests measurements-based device models and PCM synapses in neural networks. Memristive devices like PCM have potential in hardware security but require robust error correction. The Hybrid CMOS-PCM Ternary Logic design enhances security but needs further research on integration complexities. Despite PCM's potential for PUFs without tamper-sensing mechanisms, scalability concerns persist, requiring attention for more efficient security applications.

H. NEGATIVE CAPACITANCE FET (NCFET)

Over the past few decades, the relentless miniaturization of CMOS technology has played a pivotal role in reshaping the world of information processing. This trend, famously encapsulated in Moore's Law by Gordon Moore, predicts that the transistor density on integrated chips would double roughly every two years [111]. Consequently, the downsizing of device dimensions followed the Dennard scaling guidelines to create high-speed MOS integrated circuits [112]. However, as FETs continued to shrink in size, a challenge emerged: the power densities within chips began to rise, leading to increased power consumption in microelectronic circuits—a phenomenon often referred to as the "power dissipation catastrophe." To sustain a high overdrive voltage and ensure proper functionality, adjustments to both the voltage that is applied and the cut-in voltage became necessary as gate lengths scaled down. Consequently, the leakage current of transistors saw a significant increase. Unfortunately, scaling down the supply voltage in proportion was constrained by the inherent limitations of device operating principles, resulting in a bottleneck for the development of ultra-low power electronic devices. Lowering the supply voltage is recognized as a highly effective method for tackling this issue, chiefly because the power factor has a quadratic dependence upon supply voltage. In the scenario of conventional MOSFETs, the aggressive scaling of the supply voltage (V_{DD}) technique has encountered fundamental constraints, notably referred to as the 'Boltzmann Tyranny,' which limits reductions to around 60mV per decade. Hence, to address this limitation in conventional transistors, a range of devices has been created, including impact Ionization MOS transistors (IMOS) [113], [114], Tunnel FETs (TFET) [115], the Nano-Electro-Mechanical switches (NEM) [116], and the NCFET [117]. The first three devices modify electron transport to overcome the minimum threshold of 2.3KT/q (where k represents the Boltzmann constant, T stands for temperature, and q represents charge), thereby ensuring that the body factor(Vs) remains less than 1 as represented in the equation (7).

$$\begin{aligned} subthresholdswing &= \frac{\partial V_g}{\partial log_{10} I_d} \\ &= \frac{\partial V_g}{\partial V_s} \frac{\partial V_s}{\partial log_{10} I_d} \\ &= \frac{KT}{q} log10(1 + \frac{C_s}{C_{ox}}) \end{aligned} \tag{7}$$

The NCFET-based device incorporates a ferroelectric (FE) material within the gate stack of a standard FET as depicted in Figure.12. Consequently, the internal voltage of the baseline transistor gets amplified by the FE-layer because of the internal circuit model equivalent as seen in Figure.13, leading to a notable enhancement in the $\frac{I_{on}}{I_{off}}$ ratio and an improvement in the sub-threshold slope (SS) as shown in Figure.14. Through this (V_{DD}) scaling, NCFETs demonstrate the potential to overcome the limitations associated with the Boltzmann tyranny. Based on these characteristics, various configurations of NCFETs have been put forward. These include SOI-based NCFET [118], double-gate type NCFET [119], NC-SpinFETs [120], [121], two Dimensional based NCFET [122], [123],

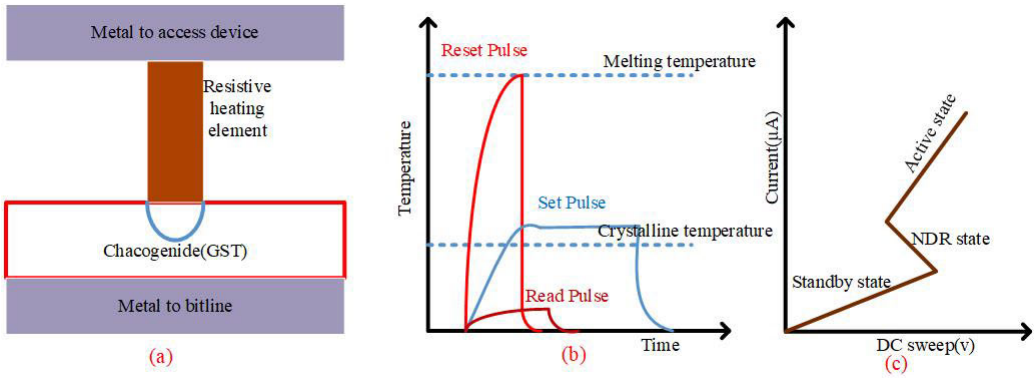

FIGURE 11. PCM a) Device internal architecture b) Demonstrational characteristics c) General DC V-I Characteristics of PCM [103].

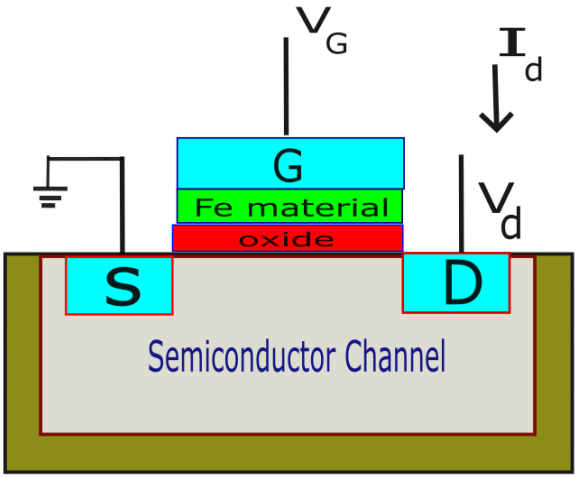

FIGURE 12. Device internal architecture.

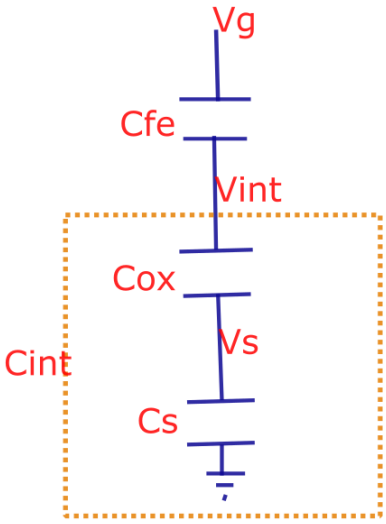

FIGURE 13. Equivalent capacitor model.

[124], [125], [126], [127], UTB type NCFET [128], anti-ferroelectric(AFE) based NCFET [129], [130], Carbon Nanotube(CNT) of NCFET [131], and nano-wire type of NCFET [132], among others. These structural variations

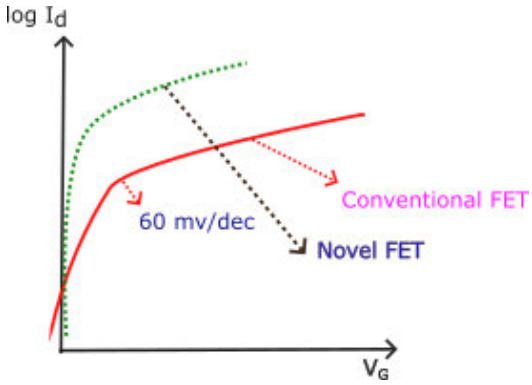

FIGURE 14. General I_d-V_{gs} on the y-axis, with logarithmic scale.

are founded on different types of ferroelectric materials, encompassing inorganic perovskite-type materials like lead zirconate titanate (PZT) [133], organic ferroelectrics such as poly (vinylidene difluoride-trifluoroethylene) and P (VDF-TrFE)) [134], as well as hafnium dioxide (HfO_2) doped with ferroelectric compounds [135]. The characteristics of the device are greatly improved when diverse architectures are given pocket doping [136]. In [137] several novel NCFET configurations, namely the Single Gate NCFET (SG-NCFET), Highly Doped Single Pocket Single Gate NCFET (HDSP-SG-NCFET), Double Gate NCFET (DG-NCFET), and Highly Doped Double Pocket Double Gate NCFET (HDDP-DG-NCFET). These configurations were developed through optimization of the ferroelectric material thickness and various key parameters. With the fine-tuned scaling parameters to attain specific performance goals, including achieving an OFF current among them, the design of HDDP-DGNCFET appears to be a more favourable solution for low-power applications. Upon examination, it becomes evident that in the comparative analysis between SG-NCFET and HDDP-DG-NCFET, the voltage and current power spectral density is shown to be superior in HDDP-DG-NCFET [138]. Manchester carry-chain dynamic adder of 4-bit are capable of achieving 10 times faster than normal NC-FINFET and 32-bit carry-look-ahead adder circuits utilizing NCFET technology have been devised, showcasing

a potential reduction of around 60% in switching energy when contrasted with equivalent FinFET designs operating at a V_{DD} of 0.7 V [139]. Novel non-volatile D-flipflop designs have been introduced, leveraging the hysteresis characteristics of NCFETs. These designs have the potential to deliver reduced area requirements, lower energy consumption, and minimized latency [140]. Likewise, memory designs based on NCFET technology enable straightforward erase, write and read operations while maintaining ultra-low power consumption. Furthermore, an NCFET-based compute-in-SRAM design has been introduced for machine learning applications, showcasing a remarkable 3-fold reduction in energy consumption and an 18-fold increase in speed compared to traditional designs [141]. Furthermore, an 8T SRAM based on NCFET ternary logic has been introduced, demonstrating non-destructive read capabilities and dependable write operations [142]. Furthermore, numerous researchers have delved into the attributes of NCFETs to enhance the performance of analog circuits and system designs [143], [144]. A design for an energy-efficient Computing-in-Memory (CiM) cell, incorporating an NCFET, has been suggested to bolster computing architectures tailored for Deep Neural Networks (DNNs). The SRAM CiM design, utilizing NCFET technology, accomplishes a reduction of approximately 2.59× and 1.62× in energy consumption at voltages 0.5V and 0.3V [145], [149]. NCFET devices exhibit improved characteristics for logic design in the of t_{fe} 3 nm-5 nm range, primarily owing to their steep subthreshold swing characteristics with this inverter, buffer, basic logic gates, few basic adders and 3.1× ring oscillator frequency faster than regular CMOS. Given the increased variations stemming from the ferroelectric layer, NCFETs exhibit promising potential and suitability for the development of hardware security primitives [146]. The NCFET PRESENT-80 cipher design undergoes evaluation against DPA attacks, and the findings reveal that the NCFET-based cipher design exhibits a significantly higher level of resilience when relative to the baseline CMOS design. It achieves an approximately fourfold increase in the attacker's effort ratio and maintains a low Signal-to-Noise Ratio (SNR) [147], some other side-channel attacks in CNN model [148].

NCFETs enhance hardware security by mitigating side-channel vulnerabilities, despite compatibility challenges. They offer higher ON current and resilience against DPA attacks, yet optimization is needed for IoT. The CNN model fusion scheme efficiently combats side-channel attacks, but ternary logic inverters pose challenges. Overall, NCFETs show promise, but further exploration and optimization are necessary.

V. COUNTER MEASURES IN HARDWARE SECURITY HARNESSING NEXT GENERATION CMOS TECHNOLOGY

System security has become a focal point in both research and industry over the past few decades. This heightened attention is partially attributable to the miniaturization of transistors, the fundamental building blocks of electronic circuits. This miniaturization enables the assembly of millions of transistors onto a compact chip. Consequently, the concept of a SoC has emerged, wherein numerous hardware modules are seamlessly integrated to create a comprehensive system within a remarkably small chip, often just a few centimetres in size. The realm of hardware security encompasses various research facets, including the creation of securely designed hardware circuits through secure processes, device authentication, cryptographic key generation within expansive networks, and the capability to actively monitor and detect potential attacks during runtime operations. Within the rapid proliferation in IoT sector, hardware vulnerabilities encompass a spectrum of concerns, including the alteration of IP designs, the introduction of malicious elements like Hardware Trojans (HT), and the inadvertent leakage of side-channel information, inadequate tampering security measures, and modifications to PCB designs, among other potential issues. While a variety of cryptographic algorithms serve vital functions in safeguarding secret keys, attackers persistently seek out hardware vulnerabilities as potential avenues to access sensitive information. In the realm of contemporary computing systems, the advent of open-source utilities, both in the commercial and FPGA CAD domains, alongside an array of cloud services, has ushered in fresh avenues for remote attacks devoid of any need for physical proximity to the target. These remote threats bear significant implications, especially within the context of critical IoT applications, with the potential to pose life-threatening risks. The categorization of hardware exploitations seen in Figure.15 and their corresponding countermeasures is presented in Figure.16 in a consolidated manner, providing clarity and ease of understanding.

A. HARDWARE SECURITY MODULES

1) TRUE RANDOM NUMBER GENERATOR (TRNG)

The effectiveness of cryptographic keys hinges on the quality of RNGs in generating a random number from the initial seed value. They can produce random numbers from seed values using a TRNG or a Pseudo_RN_Generator (PRNG). whereas PRNG are susceptible to predictability if the underlying algorithm or seed becomes known, as they rely on deterministic algorithms to generate numbers [150] and also generate a sequence of random numbers with a finite yet sufficiently extended cycle, originating from an initial seed value. Regrettably, in the context of the IoT, the available options for RNGs are rather limited. This is primarily due to the constraints posed by the IoT's resource-constrained devices, as well as the need to secure a vast amount of IoT data are playing an ever more crucial role across various domains, including cryptography, the field of artificial intelligence (AI), computational analysis finance, research simulation, and unpredictable computing. It could potentially create vulnerabilities that enable attacks to compromise encryption keys, intercept data, and ultimately

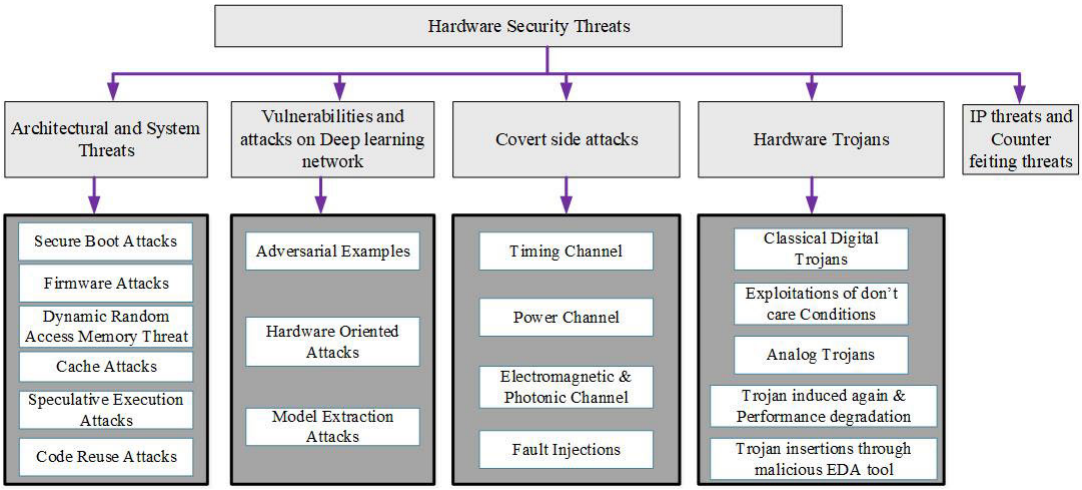

FIGURE 15. Classification of hardware security threats [13].

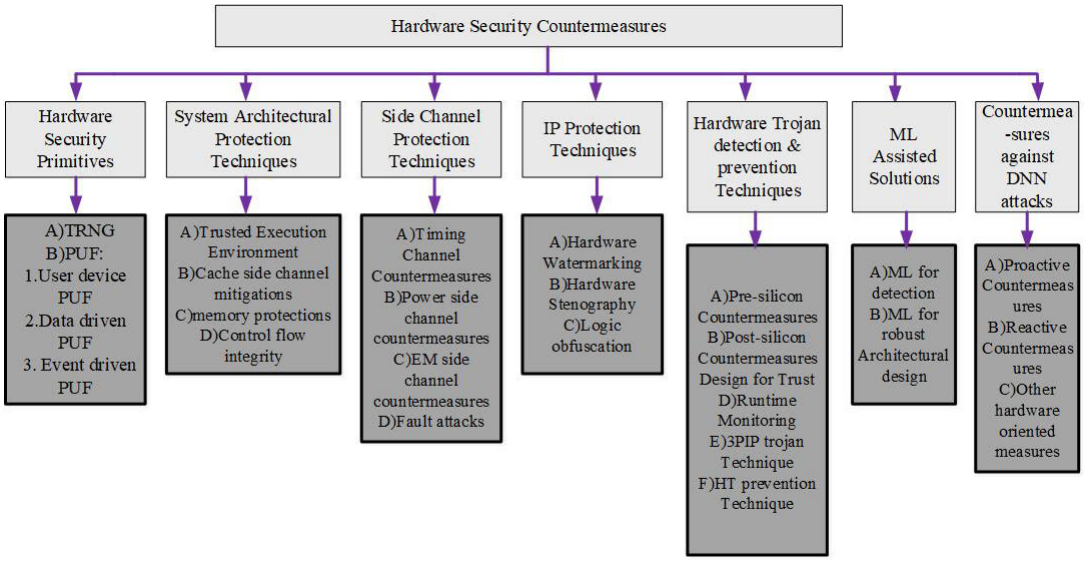

FIGURE 16. Classification of hardware security countermeasures [13].

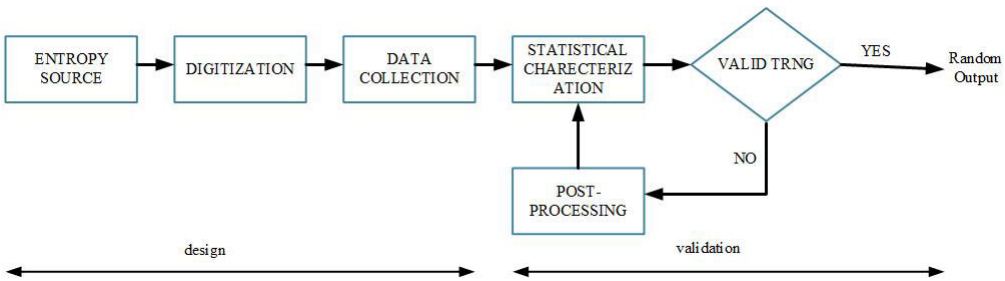

FIGURE 17. Flow chart of TRNG's development and verification procedure [152].

breach devices and communication channel [151]. It is indeed a need for algorithms that are inherently unpredictable and non-deterministic mathematical models to create random numbers from an initial seed state. So in the case of TRNG designs stemming from solid-state devices typically derive their randomness from non-deterministic physical processes, drawing from four distinct sources metastability, thermal noise, jitter and chaotic map. The general design flowchart of

TRNG is illustrated as seen in the Figure. 17. Chaos-based random number generators are ideal for creating TRNGs due to two key reasons. Firstly, the analog nature of chaotic circuits requires quantization of their states to produce random bits, making it impossible to reverse-engineer the internal state from quantized values. Secondly, like other analog circuits, chaotic circuits are impacted by noise, which not only initializes the system but also constantly alters internal states during operation. An ultra-low power TRNG employing a sub-range SAR analog-to-digital converter (ADC). The designed TRNG incorporates both a low-power adaptive-reset comparator and a dynamic amplifier. The shared coarse-ADC not only conserves space but also reduces energy consumption. It serves as both a discrete-time chaotic circuit and facilitates the selective activation of the fine-SAR ADC, leading to improved overall energy efficiency. Despite a 1/4 reduction in data rate after post-processing, the proposed TRNG achieved an impressive 29.3% power reduction. Furthermore, it attained a remarkable figure-of-merit (FOM) of 0.30 pJ/bit, setting a new state-of-the-art benchmark [153]. But in [154] has shown findings reveal that, following the completion of quantization by the SAR ADC, its residue, when quantized with a 1-bit quantization, behaves as a genuine random sequence. This architecture doesn't impose any limitations on the typical SAR operation and effectively serves as both an ADC and a TRNG in the previous work presented [153] has a consumption of 0.38 pJ/bit, which is 73% higher than in [154]. Furthermore, it relies on post-processing to attain high entropy, in contrast to designed technique, which achieves this without the need for post-processing. In the recent works a Latch type of TRNGs are well-suited for broad applications because of their less power consumption and compact size which can operate without the need for calibration or a feedback control unit, effectively improving the noise Vs mismatch ratio [155]. The proposed work in [156] TRNG derives its entropy from the jitter noise generated by two free-running current-starved ring oscillators. These oscillators are energy-efficient and provide a high throughput. The digitization principle used in this study for bitline discharge rate is entirely digital and depends solely on periphery enhancement. It approaches enable to complete reutilization of commercial bit cells and automated design through memory compilers. Extensive use of the existing SRAM array infrastructure allows for the integration of the entire key generation subsystem with only a 12.7% increase in area compared to a baseline SRAM [157]. The study, introduced a unified NVRAM-TRNG that employs high-voltage transistors to withstand the voltage requirements during the program and erase operations in NVRAM mode [158]. To capture jitter noise utilizes a single ring oscillator (RO) divided into two interconnected stages. The RO is regulated by a native NMOS transistor to mitigate the impact of supply voltage fluctuations [159]. A single approach is employed to create both PUF and TRNG using a shared entropy source, utilizing analogue-grade embedded flash memory for reduced power and secure design [160].

Despite the fact that researchers have worked hard to produce power-efficient TRNGs utilizing conventional MOSFET, the IOT industry presents several hurdles and some of security issues some of which are summarized below:

- Robustness to process and environmental fluctuations and a high producing rate are two of the TRNG's key characteristics. In contrast, which may lead the adversary to interfere with the TRNG's operation and lessen its unpredictability, an attacker could alter external variables (such as the temperature and electromagnetic field, for example).
- Due to the fact that CMOS transistors are not probabilistic switching devices, randomization is produced artificially utilizing noise signals like thermal noises. Contrarily, newly developed TRNGs take advantage of probabilistic switching behaviours that are naturally produced from devices.
- To combat randomness and for security reasons, more circuitry is needed, which inevitably results in high circuit overheads and an increase in power consumption.

Due to the limits of conventional MOSFET research has continued to put time and effort into creating new TRNGs based on various beyond post silicon technologies. The use of RRAM primarily brings a new source of entropy to conventional CMOS TRNGs, harnessing its Non-Volatile Memory (NVM) attributes to increase chip-to-chip distinctions and enhance overall security. The 3-D RRAM in [161] cell showcases a distinctive method of changing resistance the findings demonstrate that the TRNG achieves a peak throughput of 1Gbps with less energy consumption. In another work proposed for high speed and low power, the main source of entropy is present when RRAMs are in their OFF states and are using the C2C variability to generate multiple random bits [162]. The advancements in semiconductor technologies offer fresh opportunities for TRNG designs, aiming to achieve reduced power consumption and compact footprints. Unlike transistors, a technology known as STT-MTJ possesses an inherent property where the transition between its two magnetic states is inherently stochastic due to thermal fluctuations. This characteristic makes it an ideal entropy source. A high-speed TRNG circuit utilizing STT-MTJ technology has been developed. The proposed TRNG incorporates feedback control mechanisms that leverage cell-level parallelism, allowing it to deliver increased random bit throughput as required by specific target applications [163]. In an asynchronous TRNG design, a capacitor discharges simultaneously through multiple STT-MTJ devices. Once the capacitor's discharge reaches a critical level, the final state of the STT-MTJ devices is employed to extract the generated random number, bolstering its resistance to process variations [164].

GAA CNTFETs, which feature a high-k insulator and a metal gate surrounding the channel, offer excellent gate

TABLE 3. Comparison of various emerging technologies TRNG's with their energy consumption,throughput and area.

Ref	Device Technology	Energy Consumption(pJ/bit)	Throughput(Mb/s)	Area(μm^2)
155	130nm CMOS	0.186	2.39	5561
159	40nm CMOS	2.5	53	4335
153	180nm CMOS	0.3	0.027	4.5
161	RRAM	0.144	1000	–
156	65nm CMOS	5	52	366
164	STT-MJT	7.3	120.6	404.8
168	65nm CMOS/MJT	0.66	333	48.95
172	CMOS/RRAM	–	10	1.4
162	RRAM	1.3	25	43
8	CNTFET/STT-MJT	0.75	51	202
157	28nm CMOS	15.13	4.5	12.54
154	65nm cmos	0.22	1.25	90
165	40nm CMOS	2.5	128	–
160	55nm Eflash CMOS	0.58	192.3	–
166	14nm CMOS	0.46	560	2114
167	65nm CMOS	6.08	86	10
171	RRAM	0.0228	6	–
169	28nm STT-MJT	0.64	177.8	7.64
170	TFET	5.4	10	90
163	STT-MJT	2.65	303	24.69
72	STT-MJT	1.1	50	219

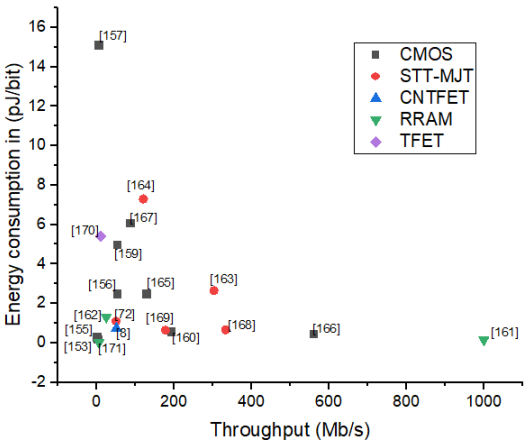

FIGURE 18. Examine of various TRNGs using latest technologies throughput vs energy consumption.

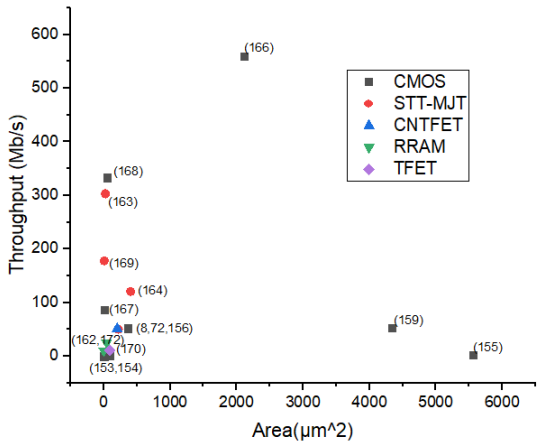

FIGURE 19. Examine of various TRNGs using latest technologies area vs throughput.

control. In the context of a hybrid CNTFET/MTJ logic and a novel TRNG design without the need for additional subsequent post-processing units, which leverages the non-deterministic behaviour of MTJs in the sub-critical current regime, the use of GAA-CNTFETs is proposed. This innovative design's efficient structure results in both low-power and high-performance operation [8]. Now researchers in looking at different TRNG designs employing post-silicon and CMOS technologies and examining how well they performed in terms of area, throughput, and energy consumption. While the CMOS-based [157] design is inefficient, the improved design with less consumption and a faster bitrate is shown in Figure.18 of the work in the reference [168]. Figure.18 and Figure.19 has been drawn from the values based on Table 3.

In Figure.18, the comparative analysis of throughput and energy consumption across emerging TRNG designs utilizing CMOS-based technologies reveals significant findings. Notably, STT-MTJ and RRAM-based TRNGs exhibit superior performance characterized by lower energy

consumption and higher throughput. Conversely, TRNG designs based on conventional CMOS technology demonstrate compromised performance when juxtaposed with these emerging alternatives.

In Figure. 19, the examination of bitrate and chip area reveals that spintronics technology delivers enhanced throughput within a reduced chip footprint. Conversely, CMOS TRNG design entails a larger chip area and demonstrates comparatively inferior throughput performance compared to STT-MTJ implementations.

The proposed TRNGs offer enhanced hardware security compared to traditional CMOS-based methods, addressing vulnerabilities to side-channel attacks and leveraging unique physical properties for cryptographic applications. Challenges such as finite precision in sawtooth maps and environmental influences on ring oscillator behavior necessitate future research to enhance robustness and mitigate vulnerabilities. These TRNG solutions aim to optimize energy efficiency, reliability, and randomness for secure IoT and cryptographic systems, offering promising alternatives to CMOS-based approaches.

B. PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

Physical Unclonable Functions, or PUFs, are being suggested as a low-cost substitute for huge e-fuses, non-volatile memory, or other specialized processing processes to permanently keep secret keys or offer device authentication and use integrated circuit manufacturing variances to create hardware-based cryptographic keys or unique identifiers. Secure communications, device authentication, and other security applications frequently use these special keys. It has been included in several security protocols and systems to improve authentication and security in RFID systems, Internet of Things devices, semiconductor devices' secure key creation and storing and more. PUF requires three things to be valid: uniqueness, unpredictability, and reliability. The data map's distribution and percentage are tracked by randomness, its uniqueness validates the encryption device's irreplaceable nature and its dependability demands that it repeats the same pattern in various settings.

The uniqueness metric for a PUF by considering the average Hamming distance between pairs of responses from different CRPs, normalized by the number of CRPs and the length of the responses. It provides a quantitative measure of the PUF's uniqueness, indicating how effectively it can generate distinct responses under different challenges. A key metric for assessing PUF responses' dissimilarity across instances is the Inter-Hamming Distance (HD_{inter}). High uniqueness, as measured by (HD_{inter}), is crucial for PUF security. The ideal value for (HD_{inter}) is 50% and its corresponding mathematical expression is shown in equation (8).

$$uniqueness = \frac{2}{k(k-1)} \sum_{k=0}^{k-1} \sum_{j=j+1}^{k} \frac{HD(R_i R_j)}{N} * 10 \quad (8)$$

'k' is the total number of challenge-response pairs (CRPs),'N' Length of the PUF response, measured in bits and HD(R_i, R_j) denotes the Hamming distance between two PUF responses, R_i, R_j from different CRPs.

PUF reliability refers to its ability to maintain consistent responses despite environmental changes. To gauge this, Intra Hamming Distance (HD_{intra}) is used, with an ideal reliability value of 100% and its value is shown in equation(9).

$$reliability = \frac{1}{s} \sum_{t=1}^{s} \frac{HD(R_i, R_{i,t})}{N} * 100 \quad (9)$$

Uniformity is a measure of a PUF's unpredictability, ensuring that responses remain unpredictable for any given challenge, even with prior circuit knowledge. The ideal uniformity value is 50%, reflecting an equal proportion of '1' and '0' in the responses, it's represented as in equation (10).

$$uniformity = \frac{1}{n} \sum_{j=1}^{n} R_{j,1} * 100 \quad (10)$$

The wide classification of PUFs design by varying sources of entropy, circuit topologies, and architectural designs has been figured as shown Figure. 20. Acoustic PUFs and optical PUFs are some examples of non-electronic PUFs that can be grouped according to the kind of material. For optical PUFs, the laser's position functions as a challenge-response pair (CRP) [173]. An Acoustical signal or stimuli, like a sound wave or sonic pulse, is usually emitted by an acoustic PUF device. The internal parts of the device are in communication with this signal a unique approach to device identification that uses acoustic signals as a challenge-response framework to fingerprint MEMS sensors [174].

The intrinsic PUF is a circuit for generating random numbers that depends on the difference in operation characteristics caused by process fluctuations. According to their respective operating principles, it is primarily classified as either delay-based or memory-based. The PUF's efficacy depends on how many CRPs it can produce with a single device. Strong PUFs can accommodate a significant quantity of CRPs, to the extent that reading all CRPs within a reasonable timeframe becomes impractical. Weak PUFs are characterized by their limited capacity for CRPs, often accommodating only a small number or none at all. Strong PUFs encompass arbiter and ring oscillator-based PUFs. Variations in manufacturing lead to timing differences between two paths in an IC, but in designing topologically and functionally identical with this arbiter PUFs (A-PUF) utilize to generate a one-bit output response. A-PUF is extensively studied due to its efficiency, requiring fewer hardware resources than RO-PUF and providing a larger challenge-response space than memory-based PUFs such as multiplexer-Based Arbiter PUF [175], Arbiter PUF (A-PUF) [176], Exclusive-OR (XOR) PUF [177], and Lightweight Secure PUF (LSPUF) [178], feed forward PUF(FFPUF) [181] irrespective of wide variety of arbiter PUFs used in different applications with different topologies. The A-PUF

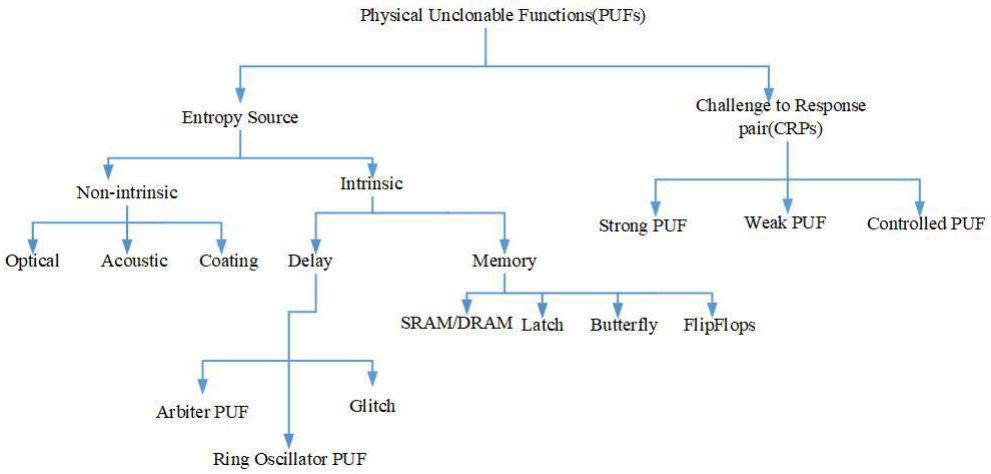

FIGURE 20. Wide variety classification of PUFs design.

circuit is susceptible to incremental delay software modelling risks [179]. A-PUF faces challenges in uniqueness and dependability due to physical layout constraints, particularly on FPGAs. To address these issues and other limitations described in [180], FFAPUF is introduced with a compact design, high uniqueness, and reliability, suitable for FPGA implementation. A-PUF on FPGAs faces issues with vulnerability to machine learning (ML) attacks and diminished uniqueness. An adversary can emulate the PUF by constructing a mathematical model with a few CRPs. Various ML modelling attacks, such as covariance matrix adaptation evolution strategies (CMA-ES), logistic regression (LR), Support Vector Machine (SVM), and Artificial Neural Network (ANN) [183] and some other attack models were employed in investigations to identify the issues towards robustness. This ML attack's advantage stems from employing a divide-and-conquer strategy [182]. LR is a potent attack on XOR APUF due to its gradient-based optimization and utilization of the mathematical model. DNN, being a formidable black box attack, is intriguing for study as it doesn't rely on a PUF's mathematical model. CMA-ES, on the other hand, is a gradient-free algorithm, setting it apart from gradient-dependent methods like LR [186]. The following Table 4 lists the APUF designs according to area, uniformity (UF), originality/uniqueness (UQ), and reliability (RE). Accuracy results of attack models for the different topologies of A-PUF designs and comparisons with prior FPGA-based A-PUF variants were examined as lists in Table 5.

Current PUF designs use CMOS-based technology's intrinsic noise and manufacturing variances as entropy sources. For security applications, CMOS technology is constrained by its low entropy and randomness. Spintronics, RRAM, CNTFET an emerging tech, pledges increased integration densities, lower power use, quicker data processing and more resilience to ML assaults. Novel sources of randomness and noise in emerging nanoelectronic devices facilitate the creation of highly efficient and robust PUFs [201]. Putting forth a novel Strong PUF (MPUF) based on Parallel MRAM that takes advantage of process-induced randomization in MRAM cells. Strong non-linearity is introduced by the use of an Array Selection Circuitry (ASC), which greatly increases secrecy potential (with maximum retrieved secure bits) and improves defence against ML assaults [192]. Multiplexers are positioned strategically in the symmetric routes of the APUF within the column region of the memory subarray to achieve minimally invasive access from a 1T-1R RRAM APUF memory subarray [193]. Usually, the embedded ring oscillators (ROs) generate responses based on comparisons of measured frequencies. The best design approach would be to develop an RO-PUF that has a high response bit generation capacity. This modification might strengthen RO-PUFs while expanding the size of CRPs, strengthening their security features even more. Expanding the CRPs in traditional RO-PUF increases hardware requirements due to a linear relationship. To mitigate hardware consumption, researchers often use a configurable RO-PUF to enlarge response bits without a significant rise in hardware resources. At first, every step of every RO had a MUX, resulting in a programmable RO, subsequently an improved CRO-PUF design, MUX-based CRO-PUF have been put forth to expand the size of CRPs that are generated [202], hybrid logic gate CRO-PUF [204]. Utilizing strengths and weaknesses from prior works for secret-key-based applications in security, the RACRO-PUF architecture shows promise as it exhibits robustness against four ML methods and offers significant improvements in CRP size, hardware utilization, and performance metrics [203]. Regarding circuit density and the per-CRP bit, the hn-CRO PUF is more economical than conventional CRO PUF designs. The suggested hn-CRO PUF is validated by Monte Carlo simulation findings achieved using UMC 65 nm

TABLE 4. Compare hardware resource usage and metrics for various PUF designs.

Ref	Design	Uniqueness(UQ)	Uniformity(UN)	Reliability(RE)	Hardware consumption(slices)	Target FPGA device
[187]	A-PUF	46.21	51.84	99.55	87	Xilinx Artix-7
	XOR A-PUF	48.69	50.73	99.41	279	
[180]	XOR A-PUF	49.88	48.74	99.2	–	ZYBO kit
[184]	Improved PUF	19.46	–	97.03	128	28 *nm* Artix7
[184]	FF-PUF	41.53	–	93.9	128	28 *nm* Artix7
[185]	Rec-DAPUF	47.6	49.75	96.51	–	Xilinx Artix-7
[185]	Rec-CMAPUF	50.3	49.5	95	–	Xilinx Artix-7
[187]	BST A-PUF	49.1	50.3	$< 10^{-9}$	150LUTs,47FFs	Xilinx Artix-7
[188]	P-SPUF	50.58	–	93.3	12×32 slices	Xilinx Artix-7
[190]	XOR-PUF	49.47	–	98.94	64	Xilinx Artix-7
[190]	XOR-PUF	49.03	–	97.54	64	Spartan-6
[191]	DD-PUF	49.48	–	98.33	64	Xilinx Artix-7
[191]	DD-PUF	49.28	–	98.37	64	Spartan-6
[192]	STT-MRAM	49.76	–	0.447	–	–
[193]	RRAM-PUF	51.4	–	0.135	–	–
[194]	APUF(64bit)	51.04	50.19	–	–	–
	5-XOR APUF(64bit)	50	49.98			
	LSPUF (m = 4; x = 4; k = 5)(64bit)	50.62	51.01			
	MPUF (k = 3)(64bit)	51.93	54.2			
	cMPUF (k = 3)(64bit)	57.47	50.92			
	rMPUF (k = 3)(64bit)	50.05	46.28			
	(4,4)-IPUF(64bit)	50.5	50			
	APUF(128bit)	50.34	50.35			
	5-XOR APUF(128bit)	50.03	50.32			
	LSPUF (m = 4; x = 4; k = 5)(128bit)	49.97	49.14			
	MPUF (k = 3)(128bit)	52.61	52.61			
	cMPUF (k = 3)(128bit)	57.47	50.92			
	rMPUF (k = 3)(128bit)	50.4	47.11			
	(4,4)-IPUF(128bit)	50.11	49.98			
[199]	7-XOR A-PUF(64bit)	53.21	49.23	–	–	–
	7-XOR A-PUF(128bit)	52.75	49.51			
[200]	MVL APUF(ternary-CNTFET)	32.75	–	–	–	–
	MVL APUF(quaternary CNTFET)	24.47				

technology with a compact RRAM model [205]. A suggested modular modulus technique aims to enhance the resilience of machine learning attacks while addressing the constraints of scalability and controllability [206]. Because they feature a restricted quantity of CRPs, memory-based PUFs are categorized as weak PUFs. Many SRAM-PUF, PICO-PUF [207], and DRAM-PUF designs were used to create these memory-based PUFs use the mismatch between the flip-flops or transistors to get a 1-bit response. A number of current approaches, including bit masking, Oxide Breakdown (BD), Temporal Majority Voting (TMV), Bias Temperature Instability (BTI), Error Correction Coding (ECC) and others, are implemented in the current PUF designs To increase reliability, it raises the area overheads [209] and, as a result of the device's propagation delay and drain from the source current contraction, eventually reduces SRAM cell performance still CRPs is a limitation. Therefore, a 2D sequence-dependent SRAM PUF is designed [208] that increases the CRPs is designed. Large amounts of power are consumed by traditional CMOS PUFs, A PUF design for all-spin circuits based on STT-mCell technology a linear feedback shift register (LFSR) with K stages is used [210]. A unique PUF design and generation scheme that uses resistive random access memory (RRAM) cells' inherent program-time variation as an entropy source as CMOS is vulnerable to secure communication [211]. As conventional CMOS is also suffering from scaling constraints a high level of reliability was attained by an RRAM PUF based on two transistors two RRAM (2T2R) cells [212].

PUFs exploit inherent physical variations in integrated circuits for cost-effective and energy-efficient hardware security, eliminating secret key storage. While configurable Ring Oscillator PUFs offer efficiency, they require robust error correction due to vulnerability to environmental variations. PUFs address hardware security concerns but may be susceptible to modeling attacks, necessitating additional safeguards. Integration of resistive memory-based PUFs enhances reliability and security but challenges such as endurance and data retention need further investigation. All-Spin PUFs leverage manufacturing variations for security but face compatibility issues and scalability limitations. Other proposed architectures like XOR-PUFs and RRAM/CMOS hybrids offer enhanced security but may suffer reliability and process variation issues. Despite vulnerabilities to machine learning attacks, efforts continue to balance performance and security in PUF design, including CNTFET-based multi-valued logic arbiter PUFs.

C. SIDE CHANNEL PROTECTION COUNTERMEASURES

1) TIMING SIDE CHANNEL ATTACK COUNTERMEASURES

Timing channel attacks refer to a class of security threats where an adversary exploits variations in the timing of system operations to gain unauthorized access to sensitive information. These attacks take advantage of the fact that the time it takes for a system to perform certain operations can reveal details about its internal state or the data being processed. By carefully observing and analyzing these timing differences, attackers may infer valuable information, such

TABLE 5. Accuracy results of attack models for the different topologies of A-PUF designs.

Ref	Design	Target FPGA device	learning model	CRP source	Challenge size	Prediction rate	Training CRP used
[183]	A-PUF	Xilinx Artix-7	LR	FPGA	64	66.50 %	40, 000
			CMA-ES			69.60 %	
			SVM			74.70 %	
			ANN			77.10 %	
	XOR-A-PUF		LR			58.20 %	
			CMA-ES			59.80 %	
			SVM			61.5 %	
			ANN			64.9 %	
[184]	Improved- PUF	28 *nm* Artix-7	LR	FPGA	64	99 %	10, 000
					256	99 %	
	Improved-PUF-based-MPUF		CMA-ES		32	100 %	
			CMA-ES		32	78 %	
	FF-PUF		LR		64	98 %	
					256	96 %	
	FF-PUF		CMA-ES		32	89 %	
	FF-PUF based MPUF		CMA-ES		32	50 %	
[185]	Rec-CMAPUF	Xilinx Artix-7	LR	FPGA	64 × 8	62 %	1, 38, 000
			SVM			62 %	
	Rec-DAPUF		LR		64	57 %	40, 000
			SVM			57 %	
[186]	IPUF	Xilinx Artix-7	CMA-ES	FPGA	64	75 %	90, 000
						50 %	
	4-XOR-A-PUF		LR			98 %	12, 000
			DNN			55 %	
			CMA-ES			50 %	
			LR			99 %	30, 000
			DNN			94 %	
	A-PUF		CMA-ES			98.44 %	50, 000
[189]	(Trit) quadruple-A-PUF	Xilinx-Artix-7	CMA-ES	FPGA	128	56 %	quadruple CRPs
			SVM			50 %	
[192]	STT-MJT-based- PUF	-	MLP	–	64	53.8 %	5000
			SVM				
			LR				
[194]	LSPUF (5-XOR)	–	DNN	–	128	96.22 %	12, 00, 000
	(4,4)-IPUF				128	97.68 %	6, 47, 000
	rMPUF (k = 5)				128	95.45 %	4, 00, 000
	5-XOR-APUF				128	97.87 %	6, 55, 000
	LSPUF-(6-XOR)				64	97.42 %	8, 00, 000
	6-XOR-APUF				64	97.68 %	6, 80, 000
	(4,4)-IPUF				64	97.44 %	3, 20, 000
[195]	8-XOR PUF	FPGA	MLP	FPGA	64	50.53 %	6000
						50.36 %	12, 000
						50.40 %	24, 000
[196]	AA- PUF	Spartan-6	LR	FPGA	64	56.60 %	10, 00, 000
			CMA-ES			78.65 %	10, 00, 000
[197]	original-A-PUF	Artix - 7	LR	FPGA	128	94.80 %	10, 000
	RSO-PUF					52.56 %	1, 00, 000
	RSO-MPUF					53.61 %	1, 00, 000
[198]	8-XOR- PUF	PyTorch package	FC-LSTM(GPU)	Python 3.7	64	99.00 %	20, 00, 000
			FC-LSTM(CPU)			99.00 %	20, 00, 000
	I-PUF		FC-LSTM(CPU)			97.00 %	6, 00, 000
[199]	7-XOR-PUF	MatLab	ECP-TRN	MatLab	64	97.78 %	5, 60, 000
			ECP-TRN		128	96.65 %	28, 00, 000
	XOR– LSPUF		ECP – TRN		64	96.73 %	4, 80, 000

as cryptographic keys or other sensitive data, compromising the security of a system. Timing channel attacks are a type of side-channel attack, focusing on the timing behaviour rather than directly attacking the cryptographic algorithms themselves. Mitigating timing channel attacks involves implementing various countermeasures to reduce or eliminate the potential information leakage through timing variations like constant-time implementations [214], noise injection, timer jitter, hardware isolation, code and compiler techniques [213].

An attack configuration based on information theory that reduces undesired noise generated by Network-On-Chip(NoC) using differential signalling techniques as well as repetition coding route to effectively carry out a realistic covert communication assault in an analysis of the assault shows that noise-based methods of mitigation are insufficient. Therefore, isolation-based mitigation strategies must be considered to stop realistic clandestine communication to guarantee robust security towards timing-based side-channel attacks [215]. The main constraint of the NTRU cryptography with a public keys system, polynomial multiplication, is presented in the paper with a light-weight FPGA-based technology solution. NTRU comprises a lattice-based, quantum-resilient exchange of keys cryptosystem that has been improved for IOT applications through reduced hardware utilization and constant-time implementation, which

provides intrinsic security over timing attacks via side channels [216]. A covert timing channel (CTC) offers a means of leaking private information by manipulating an entity's timing characteristics during non-malicious network communication. The ability to send covert messages without being discovered by conventional security mechanisms like proxies and firewalls is making this a severe danger, making it difficult to identify covert communications. The majority of ML methods for CTC identification rely on statistical features of network traffic, like packets inter-arrival time the entropy [217] this overcomes the creation of effective CTC detectors by the use of deep learning algorithms, particularly LSTM, 1D-CNN, including the LSTM-CNN composite model. The serial data relating to traffic inter-arrival time was used to train the models [218]. By offering one Trusted Execution Environment (TEE) for applications utilizing hardware characteristics like Intel SGX, confidential computing seeks to safeguard the source code as well as data under usage, so ENCIDER uses the SGX computer programming model in analysis and infers probable timing observation points to identify timing along with cache side-channel vulnerability in SGX operations [219]. For sensitive code sections, a JIT compiler creates code so that it's time to execute is mostly or entirely unaffected by the values of confidential information. Without needing duplicate code and specialization prior to distribution, this solution offers adaptive protection with reference to changes between the protection needs and the hardware that underlies it to lessen the timing channel assaults [220].

Introducing NoIR, a randomized mapping mechanism that employs encrypted addresses to map Physical Addresses (PAs) to Last-Level Cache (LLC) slices. PAs are encrypted using the QARMA block cipher, enhancing security. The encryption key changes periodically based on the Slice Access Threshold (SAT) to randomize the PA to LLC slice mapping and thwart potential Network-on-Chip (NoC) side-channel attacks. When an LLC slice surpasses the SAT value in accesses, the encryption key is changed, triggering remapping, and necessitating LLC line invalidation and write-back. This approach effectively obfuscates network contention and raises the difficulty of orchestrating an attack. In Figure. 21 and Figure. 22 for a visual representation of the NoIR mechanism flowchart and attack obfuscation [221]. Schedule-based timing side-channel attacks can be executed without prior knowledge of task parameters. The devised methods to directly infer the number of tasks, as well as the period and execution time of each task from the execution sequence. This eliminates the need for attackers to possess task parameter information beforehand, thereby intensifying the threat posed by schedule-based timing side-channel attacks [222].

The NoIR mechanism with LLC remapping defends against timing-based side-channel attacks by obfuscating interconnect contention, but may entail performance overheads. Future work aims to bolster security, optimize performance, and explore scalability. Additionally, research addresses vulnerabilities in real-time systems by proposing methods to extract task parameter information, highlighting challenges in computational costs. Furthermore, the dynamic compiler approach offers adaptability and reduced overhead, requiring further efficiency enhancements and evaluation. Future research could focus on optimizing isolation-based schemes to enhance security against timing-based SCAs on Network-on-Chip hardware. Moreover, advancements in FPGA designs are suggested to maximize benefits in mitigating timing SCA vulnerabilities and enhancing overall security, while addressing challenges in reconfigurability and complexity.

2) POWER SIDE CHANNEL ATTACK COUNTERMEASURES

A side-channel attack (SCA), a physical attack, uses statistical analysis of physical manifestations to extract private data from cryptographic circuits, first put forth by Kocher, in 1996, relied on power information. Later methods have been investigated to reveal private data in cryptographic implementations, including Simple Power Analysis (SPA) [223], Differential Power Analysis (DPA) [224], Correlation Power Analysis (CPA) [225], and Template Attack (TA) [226]. In SCAs, DPA is noteworthy for its ease of use, efficiency, and low equipment requirements. This method takes advantage of a logic circuit's dynamic power usage, which is impacted by the data that has been processed. Many circuit-level SCA measures to mitigate them, such as sense amplifier-based logic (SABL) [228], three-phased dual-rail (TDPL) [229], delay-based dual-rail precharge logic (DDPL) [230], current mode logic (CML) [227], Fin-SAL [231], EE-SPFAL [232], D3C [233], PGM [234], and dynamic current mode logic (DyCML) [235] have been developed to increase resistance against SCAs. While these techniques have demonstrated excellent resilience against DPA, they often necessitate extensive design efforts due to the inherent trade-off between performance and security. Additionally, certain approaches involve trade-offs between power consumption, delay, and area overhead, this observed trade-off arises as a consequence of the scaling of CMOS technology. Other various techniques aimed at mitigating information leakage in AES engines fall into categories such as data information hiding and/or random masking. Masking techniques serve to mitigate SCA by introducing a random mask during computation. This masking can manifest as additive masking [236], multiplicative masking [237], and the incorporation of rotating S-boxes [238]. In recent years, there's been a growing interest in employing voltage regulators to decorrelate encryption current signatures from input current signatures. On-chip integration of voltage regulators with encryption cores creates isolation for the measurement node, offering a transformed signal at the regulator's input e.g. including current equalization [239], inductive voltage regulators [240], Low-Dropout regulator (LDO) with noise injection and randomization [241], and current domain attenuation [242]. In the work presented

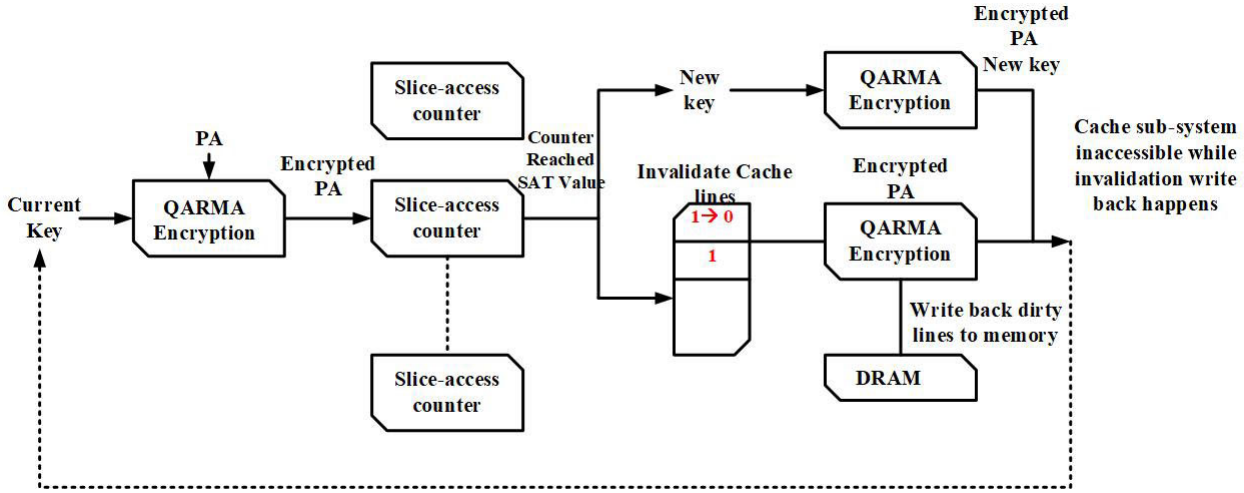

FIGURE 21. NoIR technique, which includes writeback + cache invalidating [221].

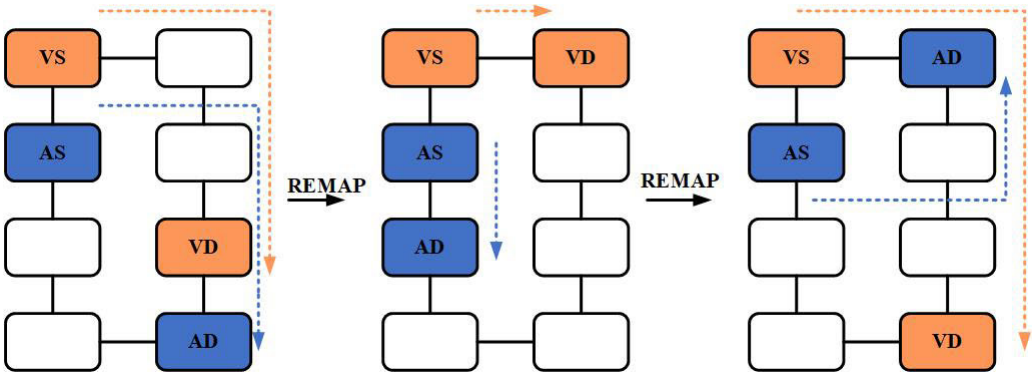

FIGURE 22. Illustration of NoIR-generated obfuscation (AS = Attack Source, AD = Attack Destination, VS = Victim Source, VD = Victim Destination) [221].

a 14-nm CMOS side-channel resistant AES-128 and RSA crypto-processor with demonstrated resistance against time- and frequency-domain power and electromagnetic (EM) attacks. To counter linear LDO vulnerabilities to frequency-domain side-channel attacks, a Non-Linear Digital LDO (NL-DLDO) with control loop randomizations is introduced. Optimizing the LDO side-channel leakage behaviour involves adjusting control loop parameters for enhanced SCA resistance. An on-die linear-feedback shift register (LFSR) randomizes these parameters, significantly improving frequency-domain MTD by 1900× over an unprotected AES engine [243]. Recently, emerging devices with unique properties have demonstrated potential in hardware security applications. Proposed SCA-resistant circuits utilizing these emerging transistors aim for high security at low cost. Presenting a novel Three-Independent-Gate Silicon Nanowire Field Effect Transistor (TIGFET) with inherent SCA-resilient features. The design seeks to strike a balance between cost, performance, and security trade-offs' in cryptographic implementations, it confirms that cryptographic implementations based on TIGFET demonstrate a 42.37% reduction in area usage, a 61.16% enhancement in energy efficiency, a 5.35× decrease in power variation, and attains a degree of SCA resistance similar to the CMOS counterpart [96]. In the work introduced the first utilization of emerging TFET characteristics and non-volatile compatibility STT-MTJ devices to bolster hardware security with ultra-low energy consumption at decreased supply voltages. TFET-based SABL gates are suggested to achieve three times lower energy consumption compared to Si FinFET SABL designs. Furthermore, a TFET PRIDE S-box, designed with TFET SABL gates, exhibits higher DPA resilience with 3.2× lower energy consumption compared to FinFET designs [47]. A different design approach shows how TFET-based Current Mode Logic (CML) might enhance DPA robustness and retain minimal power consumption in a targeted design. This approach is evaluated using the light-weight cryptographic circuitry KATAN32. The TFET CML circuit achieves roughly the same amount of DPA resistance at a 15-times lower power consumption than CMOS-based CML circuits [54]. Employing HyperFET devices in security applications and the development of new paradigms to enhance security

against Power Analysis attacks. A demonstrative example includes the design and simulation of a 4-bit Substitution box for the PRIDE algorithm using predictive models. The results show a significant improvement in security levels, with a factor of at least x25 against DPA attacks [64]. The NCFET-based PRESENT-80 block cipher design achieves approximately 3.2× lower energy consumption compared to the baseline 40 nm CMOS design under similar constraints. Evaluation against DPA attacks shows high resilience, with the NCFET-based design achieving around 4× increased attacker effort ratio and low SNR values compared to the baseline CMOS design [147]. RRAM provides opportunities to counteract SCAs/DPAs due to inherent characteristics such as write time variability, ultra-low power (0.1-3 pJ/bit), and high density ($4F^2$). The research tackles DPA attacks by obscuring the power profile through the utilization of inverse RRAM modules [244]. Utilizing TFET implementations of dualprecharge logic primitives optimized in three ways for their computation tree, the creation of the PRIDE 4-bit substitution box demonstrates significant security gains. In TFET technology, DPA attacks on these proposals show a failure rate of 34 out of 48 attacks targeting optimized computation trees, along with a substantial power reduction (×25), with comparison to CMOS-based counterparts of 65 nm [49].

MTD is the bare minimum of input patterns required to disclose a cryptographic device's accurate key. It functions as an essential parameter for measuring the efficacy of countermeasures suggested by DPA. An overview of the observed MTD values is shown in Table 6. The use of SCA to attack Neural Network(NN) implementations has gained a lot of interest lately. A convolutional neural network (CNN) may be reverse-engineered in its entirety using memory and clock side-channel leakages via off-chip memory access patterns, as proven in [245]. The FPGA-based NN solution is presented by Dubey et al. [246] to protect an MNIST classifier from power-based side-channel assaults through the use of arithmetic masking. They strengthened the defence in a later paper [247] by adding Boolean masking methods based on Trichina gates. Characterizing NN hardware becomes even more difficult since, even with the same NN circuitry, its activity might vary greatly based on the NN design, data sparsity, and scheduling technique [248]. Thus, the adoption of masking-based approaches, which are not bound by operative workloads and may be smoothly integrated with the digital procedure flow. Introducing a Threshold Implementation (TI) masking-based NN accelerator which enhances the security of model parameters and inputs against power and EM SCAs. The 0.159 mm^2 demonstration in 28 nm operates at 125 MHz with 0.95 V, featuring limited area and energy overhead at 64% and 5.5×, respectively. The design demonstrates security surpassing 2 million traces [249], and analyzed side-channel vulnerabilities, with different methods like test Vector Leakage Assessment (TVLA), correlation Power Analysis (CPA), and horizontal Power Analysis (HPA) tests. The first-ever deep learning non-profiled SCA against embedded devices is Differential Deep Learning Analysis (DDLA). To address the difficulties found, the method provides a non-profiled SCA technique using multi-output categorization. This includes using multi-output convolutional neural networks and multi-output multilayer perceptron's to a range of SCA-protected techniques, such as trace de-synchronization countermeasures, noise production, and masking. However, this model executes the assault up to 9 to 30 times faster than DDLA in the presence of masking and de-synchronization measures to counter them, respectively. DDLA requires numerous training procedures to identify the proper key. Furthermore, the suggested model obtains a success rate that is higher of not less than 20% in the scenarios when the standard deviation is between 1.0 and 1.5 when it comes to combined masking and noise creation countermeasure [250].

Various techniques are proposed to address power SCA vulnerabilities in hardware, including TIGFETs, nonlinear digital LDOs, HyperFETs, current-domain signature attenuation, TFETs, security-aware integrated all-digital LDOs, NCFETs, hybrid CMOS/memristor implementations, and the PARC design methodology. These methods aim to enhance resistance against power-based SCAs by improving power efficiency and introducing novel circuit architectures. However, challenges such as area and power overheads, fabrication complexity, and energy consumption need to be addressed through future research to optimize these solutions for broader application in power-sensitive scenarios while maintaining strong security against power SCAs.

3) ELECTROMAGNETIC (EM) WAVE SIDE CHANNEL AND FAULT ATTACK COUNTERMEASURES

Electromagnetic Wave Attacks involve exploiting unintentional electromagnetic emissions from electronic devices to glean sensitive information. These emissions can potentially leak information about the device's operations, facilitating attacks like eavesdropping or unauthorized access. The video interface linking a PC to its monitor emits electromagnetic waves due to time-varying voltage and current. This phenomenon is exploited in the TEMPEST or Van Eck Phreaking attack, where the signal is intercepted. By pointing an antenna towards the PC, attackers can deduce the displayed image on the monitor. This application is of particular interest for Software Defined Radio (SDR) in this context, gr-tempest is an open-source TEMPEST implementation that utilizes GNU Radio, the prevalent Software Defined Radio (SDR) framework. This facilitates straightforward experimentation with various SDR hardware [252]. Polymer nanocomposite-based materials eliminate the necessity for grounding, providing a cost-effective deployment in both materials and installation. Initially designed to prevent EM leakage in small electronic devices, the same methodology applies to larger applications such as Modular Data Centre (MDC) [253].

TABLE 6. Performance Comparison various emerging technologies along with their MTD.

S.No	Design	PDP(fJ)	Avg.power (μW)	Delay(ps)	Avg.MTD
1	TFET SABL based S-box [47]	12.6	6.3	2000.12	–
2	FINFET SABL based S-box [47]	40.201	6.7	6000.17	–
3	TFET classical design [49]	0.86	0.86	1000.02	2175.56
4	TFET-2P [49]	1.04	1.04	1000.23	4437.63
5	TFET - P [49]	0.89	0.89	1000.04	4999.5
6	TFET - P2P [49]	0.96	0.96	1000.15	3014.33
7	UMC-65 classical design [49]	14.103	21.05	670	45.31
8	UMC-65 2P [49]	19.4	25.88	750	1531.25
9	UMC-65 P [49]	14.63	21.83	670	77.56
10	UMC-65 P2P [49]	16.85	23.5	720	1131.19
11	4-bit CMOS based S-box [147]	4.468	5.32	840	–
12	4-bit NCFET based S-box [147]	2.133	7.9	270	–
13	CMOS based PRESENT-80 [147]	9.9382	62.9	1580	16
14	NCFET based PRESENT-80 [147]	3.0893	75.35	410	> 64
15	Present Basic CMOS [96]	0.537	0.82	655.28	512
16	Present CML CMOS [96]	96.808	188.6	513.3	512
17	Present CML TIGFET [96]	196.464	64.5	3045.96	512
18	Balancing RRAM [244]	–	–	–	40000
19	TFET S-box 4-pride [251]	0.87	0.86	1.02	$\gg 2000$
20	HyperFET-14 S-box 4-pride [64]	2.68	5.04	520	> 2000
21	FinFET-14 S-box 4-pride [64]	0.89	5.16	180	224
22	Present-80 (MJT/CMOS)	13.232	20.65	640.8	16000
23	Present-80 (CMOS)	13.723	28.336	484.3	14

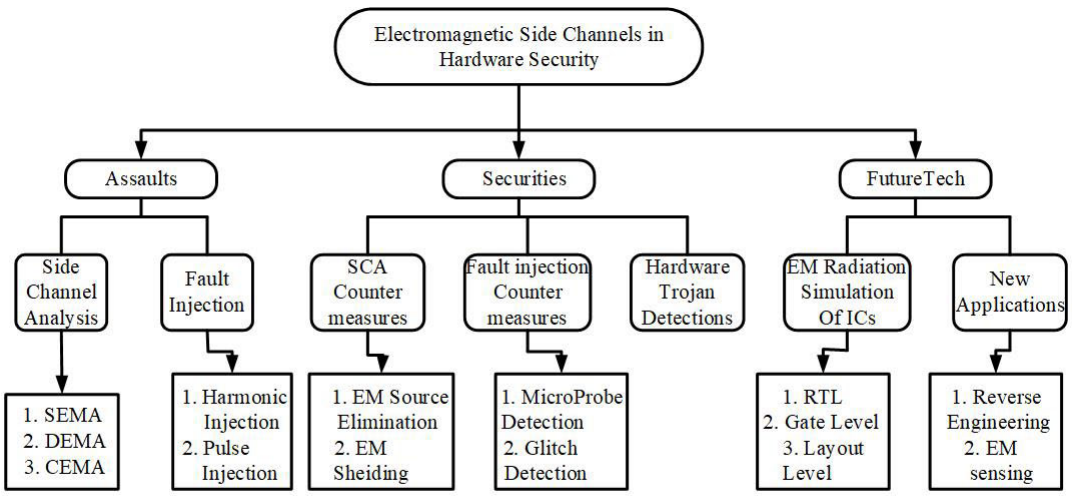

FIGURE 23. The involvement of electromagnetic (EM) side channels in ensuring hardware security [254].

In certain scenarios, attackers engage in passive interception and analysis of unintentionally generated EM waves from devices. Typically, devices exhibiting weak EM emission intensities are not the primary targets. In [255] categorizes this threat as ''Echo TEMPEST.'' Validation is conducted on diverse components, including an evaluation board simulating the I/O circuit of the IC, UART modules, and USB keyboards. Corresponding countermeasures are also provided in the study Figure. 23 presents a thorough overview of electromagnetic SCA and their associated countermeasures within the realm of hardware security. Similar to power attacks, Electromagnetic SCA methods can be categorized into Simple EM Attacks (SEMA), where cryptographic operations are directly interpreted by observing distinct

signal patterns in collected EM traces [256]. In a Differential EM Attack (DEMA), secret keys are extracted from devices applying theoretical values to gathered EM traces to carry out cryptographic algorithms and identifying peaks indicating correct predictions [257], [274]. Additionally, Correlation EM Attack (CEMA) quantifies gathered EM traces against expected values by using the Pearson correlation coefficient as a differentiator. Generally, models such as the Hamming distance and Hamming weight model [258], [259], together with additional enhanced leakage models [260], [261] are utilized to derive anticipated EM side-channel leakage. As noted very well securing cryptographic cores faces escalating challenges with the emergence of EMSCA and FIAs. Notably, techniques like differential fault attacks (DFAs) [262] have the potential to use bug injection to infer sensitive data. Both FIAs and EMSCA have gained widespread popularity due to their simplicity and cost-effectiveness. Recent research has explored circuit-level countermeasures for EMSCA [263], detection circuits for probing approaches [264], and architectures for detecting FIAs [265]. Identification of EM probes via capacitive asymmetry sensing has gained prominence [266], utilizing an on-chip sensing loop through Ansys HFSS-based simulation framework for EM analysis, and a straightforward H-probe detection [267]. The strategic mitigation strategy entails the separation of power and security pathways, facilitating the concurrent application of random parallel power injection and charge recycling mechanisms. Through this implementation, the encryption of supply power activities is achieved, thereby establishing a resilient defence against side-channel attacks. Notably, the approach is designed to mitigate potential side-channel vulnerabilities while minimizing any adverse impact on power consumption and overall system performance [270]. A research endeavour adopts the analogue Current-Mode Differential Signal Analysis (CDSA) concept but enhances scalability across technology nodes by incorporating digital-friendly current sources, a digital control loop, and a digital bleed path. This modification aims to amplify the MTD global feedback for the Digital Signature Attenuation Circuit (DSAC). Additionally, the introduction of the Time-Varying-Transfer-Function (TVTF) circuit technique eliminates the need for direct current (dc) bias in the current-domain equalizer, a prevalent switch capacitor-based countermeasure. The TVTF method transforms it into a digital format and employs a switch capacitor-based circuit for time-domain obfuscation, thereby bolstering overall security [268]. A succinct comparative assessment is provided in Table 7 regarding the contemporary status of digital-friendly countermeasures.

As physical vulnerabilities and corresponding attack methodologies from the perspective of the IC chip have increased predominating. The study introduced an enhanced model for accurately predicting EM radiation emanating from ICs [271]. The researcher showcased a secure packaging technology that seamlessly integrates backside metal wirings with front-side standard CMOS devices in a monolithic fashion. On-chip monitoring circuits were devised and implemented to detect and sense unauthorized access attempts and attacks. The resilience countering multimodal assaults was notably enhanced, particularly through heightened cryptographic analysis involving EM emission and laser injection. This resilience was demonstrated by analyzing system-level circuits-package [272]. The proposition put forth in this study offers an inaugural and comprehensive solution for the pre-fabrication assessment of ICs concerning their resilience against EMSCA [273]. The study introduces a proficient end-to-end framework for detecting and countering SCA leakages, employing EM-X-DL with a high level of confidence even when presented with fewer than 20 averaged electromagnetic (EM) traces. Through the implementation of an innovative algorithm that astutely selects multiple training devices and appropriate hyperparameters, It is possible to efficiently train the suggested 256-class deep neural network (DNN). This training process is facilitated by employing pre-processing techniques such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Fast Fourier Transform (FFT) [275]. The research investigates a physical attack on Ring Oscillator-based TRNGs employing frequency injection [276]. This attack involves the direct injection of a continuous wave into the power line, which serves as the source of randomness for the TRNG [277]. Additionally, a Transient Effect Ring Oscillator (TERO)-based TRNG, akin to an RO-based TRNG, is explored in the context of a physical attack originating from the circuit's proximity. The underlying assumption is that unimpeded physical entry to the intended device may be challenging due to the presence of tamper-resistant features in cryptographic devices [278], [279], [280]. To address this, intentional electromagnetic interference (IEMI) fault injection is proposed as a method for noninvasively injecting faults into a target device from a distance. The impact of these faults on the TRNG's randomness is assessed by tracing the signal leakage from the TRNG at a distance corresponding countermeasures against non-invasive attacks with TRNGs, along with alternative methods, are also considered [279]. Current models for EM radiation and methods for mitigating side-channel vulnerabilities often overlook the original designs' robustness. Moreover, they lack detailed security improvements for susceptible sub-modules or components, resulting in unnecessary overhead on the protected circuit. In response, adaptive strategies have been suggested at the RTL, layout, and device levels. This includes the development of a design/synthesis framework for evaluating and optimizing side-channel security depending on t-test assessment findings obtained from hardware implementations using RTL [281].

This highlights challenges in mitigating EM SCAs in ICs and proposes solutions like systematic hotspot identification. However, implementing robustness measures against EM SCAs may incur higher complexity and cost

TABLE 7. Succinct comparison of various digital-friendly countermeasures.

S.No	Technology	Cryptography Algorithm	Countermeasure Technique	CPA & MTD for Power	CPA & MTD for EM
1	65 *nm* CMOS [268]	AES-256	Digital Signature Attn. (DSAC)+TVTF	390 *M* & >1.25B(>178,000x)	248M & >1.25M(138,888x)
2	14 *nm* CMOS [242]	AES-128	NL-DLDO + Arithmetic Countermeasures	1B (>100,000x)	1B (>100,000x)
3	65 *nm* CMOS [243]	AES-256	Current Domain Signature Attenuation	>1B (125,000x)	>1B (>83,000x)
4	130 *nm* CMOS [269]	AES-128	Digital LDO with randomization	8 *M*(4210x)	6.8M(136x)

compared to CMOS technology. Future research could explore cost-effective techniques to enhance IC resilience against EM side-channel attacks. Additionally, studies on EM SCA against TERO-based TRNGs identify vulnerabilities, emphasizing the need for robust countermeasures and advanced research to mitigate security risks effectively.

D. HARDWARE TROJANS AND IP PROTECTION COUNTERMEASURES

1) HARDWARE WATERMARKING

Hardware watermarking is a technique employed to embed unique and imperceptible identifiers, known as watermarks, directly into the physical components of ICs or other hardware systems. These watermarks serve as a form of hardware-based fingerprint, signatures, enabling the identification and authentication of individual devices. This enables the intellectual property (IP) designer to embed authorship information within the design, maintaining concealment while preserving the functionality of the overall design. The requisites for an effective watermarking strategy encompass the following characteristics [282].

- The integrity of the original design's functionality should remain unaltered by the incorporation of the watermarked design.
- The insertion of the watermark should result in minimal incurred overhead.
- The watermark must exhibit resilience against a spectrum of modification and removal attacks.

IP watermarking methodologies exhibit a taxonomy comprising five distinct categories as depicted in Figure. 24 (a) Constrained (b) Side channel (c) Test structure (d) Digital signal processing (DSP) and (e) Finite state machine (FSM)-based watermarking. Constrained-based watermarking is an approach that includes synthesis at multiple levels: behaviour, system, logic, and physical levels. The number of feasible solutions to this strategy's complicated optimization problem grows exponentially about the amount of the input. IP could be understood as a remedy to the optimization problem in this context [283]. But this method is verification of embedded signatures is frequently challenging, given the potential degradation caused by process variations or aging effects [284]. Techniques based on side channels rely on using process variances to create unique fingerprints. In a study that is cited [285], researchers use glitches to generate a fingerprint, recognizing the restrictions enforced by spatial constraints. On the other hand, delay path changes are used by the researchers mentioned in [286] to incorporate signatures. Side-channel-based watermarking has the benefit of low overhead, but it has drawbacks because it depends on low-level circuit insight, particularly when properly simulating instances at lesser technology nodes and also the drawback that the verifier subsequently extracts the watermark and validates ownership through the utilization of the obtained side-channel information. The watermarking technique based on Finite State Machines (FSM) is integrated at the behavioural level, ensuring compatibility with chip functionality. This is achieved by introducing supplementary FSM transitions or states that do not compromise the overall functionality and it is separated into two categories called state and transition-based FSM techniques where state-based techniques necessitate the encoding of a dynamically changing state or the addition of supplementary states [288] in contrary unused transitions or introduce novel transitions within the FSM [289]. The FSM-based watermarking technique is suggested to adopt a transition-based approach, utilizing field-assisted SOT-MTJ for generating a unique watermark at the circuit level. The external magnetic field serves in a subservient manner employing watermark generation, with the intended circuit enabling users to align and acquire the watermark, thereby providing authentication proof. To ensure resilience against modification and removal attacks, the proposed watermark generation process is strategically embedded post-synthesis, mitigating optimization constraints. The resulting watermark is distinctive and serves as a secure proof of ownership. Notably, the practical implementation of guiding the MTJ with an external magnetic field in an IP core and combining the MTJ block with additional CMOS components in the architecture of a SoC is acknowledged to be intricate and is observed to exhibit reduced robustness against various threat models, particularly the insertion of Hardware Trojans. Skilfully inserted Trojans remain undetected unless they alter the specific 64-bit input sequence necessary to initiate the watermarking operation [290]. This introduces a resilient digital image watermarking system leveraging a memristor-based hyper chaotic oscillator to enhance resistance against image processing attacks. Image quality assessment is conducted using the Human Visual System (HVS) model, and crucial features are extracted through the Histogram of Oriented Gradients (HOG) model. Efficient training is ensured by the Extreme Learning Machine (ELM) model, and secure keys are generated through memristor-based hyper chaotic signals combined with Arnold transformation. The resulting signed image demonstrates imperceptibility and high security, with a PSNR value of up to 41.02 dB and an SSIM value of 0.999. The watermarking

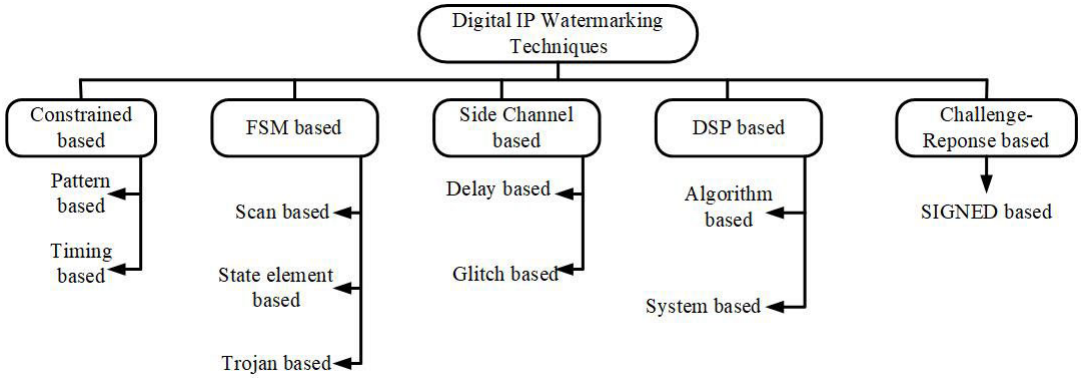

FIGURE 24. IP watermarking methodologies [288].

scheme displays robustness, nearing unity in NC value, against a variety of image processing attacks [291]. Another novel method by Tiwari and Srivastava [292] introduced two image watermarking schemes, the first utilizes Lifting Wavelet Transform (LWT)-Discrete Cosine Transform (DCT) with zigzag scanning-based embedding in the Schur domain and the second employs LWT-Schur decomposition-based embedding in the Schur domain. The LWT-DCT scheme demonstrates heightened resilience to filtering and noise intrusions, evidenced by a Normalized Correlation Coefficient (NCC) of 1.0000. Both schemes exhibit superior imperceptibility and robustness, with NCC values exceeding 0.9800 against diverse checkmark attacks. Performance analysis reveals enhanced outcomes in terms of Peak SNR and NCC, coupled with reduced computational time compared to existing schemes. In search of ensuring the security of DSP-based IP cores is vital for modern SoC designs, where reusable hardware IP cores play a crucial role. To enhance security, an effective watermark can be strategically inserted at the architectural level during the design process. This approach is particularly relevant for DSP designs, which are commonly available in algorithmic descriptions rather than gate-level netlists. Koushanfar et al. [293] included the watermark in the register allocation stage used in the High-Level Synthesis (HLS) procedure to protect IP cores in the high-level design phase. Sengupta et al. [294] also presented a watermarking approach that embeds the vendor's signature using three different stages of the HLS process. In the above two methods, a designer/vendor chooses a signature, which is then transformed into a security feature limitations based on predetermined encoding criteria. This would thwart the malevolent attacker's attempt to decode the real signature. Creating the author's signature using a reliable mechanism will overcome this restriction. Introducing a ground-breaking quadruple-phase watermarking approach, this method revolutionizes the security of hardware IP cores during HLS. Leveraging innovations such as graph partitioning, encoding tree, and eightfold mapping, it crafts a resilient watermarking signature. Notably, the signature is embedded seamlessly during four key HLS phases—scheduling, register binding, resource binding, and interconnect binding—culminating in the creation of a high-quality watermark. Crafting the author's signature involves eight variables, ingeniously encoded into 'eight-variable alphanumeric digits i.e. {'V', 'L', 'S', 'I', '1', '5', 'n', 'm'} through our innovative encoding tree. These digits undergo a transformative journey into a robust hash digest using SHA-512, culminating in the creation of a unique signature. The magic continues as these signature digits dance into security constraints, guided by the designer's chosen eightfold mapping rules. The length of this encoding adventure is tailored to the design's size, with the total bits in the signature reflecting the chosen signature size. Witness the artistry of securing intellectual property unfold, unlocking unparalleled security this [295] approach achieves a remarkable reduction in the probability of coincidence (P_c) and elevates tamper tolerance to new heights, as the number of embedding phases rises, watch in awe as the elusive (P_c) value gracefully descends, unveiling a captivating dance of diminishing probabilities. But that's not all - the watermark's prowess takes centre stage, evaluated in terms of the enchanting Tamper Tolerance (TP). Breaking free from the constraints of existing techniques, an innovative watermarking scheme, aptly named SIGNED (Signature Insertion through Challenge Response in Electronic Design) [287], introduces a dynamic challenge response protocol-based interrogation scheme. Unlike its counterparts, SIGNED breaks the mold, seamlessly integrating into the design at any point in the design process. Brace yourself for superior structural protection and resilience against detection and elimination attempts, all achieved with just modest design overheads. SIGNED where flexibility meets fortitude in electronic design security.

The field-assisted SOT-MTJ and memristor-based hyper-chaotic circuit approaches offer enhanced security in hardware watermarking over CMOS-based methods. Challenges like design complexity and signal fluctuations need addressing for improved reliability. Meanwhile, SIGNED's challenge-response protocol and CAPEC scheme embed circuits in FSM don't care states to minimize overhead, offering superior structural coverage and scalability. Future

research should focus on optimizing these methods for improved efficiency and long-term IP protection

2) LOGIC OBFUSCATION

Logic obfuscation is one of the techniques employed in IP protection to enhance the security of digital designs and prevent unauthorized access or intellectual property theft. The operation of logic obfuscation involves introducing intentional complexity and ambiguity into the design's logical structure, preventing adversaries from easily understanding the underlying reasoning and reverse engineering the original design. Logic locking empowers post-fabrication programmability through the integration of Key Gates (KGs), specialized logic gates whose behaviour is finely tuned by key bits associated with the logically locked netlists. The common unlock methods in the world of logic locking, where complexity meets creativity explore three distinct realms of obfuscation wizardry: (i) XOR-type enchantment, (ii) MUX-type sorcery, (iii) LUT-type wizardry and iv) Functional Stripping operation. The ultimate goal of the logic locking schemes is at its core, logic locking strives to introduce enough error to throw off any incorrect key, ensuring that unauthorized use of the design IP is promptly derailed. In this view to increase the resilience of logic locking techniques, researchers have provided many attacks to have the potential to completely or partially dismantle the protective barriers surrounding the obscured intellectual properties. Some of them are Satisfiable Attacks (SAT), Key Sensitization attacks (KSA), Hill climbing attacks, ATPG-based analysis, Removal or Bypass attacks, SAIL, SURF, SWEEP attacks etc. which provide either structural or functional analysis of attacks. Among all these attacks SAT attack is more potent in identifying the incorrect key sub-sets using these distinctive input patterns (DIPs) and the process repeats until the whole key field is covered and the correct key is disclosed [296]. Numerous counter strategies have been put out to lessen SAT attacks like ANTI-SAT [297], SAR-Lock [298], and TT-Lock [299] which have prioritized offering high-quality output corruptibility. However, aimed at accelerating problem-solving times by minimizing the exclusion of keys per DIP (Dynamic Invariant Point) have been developed. Additionally, ANTI-SAT techniques typically leverage AND/NAND tree-based point function structures. However, their effectiveness was swiftly challenged with the introduction of countermeasures such as removal/signal probability skew (SPS) [300] and bypass [301]. Nevertheless, a different attack known as approximate satisfiability based Attack (AppSAT) [302] poses a threat to the security provided by these techniques. It achieves this by obtaining a rough key that can unlock a netlist's capabilities. The design of Generalized (G-) Anti-SAT [14] introduced the capability for overlap among incorrect key sets. This design strategy involves incorporating a substantial variety of potential functions instead of relying on AND/NAND trees. Notably, it demonstrates increased resilience to removal attacks and enhances resistance against the AppSAT attack, all while maintaining robustness against SAT attacks [303]. CAS-Lock is a logic locking scheme that knows how to balance the risks of corruption with security, maintaining resilience in the face of potential compromises [304]. Additional countermeasures focus on elevating the complexity of SAT instances, thereby extending the runtime required for attacks. Approaches like SATConda [305] achieve this by modifying the conjunctive normal form (CNF) of the design to incorporate unsatisfiable (unSAT) instances. Stripped Functionality Logic Locking (SFLL) [306] enhances corruptibility by incorporating higher-weight Hamming distance checkers. The deliberate increase in corruptibility consistently leads to a reduction in query count. Introducing another technique [307], which seeks to enhance SFLL, involves modifying the functional restoring unit to incorporate an SAT complex function. Various methods, including Full-Lock [308], Enhanced SFLL [308], One-way Random Function (ORF) based SLL [309], and CORALL [310], leverage inherently SAT-Hard functions to significantly heighten complexity against potential attacks. The SAIL attack represents a potent and previously unexplored method in the realm of logic locking. This approach distinguishes itself by leveraging machine learning models to accurately discern structural alterations within a locked design. The feasibility of this attack stems from the fact that logic locking methods, dependent on synthesis tools, induce minimal, localized, and predictable changes to the circuit topology [311]. Within SARO, the integration of efficient hypergraph partitioning plays a pivotal role in enhancing scalability, particularly with large and intricate designs. This strategy enables the widespread implementation of both functional such as SAT-based and structural SAIL attacks. SARO achieves significant output corruption through the meticulous alteration of truth tables in individual partitions and the precise application of distributed attack resistance. As an integral element of its distributed protection framework, SARO integrates RanSAT, a random SAT-hard function generator explicitly crafted to counteract key extraction attempts by SAT attacks [312]. In [313], a novel method called delay locking is introduced to bolster the security of existing logic obfuscation techniques against emerging threats. This approach involves incorporating key-dependent delays into an obfuscated netlist, alongside traditional locking mechanisms. With delay locking, a key not only governs circuit functionality but also influences its timing profile. Consequently, defeating delay locking requires the adversary to devise an attack strategy capable of recovering both the correct functionality and the accurate timing profile of a circuit, satisfying predefined timing constraints. The Timing-SAT [314] attack, aimed at bypassing cutting-edge delay locking countermeasures [313], operates in two stages. Initially, the attacker identifies a correct functional key, followed by the utilization of timing information in the unrolled netlist to execute an iterative SAT attack for retrieving a correct delay key. Subsequently, the developed technique, SFDL,

not only withstands Timing-SAT attacks but also effectively foils any logic-locking attack that is known to exist. A novel analysis of SAT attack offers a distinct viewpoint on SAT attack efficiency through the examination of CNF stored in the SAT solver [315]. Employs a cognitive approach using neural networks to automatically extract feature variables for learning SAT and SAT-hard distributions. These distributions are then leveraged to convert a CNF from SAT to SAT-hard by adding minimal circuitry overhead, ensuring enhanced security compared to current defences [316]. Introducing Titan [318], a comprehensive attack framework targeting large-scale hardware obfuscation. Titan utilizes a Graph Neural Network (GNN) for sub-graph classification, leveraging both structural and functional hints inherent in extensive obfuscation. To enhance accuracy, an oracle-guided post-processing technique is implemented for refining GNN outputs. Introducing another twig of logic encryption ReTrust FSM, a cutting-edge FSM-based logic locking technique designed to address various threats against logic locking. Operating at the RTL, ReTrust FSM utilizes behavioural state transition coding for obfuscation, incorporating both keyless and key-based (implicit and explicit external secrecy) locking methods. This approach enhances robustness, particularly against oracle-guided I/O query-based attacks and structural+functional attacks. Additionally, ReTrust FSM formulates the connection between the predicted de-obfuscation time and Boolean features [317]. To gain further insights into recent advancements in logic locking, consult the following papers for a brief literature review [319], [320], [321], [322], [323], [324]. Overall various attacks have been devised to undermine the resilience of logic locking techniques, aiming to circumvent the protective barriers shielding obscured intellectual properties. While these attacks reveal vulnerabilities and aid in understanding the limitations of logic locking, they also necessitate extensive computational resources and expertise. Additionally, they highlight the ongoing challenge of balancing security and performance in logic locking implementations, urging researchers to continuously refine defense mechanisms against evolving threats.

SATConda improves security against SAT attacks while minimizing overhead, but scalability challenges persist. Future research aims to optimize its performance and explore broader applications. CAS-Lock enhances logic obfuscation security but needs refinement against removal attacks. Delay-locked circuits offer improved security but face IP piracy risks, prompting the need for strengthened solutions. G-Anti-SAT boosts security in logic obfuscation but may face implementation complexities, urging streamlining efforts for practicality. Overall, logic obfuscation techniques offer protection but require optimization for reduced overhead and enhanced security in IC designs.

3) HARDWARE TROJANS COUNTERMEASURES

A hardware Trojan refers to the illicit insertion of malicious circuitry or alterations into a hardware design or integrated circuit during the manufacturing or design phase. The goal of a hardware Trojan is typically to compromise the functionality, security, or reliability of the affected hardware without being easily detectable. More Common techniques used like structural obfuscation, split manufacturing, camouflaging, PUFs, and key-based security are essential for effective hardware Trojan prevention. This approach, customized to the hardware's characteristics and application, enhances overall security. Designing an IP core from the lower abstraction level of system design can be challenging for IP designers. Hence, synthesizing DSP algorithms at the hardware level using an HLS framework is crucial for IP core design. The recent advancements towards DSP IP cores presented a novel hybrid approach to secure DSP IP cores by combining structural obfuscation and encrypted chromosomal DNA impressions. This dual-layer security strategy defends against RTL-level alterations with multilevel structural obfuscation and thwarts IP piracy through covertly implanted, encrypted DNA impressions. Experimental results show superior robustness compared to recent biometric and steganography-based hardware IP security techniques, emphasizing enhanced digital evidence proof and tamper tolerance [325]. Unlike many prior works, this approach uniquely focuses on structurally obfuscating DSP circuits using a multi-key-based approach, a methodology not extensively explored in existing research. Another novel approach for DSP circuits, incorporating key-driven partitioning, folding knob-based obfuscation, and other key-driven transformations. The method introduces innovative multi-variable signature encoding for physical-level watermarking on key-based structurally obfuscated DSP circuits [326] and molecular biometric method to strengthen DSP IP core security [17]. Split manufacturing is a cutting-edge technique in semiconductor manufacturing aimed at bolstering security by dividing the fabrication process into multiple phases like Front-End-Of-Line (FEOL) and Back-End-Of-Line (BEOL). This approach involves the separation of critical components of a chip, particularly the most sensitive or security-critical parts, from the standard manufacturing process [327]. FEOL encompasses the initial stages of chip fabrication, including processes like transistor formation and interconnect layers. In split manufacturing, the sensitive logic, typically containing cryptographic elements or secure components, is fabricated during the FEOL phase. By isolating and fabricating the critical logic during the FEOL phase, security measures specific to these components can be applied. BEOL involves the later stages of chip fabrication, focusing on metal layers, interconnects, and other components that enable connectivity between different parts of the chip. In split manufacturing, the non-sensitive portions of the chip are typically fabricated during the BEOL phase, the non-sensitive portions are fabricated during BEOL, the security focus here may be on ensuring the integrity of the interconnects and preventing any tampering or malicious modifications during the back-end processes [327], [328], [329], [330]. Recently, split manufacturing has been employed in 3D integration IC design, featuring a novel Smart Partitioning

(SP) procedure with metrics to measure its effectiveness. A physical demonstration underscores the feasibility and efficacy of these manufacturing techniques [328]. A secure fabrication flow for untrusted foundries, this approach ensures k security with a flexible trade-off between area and the number of withheld private connections. Employing a scalable clustering algorithm, the method applies to large circuits, exceeding 10k gates. Results demonstrate a reduction of private wires to 74.81% for the standard cell approach and to 91.33% for the LPG/LUT approach in the k secure netlist, dependent on the specific design and the chosen value of k [329]. The feasibility of a deep learning technique combined with routing perturbation for timing-critical and congested designs. The rerouting needed after inserting blockages naturally incurs power overheads through additional buffers or upsizing standard cells, all while prioritizing timing maintenance [331].

The proposed synthesis-based approach aims to enhance security against hardware trojan attacks during fabrication through secure technology mapping and limited programmability gates. Concerted Wire Lifting offers a cost-effective solution by strategically lifting wires to higher metal layers, while split manufacturing provides robust defense by separating FEOL and BEOL processes. However, challenges like proximity attacks persist, indicating the need for advanced encryption methods. Additionally, experiments address hardware Trojan vulnerabilities in 3-D integrated circuits, highlighting the importance of optimizing partitioning processes for efficient security solutions.

VI. MACHINE LEARNING IN HARDWARE SECURITY

Machine learning is pivotal in bolstering the durability of hardware systems against a myriad of threats and vulnerabilities within the domain of hardware security. Using data-driven methods, machine learning enables the creation of advanced intrusion detection systems, anomaly detection algorithms, and security-aware hardware designs. By analyzing extensive datasets from hardware components like system logs and sensor readings, machine learning models detect abnormal behaviour signalling security breaches, pinpoint potential vulnerabilities in hardware designs, and enable proactive security measures. In PUFs various strategies have been suggested to counteract machine learning-based modelling attacks on PUFs, including injecting poison data into training sets, introducing inconsistent CRPs, and implementing additional hardware mechanisms like TRNGs or weak PUFs, but they may still retain vulnerabilities. In response, more intricate PUF designs have been proposed to heighten the difficulty of executing modelling attacks. These designs, such as reconfigurable PUFs, possess the ability to adjust their behaviour dynamically, thus thwarting attempts at modelling attacks.

In recent work with experimental validation of a protection mechanism for APUFs via FPGA implementation demonstrated by modifying the Challenge-Response Pair (CRP) mechanism and introducing contradictory data, makes the mechanism notably improved response uniformity, countering modelling attacks effectively and validating its efficacy in fortifying PUFs against adversarial threats [196]. The Recurrence-based PUF is another novel approach to utilizes feedback mechanisms and XOR functions to bolster security. Both Rec-CMAPUF and Rec-DAPUF designs in work show promise in resisting ML attacks, ensuring reliability, and optimizing power consumption and energy efficiency [185] and random Set-based Obfuscation (RSO) is employed to strengthen Strong PUFs against ML attacks [197]. Another approach without altering the hardware the reconfigurable architecture and challenge-dependent stage delays improve its security, reliability, and resilience against diverse attacks [201]. Implementing a modulus response boundary system can boost resistance against machine-learning attacks by dividing the Integer Response Value (IRV) space into regions with alternating binary response values. This approach is applied to RO-PUF. Another solution, the alternating modulus ring oscillator PUF (AMRO-PUF), aims to balance ML resilience and reliability, enhancing security against modelling attacks with minimal area overhead [206]. Logic Locking is the other twig of hardware security performs with various attacks like Satisfiable Attacks (SAT), Key Sensitization attacks (KSA), Hill climbing attacks, ATPG-based analysis, Removal or Bypass attacks, SAIL, SURF, SWEEP attacks, and others aim to conduct either structural or functional analyses to undermine locked designs. Using Neural Network models, the SAIL attack effectively analyzes and exploits structural artifacts of logic locking. SAIL-NN predicts changes in key gate localities after logic locking, prioritizing modified areas to optimize structural recovery. Additionally, the Reconstruction Model within SAIL-NN leverages machine learning to revert post-synthesis structural changes, aiding in the retrieval of the original gate-level structure. Moreover, SAIL-RD employs rule dictionaries learned through machine learning to accurately reverse synthesis-induced modifications. Through the integration of machine learning techniques, the SAIL attack offers a systematic and powerful approach to identifying vulnerabilities in locked designs, highlighting the potential of machine learning in hardware security applications [311]. Also, deep learning algorithms like CNNs and GNNs enhance the robustness of logic locking schemes by extracting features, predicting attacks, leveraging graph representations for circuit understanding, and automating design processes. This strengthens defenses against deobfuscation attacks like SnapShot and advances the development of more resilient locking mechanisms [323]. D-MUX is a multiplexer-based logic-locking scheme crafted to resist structure-exploiting machine learning attacks. It incorporates machine learning resilience to fend off known learning-based attacks, paving the way for future logic locking designs in the era of machine learning [324]. The SVM-based framework distinguishes itself from other algorithms with its generic, blind detection mechanism rooted in machine learning and statistical analysis of traffic fingerprints. This makes it a promising method for identifying

covert timing channels in network communications [217]. In summary, the ongoing research in machine learning for hardware security should emphasize more towards to enhance adversarial robustness, interpretability, develop privacy-preserving techniques, explore transfer learning, optimize for hardware efficiency, and investigate hybrid approaches. These efforts are geared towards addressing key challenges and advancing the security of hardware systems.

VII. CHALLENGES AND OPPORTUNITIES IN HARDWARE SECURITY USING EMERGING DEVICES

A. CONCEPTUAL CHALLENGES

- The diverse characteristics of emerging devices make seamless integration into existing hardware architectures challenging
- Identifying and understanding security vulnerabilities inherent in emerging devices is essential for effective mitigation.
- Lack of standardized security measures tailored to emerging devices hinders the establishment of a unified security framework.
- Establishing empirical metrics to quantify the level of security assurance provided by emerging devices is complex.
- Ensuring security throughout the lifecycle of hardware, including manufacturing, deployment, and end-of-life phases, is a multifaceted challenge.
- Developing adaptive security measures capable of dynamically responding to evolving threats is crucial for long-term efficacy.
- Achieving effective hardware security with emerging devices requires collaboration between hardware engineers, cybersecurity experts, and other relevant disciplines.
- Quantum computers have the potential to break widely used cryptographic algorithms, necessitating the development of quantum-resistant security solutions.

B. CONCEPTUAL ROADMAP

1) INTEGRATION OF EMERGING DEVICES

The integration of emerging devices with the latest technologies represents a transformative phase in the realm of electronics. This process involves seamlessly incorporating innovative components like memristors, spintronic devices, and quantum devices [332] into existing systems. One of the primary challenges lies in ensuring compatibility and establishing standardized interfaces for the smooth integration of these emerging technologies. However, the benefits are substantial, ranging from enhanced performance, characterized by lower power consumption and faster processing speeds, to the introduction of entirely new functionalities. The applications are diverse, spanning memory technologies, quantum computing, neuromorphic computing, and more. Ongoing research and collaborative efforts between interdisciplinary teams and industry partners drive the development of these emerging devices, contributing to advancements in various fields such as computing, communications, and healthcare. As these technologies continue to mature, their integration with the latest devices holds the promise of shaping a future where innovative capabilities and increased efficiency redefine the landscape of electronic systems.

2) EMERGING IN QUANTUM COMPUTING

On one hand, the advent of powerful quantum computers raises concerns about their capability to break widely-used cryptographic algorithms, rendering current security protocols vulnerable [332]. On the other hand, quantum principles also offer potential solutions for enhancing hardware security. Quantum Key Distribution (QKD) is a promising application that leverages using quantum mechanical concepts to create secure communication connections, providing a quantum-safe alternative to traditional encryption methods. As quantum computing continues to advance, its role in shaping the future of hardware security involves navigating the delicate balance between potential vulnerabilities and transformative security solutions [333].

3) VULNERABILITY ASSESSMENT

Vulnerability assessment with the latest devices involves a comprehensive examination of potential weaknesses and security gaps in cutting-edge technologies, such as IoT devices, AI-driven systems, and emerging hardware. This process is crucial for identifying and mitigating potential risks that may arise from the adoption of these advanced devices.

4) ENABLING BLOCK CHAIN LIFE CYCLE SECURITY

Securing the end-to-end lifecycle of digital assets and transactions using blockchain technology. This methodology leverages the decentralized and immutable nature of blockchain to enhance security at various stages, including the creation, storage, transmission, and utilization of digital assets. Through the use of cryptographic hashing, consensus mechanisms, and smart contracts, blockchain ensures the integrity and transparency of data, preventing unauthorized alterations and unauthorized access. Smart contracts embedded in the blockchain can automate and enforce security protocols, streamlining processes such as access control and validation. This approach is particularly impactful in industries such as supply chain, finance, and healthcare, where maintaining the integrity of digital records and transactions is paramount [334]. By integrating blockchain into the lifecycle of digital assets, organizations can establish a trustworthy and auditable foundation for their operations, reducing the risk of fraud, tampering, and unauthorized access throughout the entire lifecycle.

5) QUANTITATIVE SECURITY METRICS

The systematic measurement and analysis of security-related data to quantify the effectiveness of an organization's cybersecurity posture. These metrics aim to provide a numerical and objective assessment of various security

TABLE 8. Tabular representation of the advantages of post-CMOS technology with their unique characteristics over traditional CMOS in various hardware security primitives.

S.No	Security primitives	Traditional CMOS	Post-CMOS Technology
1	TRNG	Vulnerable to process variations and external influences affecting randomness.	Improved randomness and entropy due to unique physical phenomena, such as quantum effects in quantum-dot cellular automata (QCA) or spintronics.
2	PUF	Susceptible to modeling attacks and variations in manufacturing.	Increased security and uniqueness through unconventional physical characteristics, such as nanoscale variations in resistive switching devices or memristors.
3	Hardware Trojans	Limited defenses against insertion and detection of Trojans.	Enhanced resistance to Trojan insertion and improved Trojan detection mechanisms, leveraging nanoscale structures and unconventional materials.
4	Timing Side Channel Attack	Susceptible to timing attacks and clock manipulation.	Improved control over timing characteristics, reduced clock skew, and enhanced synchronization methods in post-CMOS technologies.
5	Power Side Channel Attack	Prone to leakage of power consumption information.	Lower power consumption and reduced leakage in post-CMOS devices, minimizing information leakage in power side-channel attacks.
6	Cache Side Channel Attack	Vulnerable to cache-based attacks, such as side-channel attacks and cache poisoning.	Enhanced cache security through novel cache designs and technologies, reducing susceptibility to side-channel attacks.
7	EM Side Channel Attack	Susceptible to electromagnetic emissions side-channel attacks.	Improved shielding and control over electromagnetic emissions in post-CMOS devices, reducing vulnerability to EM side-channel attacks.
8	Logic Obfuscations	Limited options for obfuscation techniques, making reverse engineering easier.	More advanced and diverse logic obfuscation methods, leveraging unique post-CMOS properties, to complicate reverse engineering efforts.
9	Logic Locking	Limited effectiveness in preventing reverse engineering attacks.	Enhanced resistance to reverse engineering through advanced logic locking techniques based on post-CMOS characteristics.
10	Hardware Watermarking	Limited options for embedding and detecting watermarks.	Improved capabilities for hardware watermarking, utilizing unique identifiers from post-CMOS properties, providing robust identification and authentication.

aspects, including threat detection, incident response, and overall risk management. Key quantitative security metrics may include the number of security events discovered, the typical time it takes to find and address them to a threat, the effectiveness of security controls, and the financial impact of security incidents. By quantifying these aspects, organizations gain insights into the efficiency of their security measures and can make data-driven decisions to allocate resources effectively [335]. These metrics are essential for communicating the state of cybersecurity to stakeholders,

TABLE 9. Tabular representation of the unique characteristics of various Post-CMOS technologies and more suitable hardware security primitives over traditional CMOS.

S.No	Post-CMOS Technology	Unique Characteristics	Suitable Hardware Security Primitives
1	TFET	Low subthreshold swing, reduced leakage, and improved energy efficiency compared to MOSFETs.	Suitable for TRNG, PUF, and Logic Obfuscations due to improved energy efficiency and lower vulnerability to side-channel attacks.
2	CNTFET	Excellent electrical and thermal properties, leading to high performance and energy efficiency.	Suitable for TRNG, PUF, and Hardware Trojans due to their high-performance capabilities and resilience to certain types of attacks.
3	SiNWFET	Nanoscale structure allows for better control of current flow, leading to improved performance.	Suitable for Timing Side Channel Attack and Hardware Trojans due to better control over timing characteristics and enhanced security features.
4	NCFET	Utilizes negative capacitance to amplify the gate voltage, leading to lower power consumption.	Suitable for Power Side Channel Attack, TRNG, and Logic Obfuscations due to reduced power consumption and improved security features.
5	Memristors	Non-volatile memory with resistance that can be changed and modulated..	Suitable for PUF, Hardware Trojans, and Logic Locking due to their unique resistive switching characteristics and non-volatile memory properties.
6	PCM	Utilizes the phase change between amorphous and crystalline states for data storage.	Suitable for Hardware Watermarking, PUF, and Logic Locking due to its non-volatile nature and resistance to certain types of attacks.
7	STT-MJT	Utilizes spin-polarized electrons to store data, providing non-volatility and high speed.	Suitable for TRNG, PUF, and Logic Locking due to its non-volatile and high-speed properties.
8	HyperFET	Combines TFET with ferroelectric materials for improved performance.	Suitable for Timing Side Channel Attack, Power Side Channel Attack, and Logic Obfuscations due to enhanced performance and security features.
9	RRAM	Non-volatile memory based on resistive switching.	PUF, Hardware Trojans, Logic Locking
10	2.5D /3D Integration	Stacking multiple dies for improved performance and reduced footprint.	Improved overall security by reducing inter-die communication vulnerabilities.

supporting risk assessments, and continually improving security strategies based on measurable outcomes.

6) INTERDISCIPLINARY COLLABORATION

Through interdisciplinary collaboration, researchers and practitioners can combine their expertise to develop holistic security solutions that consider the unique properties of the devices mentioned in this article. This collaborative approach fosters a comprehensive understanding of both the hardware and security aspects, enabling the creation of robust and adaptive security measures. Furthermore, interdisciplinary collaboration facilitates the integration of insights from different domains, contributing to the development of standards and best practices for securing emerging devices, thereby enhancing the overall resilience of future hardware systems.

VIII. FUTURE RESEARCH DIRECTIONS

The future of hardware security is beyond CMOS, venturing into realms like memristors, spintronics, quantum and neuromorphic computing. These exotic technologies offer unique security benefits, from physically unclonable functions to inherently resilient architectures. Research efforts are blazing

TABLE 10. Overview of emerging device candidates paired with state-of-the-art countermeasures along with future research directions.

Post - CMOS Devices	Hardware Security Primitives									Future Research Direction
	TRNGs	PUFs	Timing SCA	Power SCA	EM SCA	Hardware Trojans	Logic Locking	Hardware Watermarking	Logic Obfuscation	
CNTFET	✓	✓				✓				1.Improving Carrier Mobility. 2.Reducing Contact Resistance.
HyperFET			✓	✓					✓	1.minimize gate leakage 2.Balancing bias voltage
Memristors		✓				✓	✓			1.phase transitions 2. minimizing resistance drift 3.ion migration 4.Optimizing switching voltages and currents
NCFET	✓			✓					✓	1.Hysterisis engineering 2.Better electrostatic control 3.Transconductance
PCM		✓					✓	✓		1.stabilize resistance states
RRAM	✓	✓				✓	✓			1.Multi-Level Cell Operation 2.Endurance and Retention Improvement
SiNWFET			✓			✓				1.High drive current 2.Reducing OFF-state leakage
STT-MJT	✓	✓					✓			1.Optimizing the tunnel barrier thickness 2.Finding materials with high PMA.
TFET	✓	✓					✓			1.steeper tunneling characteristics and lower subthreshold slopes 2.Material Integration 3.negative bias temperature instability (NBTI) 4.Ambipolar Leakage

trails in exploring these materials for robust hardware primitives and secure logic, while simultaneously emphasizing proactive security through ''security-by-design'' principles. To accelerate progress, interdisciplinary collaboration is key, bringing together material scientists, computer architects, and cryptographers to unlock the full potential of beyond CMOS. In pursuit of robust hardware security primitives, future research directions involve enhancing certain characteristics of post-CMOS technologies, as delineated in the Table 10.

IX. SUMMARY AND DISCUSSION OF RECENT ADVANCES HARDWARE SECURITY USING POST-SILICON TECHNOLOGIES

After a comprehensive examination and analysis, recent advances in post-silicon technologies offer promising avenues for improving hardware security. The unique characteristics of these technologies, such as reduced power consumption, improved energy efficiency, and non-volatile memory properties, etc contribute to the development of more secure and reliable hardware components.

The integration of advanced transistor technologies and innovative memory solutions enables the creation of hardware security primitives with improved resilience against various attacks, including side-channel attacks and hardware Trojans. Additionally, stacking techniques like 2.5D/3D integration contribute to better overall security by minimizing vulnerabilities in inter-die communication which is an ongoing research in industries [336]. Table 8 presents the advantages of Post CMOS technology over traditional CMOS of various security primitives. It's important to note that the effectiveness of these advantages depends on the specific post-CMOS technology being considered and the field is continuously evolving with new developments and discoveries. Different post-CMOS technologies with unique characteristics that make them more suitable for specific security countermeasures which is depicted in Table 9. TRNG With a maximum throughput of 1 Gb/s, it is based on the Diffusive Resistivity of 3-D RRAM. The shown 3-D RRAM device has low power consumption, high density, and compatibility with cutting-edge CMOS technology [161]. When using RRAM state memory with 40,000 power traces to balance logic, the DPA attack proved ineffective [244]. Further, TFETs are a viable option for safe circuit design in new technologies because they can increase circuit design resilience to power analysis assaults [49]. At last, the key finding is that there is sufficient space for new security advancements through the use of cutting-edge technologies in low-power, secure applications.

X. CONCLUSION

The exploration of Post-silicon devices in the realm of hardware security presents a transformative landscape filled with opportunities and challenges. The inadequacies of existing hardware security methodologies, exacerbated by CMOS technology scaling and emerging threats, necessitate a shift toward alternative solutions. Post-silicon devices emerge as a promising avenue, offering superior characteristics that can enhance security measures. This review paper delves into various post-CMOS devices, showcasing their unique attributes and applications in hardware security. We have highlighted the challenges they pose and the benefits they bring compared to traditional CMOS technology. The multi-faceted nature of hardware security, spanning secure architectures, IP components, DNN models, and hardware-intrinsic security primitives, requires a nuanced approach, and Beyond-CMOS devices provide valuable insights. Ongoing efforts in developing security-driven hardware design tools further underscore the industry's commitment to addressing evolving threats. As the hardware security landscape continues to evolve, this review serves as a timely exploration of the pivotal role played by Beyond-CMOS devices, offering opportunities for future research and development in securing the next generation of computing technologies.

REFERENCES

[1] S. Schmeelk, K. Thakur, M. L. Ali, D. M. Dragos, A. Al-Hayajneh, and B. R. Pramana, ''Top reported data security risks in the age of COVID-19,'' in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Dec. 2021, pp. 204–208, doi: 10.1109/UEMCON53757.2021.9666573.

[2] J. Kim, J. Shin, K.-W. Park, and J. Taek Seo, ''Improving method of anomaly detection performance for industrial IoT environment,'' *Comput., Mater. Continua*, vol. 72, no. 3, pp. 5377–5394, 2022, doi: 10.32604/cmc.2022.026619.

[3] A. K. Alnaim and A. M. Alwakeel, "Machine-learning-based IoT-edge computing healthcare solutions," *Electronics*, vol. 12, no. 4, p. 1027, Feb. 2023, doi: 10.3390/electronics12041027.

[4] J. Zhou, Y. Shen, L. Li, C. Zhuo, and M. Chen, "Swarm intelligence based task scheduling for enhancing security for IoT devices," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 6, pp. 1756–1769, Jun. 2023, doi: 10.1109/TCAD.2022.3207328.

[5] J. H. Nguyen, W. Liao, and W. Yu, "Towards secure communications in heterogeneous Internet of Things," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Honolulu, HI, USA, Feb. 2023, pp. 426–430, doi: 10.1109/ICNC57223.2023.10074323.

[6] I. Heintz, J. Grothendieck, F. Bernardin, and G. Kuperman, "Improving text security classification towards an automated information guard," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Rockville, MD, USA, Nov. 2022, pp. 757–762, doi: 10.1109/MILCOM55135.2022.10017557.

[7] I. M. Asăvoae, R. T. Shirazi, A. Riesco, and U. Yasuyoshi, "Hardware trojan detection via rewriting logic," *J. Log. Algebr. Methods Program.*, vol. 127, Jun. 2022, Art. no. 100762, doi: 10.1016/j.jlamp.2022.100762.

[8] M. Morsali, M. H. Moaiyeri, and R. Rajaei, "A process variation resilient spintronic true random number generator for highly reliable hardware security applications," *Microelectron. J.*, vol. 129, Nov. 2022, Art. no. 105606, doi: 10.1016/j.mejo.2022.105606.

[9] Q. Ding, H. Jiang, J. Li, C. Liu, J. Yu, P. Chen, Y. Zhao, Y. Ding, T. Gong, J. Yang, Q. Luo, Q. Liu, H. Lv, and M. Liu, "Unified 0.75 pJ/bit TRNG and attack resilient 2F2/bit PUF for robust hardware security solutions with 4-layer stacking 3D NbOx threshold switching array," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2021, pp. 39.2.1–39.2.4, doi: 10.1109/IEDM19574.2021.9720641.

[10] W. Y. Yang, B. Y. Chen, C. C. Chuang, E. R. Hsieh, K. S. Li, and S. S. Chung, "Novel concept of hardware security in using gate-switching FinFET nonvolatile memory to implement true-random-number generator," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2020, pp. 39.3.1–39.3.4, doi: 10.1109/IEDM13553.2020.9371993.

[11] M. M. Fazili, M. F. Shah, S. F. Naz, and A. P. Shah, "Next generation QCA technology based true random number generator for cryptographic applications," *Microelectron. J.*, vol. 126, Aug. 2022, Art. no. 105502, doi: 10.1016/j.mejo.2022.105502.

[12] *Estimate Cost From Cybersecurity Worldwide 2017–2028*. Accessed: Sep. 15, 2023. [Online]. Available: https://www.statista.com/statistics/1280009/cost-cybercrime worldwide

[13] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1010–1038, Jun. 2021, doi: 10.1109/TCAD.2020.3047976.

[14] J. Knechtel, "Hardware security for and beyond CMOS technology," in *Proc. Int. Symp. Phys. Design*, Mar. 2021, pp. 115–126, doi: 10.1145/3439706.3446902.

[15] A. Japa, M. K. Majumder, S. K. Sahoo, R. Vaddi, and B. K. Kaushik, "Hardware security exploiting post-CMOS devices: Fundamental device characteristics, state-of-the-art countermeasures, challenges and roadmap," *IEEE Circuits Syst. Mag.*, vol. 21, no. 3, pp. 4–30, 3rd Quart., 2021, doi: 10.1109/MCAS.2021.3092532.

[16] S. Kaur, B. Singh, and H. Kaur, "Analytical classifications of side channel attacks, glitch attacks and fault injection techniques: Their countermeasures," in *Proc. Indo-Taiwan 2nd Int. Conf. Comput., Analytics Netw. (Indo-Taiwan ICAN)*, Rajpura, India, Feb. 2020, pp. 144–151, doi: 10.1109/Indo-TaiwanICAN48429.2020.9181324.

[17] A. Sengupta, R. Chaurasia, and A. Anshul, "Robust security of hardware accelerators using protein molecular biometric signature and facial biometric encryption key," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 31, no. 6, pp. 826–839, Jun. 2023, doi: 10.1109/TVLSI.2023.3265559.

[18] W.-K. Liu, B. Tan, J. M. Fung, R. Karri, and K. Chakrabarty, "Hardware-supported patching of security bugs in hardware IP blocks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 1, pp. 54–67, Jan. 2023, doi: 10.1109/TCAD.2022.3168513.

[19] 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*, vol. 10, pp. 102386–102395, 2022, doi: 10.1109/ACCESS.2022.3208650.

[20] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Physically unclonable function using GSHE driven SOT assisted p-MTJ for next generation hardware security applications," *IEEE Access*, vol. 10, pp. 93029–93038, 2022, doi: 10.1109/ACCESS.2022.3203817.

[21] T. Kroeger, W. Cheng, J.-L. Danger, S. Guilley, and N. Karimi, "Cross-PUF attacks: Targeting FPGA implementation of arbiter-PUFs," *J. Electron. Test.*, vol. 38, no. 3, pp. 261–277, Jun. 2022, doi: 10.1007/s10836-022-06012-z.

[22] M. Oh, S. Lee, Y. Kang, and D. Choi, "Implementation and characterization of flash-based hardware security primitives for cryptographic key generation," *ETRI J.*, vol. 45, no. 2, pp. 346–357, Apr. 2023, doi: 10.4218/etrij.2021-0455.

[23] S. Aftabjahani, M. Tehranipoor, F. Farahmandi, B. Ahmed, R. Kastner, F. Restuccia, A. Meza, K. Ryan, N. Fern, J. van Woudenberg, R. Velegalati, C.-B. Breunesse, C. Sturton, and C. Deutschbein, "Special session: CAD for hardware security—Promising directions for automation of security assurance," in *Proc. IEEE 41st VLSI Test Symp. (VTS)*, Farah, CA, USA, Apr. 2023, pp. 1–10, doi: 10.1109/VTS56346.2023.10140100.

[24] M. Bellare and B. Yee, "Forward integrity for secure audit logs," Dept. Comput. Sci. Eng., Univ. California, San Diego, CA, USA, Tech. Rep. CS98-580, 1997, vol. 184. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0

[25] G. Guardiola-Múzquiz and E. Soriano-Salvador, "SealFSv2: Combining storage-based and ratcheting for tamper-evident logging," *Int. J. Inf. Secur.*, vol. 22, no. 2, pp. 447–466, Apr. 2023, doi: 10.1007/s10207-022-00643-1.

[26] P. R. DaSilva and P. J. Fortier, "Hardware based detection, recovery, and tamper evident concept to protect from control flow violations in embedded processing," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Woburn, MA, USA, Nov. 2019, pp. 1–6, doi: 10.1109/HST47167.2019.9032955.

[27] R. K. L. Ko and M. A. Will, "Progger: An efficient, tamper-evident kernel-space logger for cloud data provenance tracking," in *Proc. IEEE 7th Int. Conf. Cloud Comput.*, Anchorage, AK, USA, Jun. 2014, pp. 881–889, doi: 10.1109/CLOUD.2014.121.

[28] N. Li, H. Zhang, Z. Chen, and J. Wei, "Fluorescence-structural color photonic crystal security card based on ultraviolet-responsive core-interlayer-shell colloidal particles," *J. Mater. Sci.*, vol. 57, no. 30, pp. 14310–14323, Aug. 2022, doi: 10.1007/s10853-022-07495-z.

[29] M. Yan, H. Wei, and M. Onabajo, "Modeling of thermal coupling and temperature sensor circuit design considerations for hardware trojan detection," in *Proc. IEEE 61st Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Windsor, ON, Canada, Aug. 2018, pp. 857–860, doi: 10.1109/MWSCAS.2018.8623865.

[30] H. Wei, M. Yan, and M. Onabajo, "Noise reduction via chopper stabilization of fully differential temperature sensors for hardware security applications," in *Proc. IEEE 14th Dallas Circuits Syst. Conf. (DCAS)*, Dallas, TX, USA, Nov. 2020, pp. 1–5, doi: 10.1109/DCAS51144.2020.9330638.

[31] F. Farha, H. Ning, H. Liu, L. T. Yang, and L. Chen, "Physical unclonable functions based secret keys scheme for securing big data infrastructure communication," *Inf. Sci.*, vol. 503, pp. 307–318, Nov. 2019, doi: 10.1016/j.ins.2019.06.066.

[32] M. H. Murtaza, H. Tahir, S. Tahir, Z. A. Alizai, Q. Riaz, and M. Hussain, "A portable hardware security module and cryptographic key generator," *J. Inf. Secur. Appl.*, vol. 70, Nov. 2022, Art. no. 103332, doi: 10.1016/j.jisa.2022.103332.

[33] Y. Xia, Z. Hua, Y. Yu, J. Gu, H. Chen, B. Zang, and H. Guan, "Colony: A privileged trusted execution environment with extensibility," *IEEE Trans. Comput.*, vol. 71, no. 2, pp. 479–492, Feb. 2022, doi: 10.1109/TC.2021.3055293.

[34] J. Han, I. Yun, S. Kim, T. Kim, S. Son, and D. Han, "Scalable and secure virtualization of HSM with ScaleTrust," *IEEE/ACM Trans. Netw.*, vol. 31, no. 4, pp. 1595–1610, Aug. 2023, doi: 10.1109/TNET.2022.3220427.

[35] S.-H. Cheng, M.-H. Lee, B.-C. Wu, and T.-T. Liu, "A lightweight power side-channel attack protection technique with minimized overheads using on-demand current equalizer," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 10, pp. 4008–4012, Oct. 2022, doi: 10.1109/TCSII.2022.3185608.

[36] K. S. Kumar, G. H. Rao, S. Sahoo, and K. K. Mahapatra, "Secure split test techniques to prevent IC piracy for IoT devices," *Integration*, vol. 58, pp. 390–400, Jun. 2017, doi: 10.1016/j.vlsi.2016.09.004.

[37] C. Reinbrecht, A. Susin, L. Bossuet, G. Sigl, and J. Sepúlveda, "Timing attack on NoC-based systems: Prime+probe attack and NoC-based protection," *Microprocess. Microsyst.*, vol. 52, pp. 556–565, Jul. 2017, doi: 10.1016/j.micpro.2016.12.010.

[38] M. D. Grammatikakis, P. Petrakis, A. Papagrigoriou, G. Kornaros, and M. Coppola, "High-level security services based on a hardware NoC firewall module," in *Proc. 12th Int. Workshop Intell. Solutions Embedded Syst. (WISES)*, Ancona, Italy, Oct. 2015, pp. 73–78.

[39] R. F. Faccenda, G. Comarú, L. L. Caimi, and F. G. Moraes, "SeMAP—A method to secure the communication in NoC-based many cores," *IEEE Des. Test. Comput.*, vol. 40, no. 5, pp. 42–51, Oct. 2023, doi: 10.1109/MDAT.2023.3277813.

[40] K.-J. Lee, Z.-Y. Lu, and S.-C. Yeh, "A secure JTAG wrapper for SoC testing and debugging," *IEEE Access*, vol. 10, pp. 37603–37612, 2022, doi: 10.1109/ACCESS.2022.3164712.

[41] K.-U. Müller, R. Ulrich, A. Stanitzki, and R. Kokozinski, "Enabling secure boot functionality by using physical unclonable functions," in *Proc. 14th Conf. Ph.D. Res. Microelectron. Electron. (PRIME)*, Prague, Czech Republic, Jul. 2018, pp. 81–84, doi: 10.1109/PRIME.2018.8430370.

[42] J. Zhu, Y. Zhao, Q. Huang, C. Chen, C. Wu, R. Jia, and R. Huang, "Design and simulation of a novel graded-channel heterojunction tunnel FET with high I_{ON}/I_{OFF} ratio and steep swing," *IEEE Electron Device Lett.*, vol. 38, no. 9, pp. 1200–1203, Sep. 2017, doi: 10.1109/LED.2017.2734679.

[43] J.-S. Liu, M. B. Clavel, and M. K. Hudait, "TBAL: Tunnel FET-based adiabatic logic for energy-efficient, ultra-low voltage IoT applications," *IEEE J. Electron Devices Soc.*, vol. 7, pp. 210–218, 2019, doi: 10.1109/JEDS.2019.2891204.

[44] A. Biswas and A. M. Ionescu, "1T capacitor-less DRAM cell based on asymmetric tunnel FET design," *IEEE J. Electron Devices Soc.*, vol. 3, no. 3, pp. 217–222, May 2015, doi: 10.1109/JEDS.2014.2382759.

[45] H. Madan, V. Saripalli, H. Liu, and S. Datta, "Asymmetric tunnel field-effect transistors as frequency multipliers," *IEEE Electron Device Lett.*, vol. 33, no. 11, pp. 1547–1549, Nov. 2012, doi: 10.1109/LED.2012.2214201.

[46] C. K. Pandey, D. Das, R. N. K. Kadava, T. Ashok, K. P. Anil, and R. G. Siva, "A review on emerging tunnel FET structures for high-speed and low-power circuit applications," in *Proc. IEEE Devices for Integr. Circuit (DevIC)*, Kalyani, India, Apr. 2023, pp. 163–167, doi: 10.1109/DevIC57758.2023.10134784.

[47] A. Japa, S. K. Sahoo, R. Vaddi, and M. K. Majumder, "Emerging tunnel FET and spintronics-based hardware-secure circuit design with ultra-low energy consumption," *J. Comput. Electron.*, vol. 22, no. 1, pp. 178–189, Nov. 2022, doi: 10.1007/s10825-022-01958-x.

[48] J. Luo, C. Chen, Q. Huang, and R. Huang, "A biomimetic tunnel FET-based spiking neuron for energy-efficient neuromorphic computing with reduced hardware cost," *IEEE Trans. Electron Devices*, vol. 69, no. 2, pp. 882–886, Feb. 2022, doi: 10.1109/TED.2021.3131633.

[49] I. M. Delgado-Lozano, E. Tena-Sánchez, J. Núñez, and A. J. Acosta, "Gate-level design methodology for side-channel resistant logic styles using TFETs," *IEEE Embedded Syst. Lett.*, vol. 14, no. 2, pp. 99–102, Jun. 2022, doi: 10.1109/LES.2021.3122395.

[50] C. Rajan, D. Sharma, and D. P. Samajdar, "Implementation of physical unclonable functions using hetero junction based GAA TFET," *Superlattices Microstructures*, vol. 126, pp. 72–82, Feb. 2019, doi: 10.1016/j.spmi.2018.12.010.

[51] A. Singh, S. Chaudhary, S. M. Sharma, and C. K. Sarkar, "Improved drive capability of silicon nano tube tunnel FET using halo implantation," *Silicon*, vol. 12, no. 11, pp. 2555–2561, Nov. 2020, doi: 10.1007/s12633-019-00350-y.

[52] J.-S. Yuan, J. Lin, Q. Alasad, and S. Taheri, "Ultra-low-power design and hardware security using emerging technologies for Internet of Things," *Electronics*, vol. 6, no. 3, p. 67, Sep. 2017, doi: 10.3390/electronics6030067.

[53] S. Taheri and J.-S. Yuan, "Mixed-signal hardware security: Attacks and countermeasures for $\Delta\Sigma$ ADC," *Electronics*, vol. 6, no. 3, p. 60, Aug. 2017, doi: 10.3390/electronics6030060.

[54] Y. Bi, K. Shamsi, J.-S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel FET current mode logic for DPA-resilient circuit designs," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 340–352, Jul. 2017, doi: 10.1109/TETC.2016.2559159.

[55] J. Zhang and G. Qu, "Recent attacks and defenses on FPGA-based systems," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 12, no. 3, pp. 1–24, Sep. 2019, doi: 10.1145/3340557.

[56] K. R. N. Karthik and C. K. Pandey, "A review of tunnel field-effect transistors for improved ON-state behaviour," *Silicon*, vol. 15, no. 1, pp. 1–23, Jan. 2023, doi: 10.1007/s12633-022-02028-4.

[57] A. Verma, B. Song, B. Downey, V. D. Wheeler, D. J. Meyer, H. G. Xing, and D. Jena, "Steep sub-Boltzmann switching in AlGaN/GaN phase-FETs with ALD VO2," *IEEE Trans. Electron Devices*, vol. 65, no. 3, pp. 945–949, Mar. 2018, doi: 10.1109/TED.2018.2795105.

[58] S. J. Bader, "GaN-on-AlN as a platform for high-voltage complementary electronics," Ph.D. thesis, Dept. Appl. Eng. Phys., Cornell Univ., Ithaca, NY, USA, 2020.

[59] A. Verma, B. Song, D. Meyer, B. Downey, V. Wheeler, H. G. Xing, and D. Jena, "Demonstration of GaN HyperFETs with ALD VO_2," in *Proc. 74th Annu. Device Res. Conf. (DRC)*, Newark, DE, USA, Jun. 2016, pp. 1–2, doi: 10.1109/DRC.2016.7548397.

[60] A. Aziz, N. Shukla, S. Datta, and S. K. Gupta, "Steep switching hybrid phase transition FETs (Hyper-FET) for low power applications: A device-circuit co-design perspective–Part I," *IEEE Trans. Electron Devices*, vol. 64, no. 3, pp. 1350–1357, Mar. 2017, doi: 10.1109/TED.2016.2642884.

[61] A. Aziz, N. Shukla, S. Datta, and S. K. Gupta, "Steep switching hybrid phase transition FETs (Hyper-FET) for low power applications: A device-circuit co-design perspective—Part II," *IEEE Trans. Electron Devices*, vol. 64, no. 3, pp. 1358–1365, Mar. 2017, doi: 10.1109/TED.2017.2650598.

[62] R. Sorot, A. Goel, and S. Rewari, "Phase transition material modulated hyper FET for digital applications," in *Proc. IEEE Devices Integr. Circuit (DevIC)*, Kalyani, India, Apr. 2023, pp. 261–265, doi: 10.1109/DevIC57758.2023.10134819.

[63] W.-Y. Tsai, X. Li, M. Jerry, B. Xie, N. Shukla, H. Liu, N. Chandramoorthy, M. Cotter, A. Raychowdhury, D. M. Chiarulli, S. P. Levitan, S. Datta, J. Sampson, N. Ranganathan, and V. Narayanan, "Enabling new computation paradigms with HyperFET—An emerging device," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 1, pp. 30–48, Jan. 2016, doi: 10.1109/TMSCS.2016.2519022.

[64] I. M. Delgado-Lozano, E. Tena-SÁnchez, J. Núñez, and A. J. Acosta, "Design and analysis of secure emerging crypto-hardware using HyperFET devices," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 2, pp. 787–796, Apr. 2021, doi: 10.1109/TETC.2020.2977735.

[65] M. Jiménez, J. Núnez, and M. J. Avedillo, "An approach to the device-circuit co-design of HyperFET circuits," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Seville, Spain, Oct. 2020, pp. 1–5, doi: 10.1109/ISCAS45731.2020.9180660.

[66] S. V. V. Satyanarayana, S. R. Shailendra, V. N. Ramakrishnan, and S. Sriadibhatla, "Dual-chirality GAA-CNTFET-based SCPF-TCAM cell design for low power and high performance," *J. Comput. Electron.*, vol. 18, no. 3, pp. 1045–1054, Sep. 2019, doi: 10.1007/s10825-019-01362-y.

[67] H. Mahmoodian and M. Dolatshahi, "An energy-efficient sample-and-hold circuit in CNTFET technology for high-speed applications," *Anal. Integr. Circuits Signal Process.*, vol. 103, no. 1, pp. 209–221, Apr. 2020, doi: 10.1007/s10470-020-01607-y.

[68] C. Qiu, Z. Zhang, and L.-M. Peng, "Scaling carbon nanotube CMOS FETs towards quantum limit," in *IEDM Tech. Dig.*, Dec. 2017, pp. 5.5.1–5.5.4, doi: 10.1109/IEDM.2017.8268334.

[69] S. Banerjee, A. Chaudhuri, and K. Chakrabarty, "Analysis of the impact of process variations and manufacturing defects on the performance of carbon-nanotube FETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1513–1526, Jun. 2020, doi: 10.1109/TVLSI.2020.2976734.

[70] M. Moradi, S. Tao, and R. F. Mirzaee, "Physical unclonable functions based on carbon nanotube FETs," in *Proc. IEEE 47th Int. Symp. Multiple-Valued Log. (ISMVL)*, Novi Sad, Serbia, May 2017, pp. 124–129, doi: 10.1109/ISMVL.2017.33.

[71] L. Liu, H. Huang, and S. Hu, "Lorenz chaotic system-based carbon nanotube physical unclonable functions," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 7, pp. 1408–1421, Jul. 2018, doi: 10.1109/TCAD.2017.2762919.

[72] A. Amirany, K. Jafari, and M. H. Moaiyeri, "True random number generator for reliable hardware security modules based on a neuromorphic variation-tolerant spintronic structure," *IEEE Trans. Nanotechnol.*, vol. 19, pp. 784–791, 2020, doi: 10.1109/TNANO.2020.3034818.

[73] S. Musala, R. M. Gajula, S. V. R. S. Reddy, and P. P. Reddy, "High-speed low power energy efficient 1-trit multiplier with less number of CNTFETs," *Multimedia Tools Appl.*, vol. 83, no. 8, pp. 23297–23309, Aug. 2023, doi: 10.1007/s11042-023-16403-9.

[74] C. K. H. Suresh, B. Mazumdar, S. S. Ali, and O. Sinanoglu, "Power-side-channel analysis of carbon nanotube FET based design," in *Proc. IEEE 22nd Int. Symp. On-Line Test. Robust Syst. Design (IOLTS)*, Sant Feliu de Guixols, Spain, Jul. 2016, pp. 215–218, doi: 10.1109/IOLTS.2016.7604705.

[75] H. Zhang, L. Liu, D. Wang, H. Lin, X. Zhao, and C. Xie, "Ultralow-power and high-speed in-memory computing unit based on field-accelerated spin-orbit torque MRAM utilizing voltage-controlled magnetic anisotropy," *IEEE Trans. Electron Devices*, pp. 1–7, Aug. 2023, doi: 10.1109/TED.2023.3288496.

[76] I. Bendjeddou, M. J. Garcia, A. S. E. Valli, A. Litvinenko, V. Cros, U. Ebels, A. Jenkins, R. Ferreira, R. Dutra, D. Morche, E. Pistono, S. Bourdel, Y. L. Guennec, and F. Podevin, "Electrical modeling of spin-torque diodes used as radio frequency detectors: A step-by-step methodology for parameter extraction," *IEEE Trans. Microw. Theory Techn.*, vol. 71, no. 7, pp. 2771–2781, Jul. 2023, doi: 10.1109/TMTT.2023.3259528.

[77] J. Qin, B. Sun, G. Zhou, T. Guo, Y. Chen, C. Ke, S. Mao, X. Chen, J. Shao, and Y. Zhao, "From spintronic memristors to quantum computing," *ACS Mater. Lett.*, vol. 5, no. 8, pp. 2197–2215, Aug. 2023, doi: 10.1021/acsmaterialslett.3c00088.

[78] A. Sharma and A. A. Tulapurkar, "Preparation of spin eigenstates including the Dicke states with generalized all-coupled interaction in a spintronic quantum computing architecture," *Quantum Inf. Process.*, vol. 20, no. 5, p. 172, May 2021, doi: 10.1007/s11128-021-03063-7.

[79] Z. Wang, W. Zhao, E. Deng, J.-O. Klein, and C. Chappert, "Perpendicular-anisotropy magnetic tunnel junction switched by spin-Hall-assisted spin-transfer torque," *J. Phys. D, Appl. Phys.*, vol. 48, no. 6, Feb. 2015, Art. no. 065001, doi: 10.1088/0022-3727/48/6/065001.

[80] Y. Zhang, W. Zhao, Y. Lakys, J.-O. Klein, J.-V. Kim, D. Ravelosona, and C. Chappert, "Compact modeling of perpendicular-anisotropy CoFeB/MgO magnetic tunnel junctions," *IEEE Trans. Electron Devices*, vol. 59, no. 3, pp. 819–826, Mar. 2012, doi: 10.1109/TED.2011.2178416.

[81] Y. Wang, Y. Zhang, E. Y. Deng, J. O. Klein, L. A. B. Naviner, and W. S. Zhao, "Compact model of magnetic tunnel junction with stochastic spin transfer torque switching for reliability analyses," *Microelectron. Rel.*, vol. 54, nos. 9–10, pp. 1774–1778, Sep. 2014, doi: 10.1016/j.microrel.2014.07.019.

[82] S. Mehri, A. Amirany, M. H. Moaiyeri, and K. Jafari, "Theoretical circuit design of an efficient spintronic random number generator with an internal postprocessing unit," *IEEE Magn. Lett.*, vol. 13, pp. 1–5, 2022, doi: 10.1109/LMAG.2022.3200326.

[83] K. Zhang, D. Zhang, C. Wang, L. Zeng, Y. Wang, and W. Zhao, "Compact modeling and analysis of voltage-gated spin-orbit torque magnetic tunnel junction," *IEEE Access*, vol. 8, pp. 50792–50800, 2020, doi: 10.1109/ACCESS.2020.2980073.

[84] X. Xing, S. Huang, Y. Gong, J. Wang, Z. Lv, Y. Zhou, X. Zhao, J. Hao, and S.-T. Han, "Stochastic current response in diffusive memristor for security applications," *Mater. Today Nano*, vol. 22, Jun. 2023, Art. no. 100315, doi: 10.1016/j.mtnano.2023.100315.

[85] M. Riahi Alam, M. H. Najafi, N. Taherinejad, M. Imani, and R. Gottumukkala, "Stochastic computing in beyond von-neumann era: Processing bit-streams in memristive memory," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 5, pp. 2423–2427, May 2022, doi: 10.1109/TCSII.2022.3161995.

[86] C. Wang, B. Chen, J. Mei, L. Tai, Y. Qi, Y. Gao, J. Wu, X. Zhan, and J. Chen, "Complementary digital and analog resistive switching based on AlO_x monolayer memristors for mixed-precision neuromorphic computing," *IEEE Trans. Electron Devices*, vol. 70, no. 8, pp. 4488–4492, Aug. 2023, doi: 10.1109/TED.2023.3280146.

[87] S. Zeitouni, E. Stapf, H. Fereidooni, and A.-R. Sadeghi, "On the security of strong memristor-based physically unclonable functions," in *Proc. 57th ACM/IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jul. 2020, pp. 1–6, doi: 10.1109/DAC18072.2020.9218491.

[88] J. Sun, Z. Wang, S. Wang, M. Yang, H. Gao, H. Wang, X. Ma, and Y. Hao, "Physical unclonable functions based on transient form of memristors for emergency defenses," *IEEE Electron Device Lett.*, vol. 43, no. 3, pp. 378–381, Mar. 2022, doi: 10.1109/LED.2022.3145487.

[89] C. Yang, B. Liu, H. Li, Y. Chen, M. Barnell, Q. Wu, W. Wen, and J. Rajendran, "Thwarting replication attack against memristor-based neuromorphic computing system," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2192–2205, Oct. 2020, doi: 10.1109/TCAD.2019.2937817.

[90] A. K. Rajput, A. K. Tiwari, and M. Pattanaik, "An energy-efficient hybrid SRAM-based in-memory computing macro for artificial intelligence edge devices," *Circuits, Syst., Signal Process.*, vol. 42, no. 6, pp. 3589–3616, Jun. 2023, doi: 10.1007/s00034-022-02284-0.

[91] P. Qiu, Y. Qin, and Q. Xia, "Ultrasensitive gas sensor developed from SnS/TiO_2-based memristor for dilute methanol detection at room temperature," *Sens. Actuators B, Chem.*, vol. 392, Oct. 2023, Art. no. 134038, doi: 10.1016/j.snb.2023.134038.

[92] S. Deshpande, S. Sopariwala, R. Singhvi, R. Khandelwal, J. Marvaniya, and R. Parekh, "Performance analysis of silicon nanowire FET for GAA and pi gate configurations," in *Proc. IEEE Int. Conf. Nanoelectronics, Nanophotonics, Nanomaterials, Nanobiosci. Nanotechnol. (5NANO)*, Kottayam, India, Apr. 2022, pp. 1–6, doi: 10.1109/5NANO53044.2022.9828888.

[93] Y. Bi, K. Shamsi, J.-S. Yuan, P.-E. Gaillardon, G. D. Micheli, X. Yin, X. S. Hu, M. Niemier, and Y. Jin, "Emerging technology-based design of primitives for hardware security," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–19, Jan. 2017, doi: 10.1145/2816818.

[94] Y. Bi, P.-E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security—Case study on silicon nanowire FETs and graphene SymFETs," in *Proc. IEEE 23rd Asian Test Symp.*, Hangzhou, China, Nov. 2014, pp. 342–347, doi: 10.1109/ATS.2014.69.

[95] S. Rai, S. Patnaik, A. Rupani, J. Knechtel, O. Sinanoglu, and A. Kumar, "Security promises and vulnerabilities in emerging reconfigurable nanotechnology-based circuits," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 763–778, Apr. 2022, doi: 10.1109/TETC.2020.3039375.

[96] Y. Liu, J. He, H. Ma, T. Qu, and Z. Dai, "A comprehensive evaluation of integrated circuits side-channel resilience utilizing three-independent-gate silicon nanowire field effect transistors-based current mode logic," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 10, pp. 3228–3238, Oct. 2022, doi: 10.1109/TCAD.2021.3128364.

[97] A. A. Leonardi, M. J. Lo Faro, C. Di Franco, G. Palazzo, C. D'Andrea, D. Morganti, K. Manoli, P. Musumeci, B. Fazio, M. Lanza, L. Torsi, F. Priolo, and A. Irrera, "Silicon nanowire luminescent sensor for cardiovascular risk in saliva," *J. Mater. Sci., Mater. Electron.*, vol. 31, no. 1, pp. 10–17, Jan. 2020, doi: 10.1007/s10854-018-0417-y.

[98] M. Simon, A. Heinzig, J. Trommer, T. Baldauf, T. Mikolajick, and W. M. Weber, "Top–down technology for reconfigurable nanowire FETs with symmetric on-currents," *IEEE Trans. Nanotechnol.*, vol. 16, no. 5, pp. 812–819, Sep. 2017, doi: 10.1109/TNANO.2017.2694969.

[99] M. S. Narula and A. Pandey, "Dual-gate silicon nanowire FET with a corner spacer for high-performance and high-frequency applications," *J. Electron. Mater.*, vol. 52, no. 10, pp. 6708–6718, Oct. 2023, doi: 10.1007/s11664-023-10597-2.

[100] V. B. Sreenivasulu and V. Narendar, "Circuit analysis and optimization of GAA nanowire FET towards low power and high switching," *Silicon*, vol. 14, no. 16, pp. 10401–10411, Nov. 2022, doi: 10.1007/s12633-022-01777-6.

[101] C. Paolino, A. Antolini, F. Pareschi, M. Mangia, R. Rovatti, E. F. Scarselli, G. Setti, R. Canegallo, M. Carissimi, and M. Pasotti, "Phase-change memory in neural network layers with measurements-based device models," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Austin, TX, USA, May 2022, pp. 1536–1540, doi: 10.1109/ISCAS48785.2022.9937856.

[102] V. Joshi, M. Le Gallo, S. Haefeli, I. Boybat, S. R. Nandakumar, C. Piveteau, M. Dazzi, B. Rajendran, A. Sebastian, and E. Eleftheriou, "Accurate deep neural network inference using computational phase-change memory," *Nature Commun.*, vol. 11, no. 1, p. 2473, May 2020, doi: 10.1038/s41467-020-16108-9.

[103] M. Kumar and M. Suri, "Hybrid CMOS-PCM ternary logic for digital circuit applications," *IEEE Trans. Nanotechnol.*, vol. 22, pp. 228–237, 2023, doi: 10.1109/TNANO.2023.3272831.

[104] M. Boniardi, D. Ielmini, S. Lavizzari, A. L. Lacaita, A. Redaelli, and A. Pirovano, "Statistics of resistance drift due to structural relaxation in phase-change memory arrays," *IEEE Trans. Electron Devices*, vol. 57, no. 10, pp. 2690–2696, Oct. 2010, doi: 10.1109/TED.2010.2058771.

[105] N. Noor, S. Muneer, R. S. Khan, A. Gokirmak, and H. Silva, "Enhanced reset variability in phase change memory for hardware security applications," in *Proc. APS March Meeting Abstracts*, 2019, Paper no. K33-008. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0

[106] N. Noor, "Exploiting phase change memory nano-device properties for hardware security applications," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Connecticut, Storrs, 2019.

[107] N. Noor and H. Silva, "Phase change memory for physical unclonable functions," in *Applications of Emerging Memory Technology: Beyond Storage* (Springer Series in Advanced Microelectronics), vol 63. Singapore: Springer, 2020, pp. 59–91. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-8379-3_3

[108] R. Sayeed Khan, N. Noor, C. Jin, J. Scoggin, Z. Woods, S. Muneer, A. Ciardullo, P. Ha Nguyen, A. Gokirmak, M. van Dijk, and H. Silva, "Phase change memory and its applications in hardware security," in *Security Opportunities in Nano Devices and Emerging Technologies*. Boca Raton, FL, USA: CRC Press, 2017, pp. 93–114.

[109] N. Noor, S. Muneer, R. S. Khan, A. Gorbenko, L. Adnane, M. T. B. Kashem, J. Scoggin, F. Dirisaglik, A. Cywar, A. Gokirmak, and H. Silva, "Reset variability in phase change memory for hardware security applications," *IEEE Trans. Nanotechnol.*, vol. 20, pp. 75–82, 2021, doi: 10.1109/TNANO.2020.3041400.

[110] N. Noor, S. Muneer, L. Adnane, R. S. Khan, A. Gorbenko, F. Dirisaglik, C. A. C. Lam, Y. Zhu, A. Gokirmak, and H. Silva, "Utilizing programming variability in phase change memory cells for security," in *Proc. Materials Res. Soc. (MRS) Fall Meeting Exhib.*, Boston, MA, USA, Nov. 2017, Paper no. EM07.04.04. [Online]. Available: https://www.mrs.org/fall2017-symposiumsessions?Code=EM07

[111] D. C. Brock, *Understanding Moore's Law: Four Decades of Innovation*. Philadelphia, PA, USA: Chemical Heritage Foundation, 2006. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0

[112] R. H. Dennard, F. H. Gaensslen, H.-N. Yu, V. L. Rideout, E. Bassous, and A. R. LeBlanc, "Design of ion-implanted MOSFET's with very small physical dimensions," *IEEE J. Solid-State Circuits*, vol. SSC-9, no. 5, pp. 256–268, Oct. 1974, doi: 10.1109/JSSC.1974.1050511.

[113] W. Young Choi, J. Young Song, J. Duk Lee, Y. June Park, and B.-G. Park, "100-nm n-/p-channel I-MOS using a novel self-aligned structure," *IEEE Electron Device Lett.*, vol. 26, no. 4, pp. 261–263, Apr. 2005, doi: 10.1109/LED.2005.844695.

[114] S. Ramaswamy and M. J. Kumar, "Junctionless impact ionization MOS: Proposal and investigation," *IEEE Trans. Electron Devices*, vol. 61, no. 12, pp. 4295–4298, Dec. 2014, doi: 10.1109/TED.2014.2361343.

[115] A. M. Ionescu and H. Riel, "Tunnel field-effect transistors as energy-efficient electronic switches," *Nature*, vol. 479, no. 7373, pp. 329–337, Nov. 2011, doi: 10.1038/nature10679.

[116] H. Kam, D. T. Lee, R. T. Howe, and T.-J. King, "A new nano-electro-mechanical field effect transistor (NEMFET) design for low-power electronics," in *Proc. IEEE Int. Electron. Devices Meeting (IEDM)*, Dec. 2005, pp. 463–466, doi: 10.1109/IEDM.2005.1609380.

[117] A. I. Khan, C. W. Yeung, C. Hu, and S. Salahuddin, "Ferroelectric negative capacitance MOSFET: Capacitance tuning & antiferroelectric operation," in *IEDM Tech. Dig.*, Washington, DC, USA, Dec. 2011, pp. 11.3.1–11.3.4, doi: 10.1109/IEDM.2011.6131532.

[118] H. Ota, S. Migita, J. Hattori, K. Fukuda, and A. Toriumi, "Material and device engineering in fully depleted silicon-on-insulator transistors to realize a steep subthreshold swing using negative capacitance," *Jpn. J. Appl. Phys.*, vol. 55, no. 8S2, Aug. 2016, Art. no. 08PD01, doi: 10.7567/jjap.55.08pd01.

[119] H. Ota, S. Migita, J. Hattori, K. Fukuda, and A. Toriumi, "Design and simulation of steep-slope silicon-on-insulator FETs using negative capacitance: Impact of buried oxide thickness and remnant polarization," in *Proc. IEEE 16th Int. Conf. Nanotechnol. (IEEE-NANO)*, Sendai, Japan, Aug. 2016, pp. 770–772, doi: 10.1109/NANO.2016.7751500.

[120] S. Saikin, M. Shen, and M.-C. Cheng, "Study of spin-polarized transport properties for spin-FET design optimization," *IEEE Trans. Nanotechnol.*, vol. 3, no. 1, pp. 173–179, Mar. 2004, doi: 10.1109/TNANO.2004.824021.

[121] L. G. D. Ginzburg-Devonshire's, "Novel SPINFET: By simultaneous utilization of Rashba effect, Zeeman effect & negative capacitance," in *Proc. Int. Semicond. Dev. Res. Symp.*, 2016, pp. 1–11.

[122] F. Liu, Y. Zhou, Y. Wang, X. Liu, J. Wang, and H. Guo, "Negative capacitance transistors with monolayer black phosphorus," *npj Quantum Mater.*, vol. 1, no. 1, pp. 1–6, Jul. 2016, doi: 10.1038/npjquantmats.2016.4.

[123] F. A. McGuire, Z. Cheng, K. Price, and A. D. Franklin, "Sub-60 mV/decade switching in 2D negative capacitance field-effect transistors with integrated ferroelectric polymer," *Appl. Phys. Lett.*, vol. 109, no. 9, pp. 3101–3105, Aug. 2016, doi: 10.1063/1.4961108.

[124] F. A. McGuire, Y.-C. Lin, K. Price, G. B. Rayner, S. Khandelwal, S. Salahuddin, and A. D. Franklin, "Sustained sub-60 mV/decade switching via the negative capacitance effect in MoS_2 transistors," *Nano Lett.*, vol. 17, no. 8, pp. 4801–4806, Aug. 2017, doi: 10.1021/acs.nanolett.7b01584.

[125] M. Si, C.-J. Su, C. Jiang, N. J. Conrad, H. Zhou, K. D. Maize, G. Qiu, C.-T. Wu, A. Shakouri, M. A. Alam, and P. D. Ye, "Steep-slope hysteresis-free negative capacitance MoS_2 transistors," *Nature Nanotechnol.*, vol. 13, no. 1, pp. 24–28, Jan. 2018, doi: 10.1038/s41565-017-0010-1.

[126] W.-X. You and P. Su, "Design space exploration considering back-gate biasing effects for 2D negative-capacitance field-effect transistors," *IEEE Trans. Electron Devices*, vol. 64, no. 8, pp. 3476–3481, Aug. 2017, doi: 10.1109/TED.2017.2714687.

[127] X. Wang, Y. Chen, G. Wu, D. Li, L. Tu, S. Sun, H. Shen, T. Lin, Y. Xiao, M. Tang, W. Hu, L. Liao, P. Zhou, J. Sun, X. Meng, J. Chu, and J. Wang, "Two-dimensional negative capacitance transistor with polyvinylidene fluoride-based ferroelectric polymer gating," *NPJ 2D Mater. Appl.*, vol. 1, no. 2017, pp. 1–7, 2017, doi: 10.1038/s41699-017-0040-4.

[128] C. W. Yeung, A. I. Khan, A. Sarker, S. Salahuddin, and C. Hu, "Low power negative capacitance FETs for future quantum-well body technology," in *Proc. Int. Symp. VLSI Technol., Syst. Appl. (VLSI-TSA)*, Hsinchu, Taiwan, Apr. 2013, pp. 1–2, doi: 10.1109/VLSI-TSA.2013.6545648.

[129] M. H. Lee, Y.-T. Wei, K.-Y. Chu, J.-J. Huang, C.-W. Chen, C.-C. Cheng, M.-J. Chen, H.-Y. Lee, Y.-S. Chen, L.-H. Lee, and M.-J. Tsai, "Steep slope and near non-hysteresis of FETs with antiferroelectric-like HfZrO for low-power electronics," *IEEE Electron Device Lett.*, vol. 36, no. 4, pp. 294–296, Apr. 2015, doi: 10.1109/LED.2015.2402517.

[130] K. Karda, A. Jain, C. Mouli, and M. A. Alam, "An anti-ferroelectric gated Landau transistor to achieve sub-60 mV/dec switching at low voltage and high speed," *Appl. Phys. Lett.*, vol. 106, no. 16, pp. 3501-3505, Apr. 2015, doi: 10.1063/1.4918649.

[131] T. Srimani, G. Hills, M. D. Bishop, U. Radhakrishna, A. Zubair, R. S. Park, Y. Stein, T. Palacios, D. Antoniadis, and M. M. Shulaker, "Negative capacitance carbon nanotube FETs," *IEEE Electron Device Lett.*, vol. 39, no. 2, pp. 304–307, Feb. 2018, doi: 10.1109/LED.2017.2781901.

[132] K. Jang, T. Saraya, M. Kobayashi, and T. Hiramoto, "I_{on}/I_{off} ratio enhancement and scalability of gate-all-around nanowire negative-capacitance FET with ferroelectric HfO_2," *Solid-State Electron.*, vol. 136, pp. 60–67, Oct. 2017, doi: 10.1016/j.sse.2017.06.011.

[133] W. C. Goh, K. Yao, and C. K. Ong, "Pseudo-epitaxial lead zirconate titanate thin film on silicon substrate with enhanced ferroelectric polarization," *Appl. Phys. Lett.*, vol. 87, no. 7, Aug. 2005, Art. no. 072906, doi: 10.1063/1.2010606.

[134] M. H. Park, Y. H. Lee, H. J. Kim, Y. J. Kim, T. Moon, K. D. Kim, J. Müller, A. Kersch, U. Schroeder, T. Mikolajick, and C. S. Hwang, "Ferroelectricity and antiferroelectricity of doped thin HfO_2-based films," *Adv. Mater.*, vol. 27, no. 11, pp. 1811–1831, Mar. 2015, doi: 10.1002/adma.201404531.

[135] A. V. Bune, V. M. Fridkin, S. Ducharme, L. M. Blinov, S. P. Palto, A. V. Sorokin, S. G. Yudin, and A. Zlatkin, "Two-dimensional ferroelectric films," *Nature*, vol. 391, no. 6670, pp. 874–877, Feb. 1998, doi: 10.1038/36069.

[136] J. Talukdar, G. Rawat, and K. Mummaneni, "A novel extended source TFET with δp^+-SiGe layer," *Silicon*, vol. 12, no. 10, pp. 2273–2281, Oct. 2020, doi: 10.1007/s12633-019-00321-3.

[137] M. Malvika, B. Choudhuri, and K. Mummaneni, "A new pocket-doped NCFET for low power applications: Impact of ferroelectric and oxide thickness on its performance," *Micro Nanostruct.*, vol. 169, Sep. 2022, Art. no. 207360, doi: 10.1016/j.micrna.2022.207360.

[138] M. Malvika, J. Talukdar, V. Kumar, B. Choudhuri, and K. Mummaneni, "Comparative analysis of noise behavior of highly doped double pocket double-gate and single-gate negative capacitance FET," *J. Electron. Mater.*, vol. 52, no. 9, pp. 6203–6215, Sep. 2023, doi: 10.1007/s11664-023-10558-9.

[139] W.-X. You, P. Su, and C. Hu, "Evaluation of NC-FinFET based subsystem-level logic circuits," *IEEE Trans. Electron Devices*, vol. 66, no. 4, pp. 2004–2009, Apr. 2019, doi: 10.1109/TED.2019.2898445.

[140] X. Li, J. Sampson, A. Khan, K. Ma, S. George, A. Aziz, S. K. Gupta, S. Salahuddin, M.-F. Chang, S. Datta, and V. Narayanan, "Enabling energy-efficient nonvolatile computing with negative capacitance FET," *IEEE Trans. Electron Devices*, vol. 64, no. 8, pp. 3452–3458, Aug. 2017, doi: 10.1109/TED.2017.2716338.

[141] C.-H. Lee, Y.-T. Hsu, T.-T. Liu, and T.-D. Chiueh, "Design of an 45 nm NCFET based compute-in-SRAM for energy-efficient machine learning applications," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst. (APCCAS)*, Ha Long, Vietnam, Dec. 2020, pp. 193–196, doi: 10.1109/APCCAS50809.2020.9301709.

[142] W. Huang, H. Zhu, Y. Zhang, Z. Wu, Q. Huo, Z. Xiao, and K. Jia, "Ternary logic circuit based on negative capacitance field-effect transistors and its variation immunity," *IEEE Trans. Electron Devices*, vol. 68, no. 7, pp. 3678–3683, Jul. 2021, doi: 10.1109/TED.2021.3081523.

[143] K. Han, C. Sun, E. Y. J. Kong, Y. Wu, C.-H. Heng, and X. Gong, "Hybrid design using metal–oxide–semiconductor field-effect transistors and negative-capacitance field-effect transistors for analog circuit applications," *IEEE Trans. Electron Devices*, vol. 68, no. 2, pp. 846–852, Feb. 2021, doi: 10.1109/TED.2020.3043207.

[144] Y. Liang, Z. Zhu, X. Li, S. K. Gupta, S. Datta, and V. Narayanan, "Utilization of negative-capacitance FETs to boost analog circuit performances," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2855–2860, Dec. 2019, doi: 10.1109/TVLSI.2019.2932268.

[145] V. Birudu, S. S. Yellampalli, and R. Vaddi, "A negative capacitance FET based energy efficient 6T SRAM computing-in-memory (CiM) cell design for deep neural networks," *Microelectron. J.*, vol. 139, Sep. 2023, Art. no. 105867, doi: 10.1016/j.mejo.2023.105867.

[146] R. C. Bheemana, A. Japa, S. S. Yellampalli, and R. Vaddi, "Negative capacitance FETs for energy efficient and hardware secure logic designs," *Microelectron. J.*, vol. 119, Jan. 2022, Art. no. 105320, doi: 10.1016/j.mejo.2021.105320.

[147] R. C. Bheemana, A. Japa, S. S. Yellampalli, and R. Vaddi, "Negative capacitance FET based energy efficient and DPA attack resilient ultra-light weight block cipher design," *Microelectron. J.*, vol. 133, Mar. 2023, Art. no. 105711, doi: 10.1016/j.mejo.2023.105711.

[148] L. Ni, P. Wang, Y. Zhang, H. Zhang, X. Li, L. Ni, J. Lv, and W. Zheng, "Profiling side-channel attacks based on CNN model fusion," *Microelectron. J.*, vol. 139, Sep. 2023, Art. no. 105901, doi: 10.1016/j.mejo.2023.105901.

[149] B. Venu, T. Kadiyam, K. Penumalli, S. Yellampalli, and R. Vaddi, "Negative capacitance FET based dual-split control 6T-SRAM cell design for energy efficient and robust computing-in memory architectures," *Microelectronic Eng.*, vol. 288, May 2024, Art. no. 112165, doi: 10.1016/j.mee.2024.112165.

[150] U. Zia, M. McCartney, B. Scotney, J. Martinez, and A. Sajjad, "A resource efficient pseudo random number generator based on sawtooth maps for Internet of Things," *Secur. Privacy*, vol. 6, no. 5, p. e304, Sep. 2023, doi: 10.1002/spy2.304.

[151] M. Dichtl, "How to predict the output of a hardware random number generator," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Cologne, Germany. Berlin, Germany: Springer, Sep. 2003, pp. 181–188, doi: 10.1007/978-3-540-45238-6_15.

[152] L. F. Rojas-Muñoz, S. Sánchez-Solano, M. C. Martínez-Rodríguez, and P. Brox, "True random number generation capability of a ring oscillator PUF for reconfigurable devices," *Electronics*, vol. 11, no. 23, p. 4028, Dec. 2022, doi: 10.3390/electronics11234028.

[153] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H.-J. Yoo, "A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC," *IEEE J. Solid-State Circuits*, vol. 52, no. 7, pp. 1953–1965, Jul. 2017, doi: 10.1109/JSSC.2017.2694833.

[154] A. Jayaraj, N. Nitin Gujarathi, I. Venkatesh, and A. Sanyal, "0.6–1.2 V, 0.22 pJ/bit true random number generator based on SAR ADC," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 10, pp. 1765–1769, Oct. 2020, doi: 10.1109/TCSII.2019.2949775.

[155] R. Zhang, X. Wang, K. Liu, and H. Shinohara, "A 0.186-pJ per bit latch-based true random number generator featuring mismatch compensation and random noise enhancement," *IEEE J. Solid-State Circuits*, vol. 57, no. 8, pp. 2498–2508, Aug. 2022, doi: 10.1109/JSSC.2021.3137312.

[156] Y. Cao, X. Zhao, W. Zheng, Y. Zheng, and C.-H. Chang, "A new energy-efficient and high throughput two-phase multi-bit per cycle ring oscillator-based true random number generator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 1, pp. 272–283, Jan. 2022, doi: 10.1109/TCSI.2021.3087512.

[157] S. Taneja, V. K. Rajanna, and M. Alioto, "In-memory unified TRNG and multi-bit PUF for ubiquitous hardware security," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 153–166, Jan. 2022, doi: 10.1109/JSSC.2021.3125255.

[158] R. Serrano, C. Duran, M. Sarmiento, and C.-K. Pham, "A unified NVRAM and TRNG in standard CMOS technology," *IEEE Access*, vol. 10, pp. 79213–79221, 2022, doi: 10.1109/ACCESS.2022.3193639.

[159] Y. Luo, J. Zhang, J. Hao, and X. Zhao, "A 2.5 pJ/bit PVT-tolerant true random number generator based on native-NMOS-regulated ring oscillator," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 70, no. 10, pp. 3927–3931, Oct. 2023, doi: 10.1109/TCSII.2023.3288036.

[160] S. Larimian, M. R. Mahmoodi, and D. B. Strukov, "Lightweight integrated design of PUF and TRNG security primitives based on eFlash memory in 55-nm CMOS," *IEEE Trans. Electron Devices*, vol. 67, no. 4, pp. 1586–1592, Apr. 2020, doi: 10.1109/TED.2020.2976632.

[161] X. Li, Y. Wang, Y. Yang, S. Lv, Q. Luo, X. Wang, X. Xu, D. Lei, and F. Zhang, "A 144-fJ/bit reliable and compact TRNG based on the diffusive resistance of 3-D resistive random access memory," *IEEE Trans. Electron Devices*, vol. 70, no. 8, pp. 4139–4144, Aug. 2023, doi: 10.1109/TED.2023.3288839.

[162] M. Akbari, S. Mirzakuchaki, D. Arumí, S. Manich, A. Gómez-Pau, F. Campabadal, M. B. González, and R. Rodríguez-Montañés, "True random number generator based on the variability of the high resistance state of RRAMs," *IEEE Access*, vol. 11, pp. 66682–66693, 2023, doi: 10.1109/ACCESS.2023.3290896.

[163] S. Fu, T. Li, C. Zhang, H. Li, S. Ma, J. Zhang, R. Zhang, and L. Wu, "RHS-TRNG: A resilient high-speed true random number generator based on STT-MTJ device," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 31, no. 10, pp. 1578–1591, Oct. 2023, doi: 10.1109/TVLSI.2023.3298327.

[164] B. Perach and S. Kvatinsky, "An asynchronous and low-power true random number generator using STT-MTJ," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 11, pp. 2473–2484, Nov. 2019, doi: 10.1109/TVLSI.2019.2927816.

[165] S. Taneja and M. Alioto, "Fully synthesizable all-digital unified dynamic entropy generation, extraction, and utilization within the same cryptographic core," *IEEE Solid-State Circuits Lett.*, vol. 3, pp. 402–405, 2020, doi: 10.1109/LSSC.2020.3025191.

[166] S. K. Satpathy, S. K. Mathew, R. Kumar, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, R. K. Krishnamurthy, and V. De, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical von Neumann extraction in 14-nm tri-gate CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, Apr. 2019, doi: 10.1109/JSSC.2018.2886350.

[167] V. R. Pamula, X. Sun, S. M. Kim, F. U. Rahman, B. Zhang, and V. S. Sathe, "A 65-nm CMOS 3.2-to-86 Mb/s 2.58 pJ/bit highly digital true-random-number generator with integrated de-correlation and bias correction," *IEEE Solid-State Circuits Lett.*, vol. 1, no. 12, pp. 237–240, Dec. 2018, doi: 10.1109/LSSC.2019.2896777.

[168] N. Onizawa, S. Mukaida, A. Tamakoshi, H. Yamagata, H. Fujita, and T. Hanyu, "High-throughput/low-energy MTJ-based true random number generator using a multi-voltage/current converter," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 10, pp. 2171–2181, Oct. 2020, doi: 10.1109/TVLSI.2020.3005413.

[169] Y. Qu, B. F. Cockburn, Z. Huang, H. Cai, Y. Zhang, W. Zhao, and J. Han, "Variation-resilient true random number generators based on multiple STT-MTJs," *IEEE Trans. Nanotechnol.*, vol. 17, no. 6, pp. 1270–1281, Nov. 2018, doi: 10.1109/TNANO.2018.2873970.

[170] A. Japa, M. K. Majumder, S. K. Sahoo, and R. Vaddi, "Tunnel FET ambipolarity-based energy efficient and robust true random number generator against reverse engineering attacks," *IET Circuits, Devices Syst.*, vol. 13, no. 5, pp. 689–695, Aug. 2019, doi: 10.1049/iet-cds.2018.5297.

[171] R. Govindaraj, S. Ghosh, and S. Katkoori, "CSRO-based reconfigurable true random number generator using RRAM," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2661–2670, Dec. 2018, doi: 10.1109/TVLSI.2018.2823274.

[172] M. S. Equbal, T. Ketkar, and S. Sahay, "Hybrid CMOS-RRAM true random number generator exploiting coupled entropy sources," *IEEE Trans. Electron Devices*, vol. 70, no. 3, pp. 1061–1066, Mar. 2023, doi: 10.1109/TED.2023.3241122.

[173] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, Nov. 2002, pp. 148–160, doi: 10.1145/586110.586132.

[174] S. Lee and D. H. Lee, "From attack to identification: MEMS sensor fingerprinting using acoustic signals," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 5447–5460, Mar. 2023, doi: 10.1109/JIOT.2022.3221930.

[175] D. P. Sahoo, D. Mukhopadhyay, R. S. Chakraborty, and P. H. Nguyen, "A multiplexer-based arbiter PUF composition with enhanced reliability and security," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 403–417, Mar. 2018, doi: 10.1109/TC.2017.2749226.

[176] P. H. Nguyen, D. P. Sahoo, R. S. Chakraborty, and D. Mukhopadhyay, "Security analysis of arbiter PUF and its lightweight compositions under predictability test," *ACM Trans. Design Autom. Electron. Syst.*, vol. 22, no. 2, pp. 1–28, Apr. 2017, doi: 10.1145/2940326.

[177] R. Podeti, S. R. Patri, and P. Muralidhar, "Highly reliable XoR feed arbiter physical unclonable function (XFAPUF) in 180 nm process for IoT security," *Microprocess. Microsyst.*, vol. 87, Nov. 2021, Art. no. 104355, doi: 10.1016/j.micpro.2021.104355.

[178] T. Idriss and M. Bayoumi, "Lightweight highly secure PUF protocol for mutual authentication and secret message exchange," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Warsaw, Poland, Sep. 2017, pp. 214–219, doi: 10.1109/RFID-TA.2017.8098893.

[179] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005, doi: 10.1109/TVLSI.2005.859470.

[180] R. Naveenkumar, N. M. Sivamangai, A. Napolean, and S. S. S. Priya, "Design and evaluation of XOR arbiter physical unclonable function and its implementation on FPGA in hardware security applications," *J. Electron. Test.*, vol. 38, no. 6, pp. 653–666, Dec. 2022, doi: 10.1007/s10836-022-06034-7.

[181] S. V. S. Avvaru, Z. Zeng, and K. K. Parhi, "Homogeneous and heterogeneous feed-forward XOR physical unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2485–2498, 2020, doi: 10.1109/TIFS.2020.2968113.

[182] G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, vol. 9293, Saint-Malo, France. Berlin, Germany: Springer, Sep. 2015, pp. 535–555, doi: 10.1007/978-3-662-48324-4_27.

[183] N. N. Anandakumar, M. S. Hashmi, and M. A. Chaudhary, "Implementation of efficient XOR arbiter PUF on FPGA with enhanced uniqueness and security," *IEEE Access*, vol. 10, pp. 129832–129842, 2022, doi: 10.1109/ACCESS.2022.3228635.

[184] C. Gu, W. Liu, Y. Cui, N. Hanley, M. O'Neill, and F. Lombardi, "A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1853–1866, Oct. 2021, doi: 10.1109/TETC.2019.2935465.

[185] N. Shah, D. Chatterjee, B. Sapui, D. Mukhopadhyay, and A. Basu, "Introducing recurrence in strong PUFs for enhanced machine learning attack resistance," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 319–332, Jun. 2021, doi: 10.1109/JETCAS.2021.3075767.

[186] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rhrmair, and M. Van Dijk, "The interpose PUF: Secure PUF design against state-of-the-art machine learning attacks," *IACR Trans. Cryptograph. Hardware Embedded Syst.*, vol. 2019, no. 4, pp. 243–290, 2019, doi: 10.13154/tches.v2019.i4.243-290.

[187] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn, "A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test," *IEEE Access*, vol. 8, pp. 181751–181762, 2020, doi: 10.1109/ACCESS.2020.3028514.

[188] S. Hou, Y. Guo, S. Li, D. Deng, and Y. Lei, "A lightweight and secure-enhanced strong PUF design on FPGA," *IEICE Electron. Exp.*, vol. 16, no. 24, 2019, Art. no. 20190695, doi: 10.1587/elex.16.20190695.

[189] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, "Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 1109–1123, Apr. 2019, doi: 10.1109/TIFS.2018.2870835.

[190] R. Della Sala, D. Bellizia, and G. Scotti, "A lightweight FPGA compatible weak-PUF primitive based on XOR gates," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 2972–2976, Jun. 2022, doi: 10.1109/TCSII.2022.3156788.

[191] R. Della Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA PUF: The DD-PUF," *Cryptography*, vol. 5, no. 3, p. 23, Sep. 2021, doi: 10.3390/cryptography5030023.

[192] R. Ali, D. Zhang, H. Cai, W. Zhao, and Y. Wang, "A machine learning attack-resilient strong PUF leveraging the process variation of MRAM," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 2712–2716, Jun. 2022, doi: 10.1109/TCSII.2022.3144497.

[193] R. Govindaraj, S. Ghosh, and S. Katkoori, "Design, analysis and application of embedded resistive RAM based strong arbiter PUF," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 6, pp. 1232–1242, Nov. 2020, doi: 10.1109/TDSC.2018.2866425.

[194] P. Santikellur, A. Bhattacharyay, and R. S. Chakraborty, "Deep learning based model building attacks on arbiter PUF compositions," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 566, Sep. 2019.

[195] K. T. Mursi, Y. Zhuang, M. S. Alkatheiri, and A. O. Aseeri, "Extensive examination of XOR arbiter PUFs as security primitives for resource-constrained IoT devices," in *Proc. 17th Int. Conf. Privacy, Secur. Trust (PST)*, Fredericton, NB, Canada, Aug. 2019, pp. 1–9, doi: 10.1109/PST47121.2019.8949070.

[196] S.-J. Wang, Y.-S. Chen, and K. S. Li, "Modeling attack resistant PUFs based on adversarial attack against machine learning," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 306–318, Jun. 2021, doi: 10.1109/JETCAS.2021.3062413.

[197] J. Zhang and C. Shen, "Set-based obfuscation for strong PUFs against machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 1, pp. 288–300, Jan. 2021, doi: 10.1109/TCSI.2020.3028508.

[198] S. S. Fard, M. Kaveh, M. R. Mosavi, and S.-B. Ko, "An efficient modeling attack for breaking the security of XOR-arbiter PUFs by using the fully connected and long-short term memory," *Microprocess. Microsyst.*, vol. 94, Oct. 2022, Art. no. 104667, doi: 10.1016/j.micpro.2022.104667.

[199] P. Santikellur and R. S. Chakraborty, "A computationally efficient tensor regression network-based modeling attack on XOR arbiter PUF and its variants," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1197–1206, Jun. 2021, doi: 10.1109/TCAD.2020.3032624.

[200] H. Momeni, A. Ghazizadeh, and F. Sharifi, "Multi-valued logic arbiter PUF designs based on CNTFETs," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108295, doi: 10.1016/j.compeleceng.2022.108295.

[201] R. Ali, H. Ma, Z. Hou, D. Zhang, E. Deng, and Y. Wang, "A reconfigurable arbiter MPUF with high resistance against machine learning attack," *IEEE Trans. Magn.*, vol. 57, no. 10, pp. 1–7, Oct. 2021, doi: 10.1109/TMAG.2021.3102838.

[202] L. Yao, H. Liang, Q. Han, H. Zhang, Z. Huang, C. Jiang, M. Yi, and Y. Lu, "M-RO PUF: A portable pure digital RO PUF based on MUX unit," *Microelectron. J.*, vol. 119, Jan. 2022, Art. no. 105314, doi: 10.1016/j.mejo.2021.105314.

[203] H. Kareem and D. Dunaev, "A robust architecture of ring oscillator PUF: Enhancing cryptographic security with configurability," *Microelectron. J.*, vol. 143, Jan. 2024, Art. no. 106022, doi: 10.1016/j.mejo.2023.106022.

[204] D. Deng, S. Hou, Z. Wang, and Y. Guo, "Configurable ring oscillator PUF using hybrid logic gates," *IEEE Access*, vol. 8, pp. 161427–161437, 2020, doi: 10.1109/ACCESS.2020.3021205.

[205] Y. Cui, C. Wang, W. Liu, C. Gu, M. O'Neill, and F. Lombardi, "Lightweight configurable ring oscillator PUF based on RRAM/CMOS hybrid circuits," *IEEE Open J. Nanotechnol.*, vol. 1, pp. 128–134, 2020, doi: 10.1109/OJNANO.2020.3040787.

[206] Y. Jiang, Y. Hu, and W. Wang, "A design strategy to improve machine learning resiliency for ring oscillator physically unclonable function," *IEEE Access*, vol. 11, pp. 34104–34118, 2023, doi: 10.1109/ACCESS.2023.3260841.

[207] C. Gu, J. Murphy, and M. O'Neill, "A unique and robust single slice FPGA identification generator," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Melbourne, VIC, Australia, Jun. 2014, pp. 1223–1226, doi: 10.1109/ISCAS.2014.6865362.

[208] L. Lu, T. Yoo, and T. T. Kim, "A 6T SRAM based two-dimensional configurable challenge-response PUF for portable devices," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 6, pp. 2542–2552, Jun. 2022, doi: 10.1109/TCSI.2022.3156983.

[209] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "16.2 A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS," in *Proc. IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers (ISSCC)*, San Francisco, CA, USA, Feb. 2014, pp. 278–279, doi: 10.1109/ISSCC.2014.6757433.

[210] K. Xu, D. Zhang, Q. Ren, Y. Cheng, and P. Girard, "All-spin PUF: An area-efficient and reliable PUF design with signature improvement for spin-transfer torque magnetic cell-based all-spin circuits," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 18, no. 4, pp. 1–20, Oct. 2022, doi: 10.1145/3517811.

[211] T. K. Esatu, A. Prakash, Z. Li, D. Lau, S. H. Jo, and T. K. Liu, "Highly reliable and secure PUF using resistive memory integrated into a 28 nm CMOS process," *IEEE Trans. Electron Devices*, vol. 70, no. 5, pp. 2291–2296, May 2023, doi: 10.1109/TED.2023.3251953.

[212] J. Li, Y. Cui, C. Wang, C. Gu, and W. Liu, "A fully configurable PUF using dynamic variations of resistive crossbar arrays," *IEEE Trans. Nanotechnol.*, vol. 21, pp. 737–746, 2022, doi: 10.1109/TNANO.2022.3221372.

[213] B. Coppens, I. Verbauwhede, K. De Bosschere, and B. De Sutter, "Practical mitigations for timing-based side-channel attacks on modern x86 processors," in *Proc. 30th IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2009, pp. 45–60, doi: 10.1109/SP.2009.19.

[214] Y. Sovyn, V. Khoma, and I. Opirskyy, "Minimization of bitsliced-representation of 4×4 S-boxes based on ternary logic instruction," *Comput. Syst. Netw.*, vol. 5, no. 1, pp. 103–113, Dec. 2023, doi: 10.23939/csn2023.01.103.

[215] U. Ali, S. A. R. Sahni, and O. Khan, "Characterization of timing-based software side-channel attacks and mitigations on network-on-chip hardware," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 19, no. 3, pp. 1–23, Jul. 2023, doi: 10.1145/3585519.

[216] S. Khan, W.-K. Lee, A. Khalid, A. Majeed, and S. O. Hwang, "Area-optimized constant-time hardware implementation for polynomial multiplication," *IEEE Embedded Syst. Lett.*, vol. 15, no. 1, pp. 5–8, Mar. 2023, doi: 10.1109/LES.2022.3185265.

[217] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif, "A support vector machine-based framework for detection of covert timing channels," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 274–283, Mar. 2016, doi: 10.1109/TDSC.2015.2423680.

[218] S. Al-Eidi, O. Darwish, Y. Chen, M. Maabreh, and Y. Tashtoush, "A deep learning approach for detecting covert timing channel attacks using sequential data," *Cluster Comput.*, vol. 27, no. 2, pp. 1655–1665, Apr. 2024, doi: 10.1007/s10586-023-04035-5.

[219] T. Yavuz, F. Fowze, G. Hernandez, K. Y. Bai, K. R. B. Butler, and D. J. Tian, "ENCIDER: Detecting timing and cache side channels in SGX enclaves and cryptographic Apis," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1577–1595, Mar. 2023, doi: 10.1109/TDSC.2022.3160346.

[220] J. Van Cleemput, B. De Sutter, and K. De Bosschere, "Adaptive compiler strategies for mitigating timing side channel attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 1, pp. 35–49, Jan. 2020, doi: 10.1109/TDSC.2017.2729549.

[221] A. Kar, X. Liu, Y. Kim, G. Saileshwar, H. Kim, and T. Krishna, "Mitigating timing-based NoC side-channel attacks with LLC remapping," *IEEE Comput. Archit. Lett.*, vol. 22, no. 1, pp. 53–56, Jan. 2023, doi: 10.1109/LCA.2023.3276709.

[222] S. Liu and W. Yi, "Task parameters analysis in schedule-based timing side-channel attack," *IEEE Access*, vol. 8, pp. 157103–157115, 2020, doi: 10.1109/ACCESS.2020.3019323.

[223] C. Zhang, Z. Liu, Y. Chen, J. Lu, and D. Liu, "A flexible and generic Gaussian sampler with power side-channel countermeasures for quantum-secure Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8167–8177, Sep. 2020, doi: 10.1109/JIOT.2020.2981133.

[224] M. Masoumi, "Novel hybrid CMOS/Memristor implementation of the AES algorithm robust against differential power analysis attack," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 7, pp. 1314–1318, Jul. 2020, doi: 10.1109/TCSII.2019.2932337.

[225] D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, A. Trifiletti, and F. B. Trotta, "Secure double rate registers as an RTL countermeasure against power analysis attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 7, pp. 1368–1376, Jul. 2018, doi: 10.1109/TVLSI.2018.2816914.

[226] U. Rioja, L. Batina, J. L. Flores, and I. Armendariz, "Towards automatic and portable data loading template attacks on micro-controllers," in *Proc. 22nd Int. Symp. Quality Electron. Design (ISQED)*, Santa Clara, CA, USA, Apr. 2021, pp. 437–443, doi: 10.1109/ISQED51717.2021.9424276.

[227] Y. Bi, P.-E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Polarity-controllable silicon NanoWire FET-based security," in *Security Opportunities in Nano Devices and Emerging Technologies*. Boca Raton, FL, USA: CRC Press, 2017, pp. 143–156, doi: 10.1201/9781315265056-8.

[228] I. M. Verbauwhede and K. J. Tiri, "Dynamic and differential CMOS logic with signal-independent power consumption to withstand differential power analysis," U.S. Patent 7 417 468, Aug. 26, 2008.

[229] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. 8th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Yokohama, Japan. Berlin, Germany: Springer, 2006, pp. 232–241, doi: 10.1007/11894063_19.

[230] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 7, pp. 1147–1153, Jul. 2011, doi: 10.1109/TVLSI.2010.2046505.

[231] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: A novel FinFET based secure adiabatic logic for energy-efficient and DPA resistant IoT devices," in *Proc. IEEE Int. Conf. Rebooting Comput. (ICRC)*, San Diego, CA, USA, Oct. 2016, pp. 1–8, doi: 10.1109/ICRC.2016.7738710.

[232] S. D. Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart card," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 281–293, Apr. 2019, doi: 10.1109/TETC.2016.2645128.

[233] S. Kaedi, M. A. Doostari, and M. B. Ghaznavi-Ghoushchi, "A DPA attack on IOA data-dependent delay countermeasure based on an inherent tempo-spatial data dependency," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 8, pp. 1341–1345, Aug. 2019, doi: 10.1109/TCSII.2018.2877525.

[234] A. Roohi and R. F. DeMara, "PARC: A novel design methodology for power analysis resilient circuits using spintronics," *IEEE Trans. Nanotechnol.*, vol. 18, pp. 885–889, 2019, doi: 10.1109/TNANO.2019.2934887.

[235] M. W. Allam and M. I. Elmasry, "Dynamic current mode logic (DyCML): A new low-power high-performance logic style," *IEEE J. Solid-State Circuits*, vol. 36, no. 3, pp. 550–558, Mar. 2001, doi: 10.1109/4.910495.

[236] D. Canright and L. Batina, "A very compact 'perfectly masked' S-box for AES," in *Proc. 6th Int. Conf. Appl. Cryptogr. Netw. Secur.*, New York, NY, USA. Berlin, Germany: Springer, 2008, pp. 446–459, doi: 10.1007/978-3-540-68914-0_27.

[237] J. D. Golić and C. Tymen, "Multiplicative masking and power analysis of AES," in *Proc. 4th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Redwood Shores, CA, USA. Berlin, Germany: Springer, Aug. 2002, pp. 198–212, doi: 10.1007/3-540-36400-5_16.

[238] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, "RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2012, pp. 1173–1178.

[239] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010, doi: 10.1109/JSSC.2009.2034081.

[240] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018, doi: 10.1109/JSSC.2018.2822691.

[241] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020, doi: 10.1109/JSSC.2019.2945944.

[242] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D.-H. Seo, M. Chang, A. L. Varna, H. K. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen, "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021, doi: 10.1109/JSSC.2020.3032975.

[243] R. Kumar, X. Liu, V. Suresh, H. K. Krishnamurthy, S. Satpathy, M. A. Anders, H. Kaul, K. Ravichandran, V. De, and S. K. Mathew, "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021, doi: 10.1109/JSSC.2021.3052146.

[244] G. Khedkar, D. Kudithipudi, and G. S. Rose, "Power profile obfuscation using nanoscale memristive devices to counter DPA attacks," *IEEE Trans. Nanotechnol.*, vol. 14, no. 1, pp. 26–35, Jan. 2015, doi: 10.1109/TNANO.2014.2362416.
[245] W. Hua, Z. Zhang, and G. E. Suh, "Reverse engineering convolutional neural networks through side-channel information leaks," in *Proc. 55th ACM/ESDA/IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2018, pp. 1–6, doi: 10.1109/DAC.2018.8465773.
[246] A. Dubey, R. Cammarota, and A. Aysu, "MaskedNet: The first hardware inference engine aiming power side-channel protection," in *Proc. Int. Symp. Hardware Oriented Security Trust (HOST)*, Dec. 2020, pp. 197–208, doi: 10.1109/HOST45689.2020.9300276.
[247] A. Dubey, R. Cammarota, and A. Aysu, "BoMaNet: Boolean masking of an entire neural network," in *Proc. IEEE/ACM Int. Conf. Comput. Aided Design (ICCAD)*, San Diego, CA, USA, Nov. 2020, pp. 1–9.
[248] Y. N. Wu, J. S. Emer, and V. Sze, "Accelergy: An architecture-level energy estimation methodology for accelerator designs," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, Westminster, CO, USA, Nov. 2019, pp. 1–8, doi: 10.1109/ICCAD45719.2019.8942149.
[249] S. Maji, U. Banerjee, S. H. Fuller, and A. P. Chandrakasan, "A threshold implementation-based neural network accelerator with power and electromagnetic side-channel countermeasures," *IEEE J. Solid-State Circuits*, vol. 58, no. 1, pp. 141–154, Jan. 2023, doi: 10.1109/JSSC.2022.3215670.
[250] V.-P. Hoang, N.-T. Do, and V. Sang Doan, "Efficient nonprofiled side-channel attack using multi-output classification neural network," *IEEE Embedded Syst. Lett.*, vol. 15, no. 3, pp. 145–148, Sep. 2023, doi: 10.1109/LES.2022.3213443.
[251] I. M. Delgado-Lozano, E. Tena-Sánchez, J. Núñez, and A. J. Acosta, "Projection of dual-rail DPA countermeasures in future FinFET and emerging TFET technologies," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 3, pp. 1–16, Jul. 2020, doi: 10.1145/3381857.
[252] F. Larroca, P. Bertrand, F. Carrau, and V. Severi, "Gr-tempest: An open-source GNU radio implementation of TEMPEST," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Singapore, Dec. 2022, pp. 1–6, doi: 10.1109/AsianHOST56390.2022.10022149.
[253] S. Saadat, "Protection of modular data centers from cyber attack via electromagnetic emanations," in *Proc. Asia–Pacific Int. Symp. Electromagn. Compat. (APEMC)*, Bali, Indonesia, Sep. 2021, pp. 1–4, doi: 10.1109/APEMC49932.2021.9596867.
[254] J. He, X. Guo, M. Tehranipoor, A. Vassilev, and Y. Jin, "EM side channels in hardware security: Attacks and defenses," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 39, no. 2, pp. 100–111, Apr. 2022, doi: 10.1109/MDAT.2021.3135324.
[255] S. Kaji, D. Fujimoto, M. Kinugawa, and Y. Hayashi, "Echo TEMPEST: EM information leakage induced by IEMI for electronic devices," *IEEE Trans. Electromagn. Compat.*, vol. 65, no. 3, pp. 655–666, Jun. 2023, doi: 10.1109/TEMC.2023.3252636.
[256] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Paris, France. Berlin, Germany: Springer, May 2001, pp. 251–261, doi: 10.1007/3-540-44709-1_21.
[257] J. Pan, J. G. J. Van Woudenberg, J. I. D. Hartog, and M. F. Witteman, "Improving DPA by peak distribution analysis," in *Proc. 17th Int. Workshop Select. Areas Cryptogr.*, Waterloo, ON, Canada. Berlin, Germany: Springer, 2010, pp. 241–261, doi: 10.1007/978-3-642-19574-7_17.
[258] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 16th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Cambridge, MA, USA. Berlin, Germany: Springer, Aug. 2004, pp. 16–29, doi: 10.1007/978-3-540-28632-5_2.
[259] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397, doi: 10.1007/3-540-48405-1_25.
[260] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration*, vol. 40, no. 1, pp. 52–60, Jan. 2007, doi: 10.1016/j.vlsi.2005.12.013.
[261] F.-X. Standaert, F. Mac, E. Peeters, and J -J. Quisquater, "Updates on the security of FPGAs against power analysis attacks," in *Proc. 2nd Reconfigurable Comput. Architectures Appl. Conf.*, Delft, The Netherlands. Berlin, Germany: Springer, Mar. 2006, pp. 335–346, doi: 10.1007/11802839_42.
[262] M. Tunstall, D. Mukhopadhyay, and S. Ali, "Differential fault analysis of the advanced encryption standard using a single fault," in *Proc. IFIP 5th Int. Workshop Inf. Secur. Theory Practices*, Crete, Greece. Berlin, Germany: Springer, Jun. 2011, pp. 224–233, doi: 10.1007/978-3-642-21040-2_15.
[263] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D. Seo, M. Chang, A. Varna, H. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen, "27.3 EM and power SCA-resilient AES-256 in 65 nm CMOS through >350× current-domain signature attenuation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2020, pp. 424–426, doi: 10.1109/ISSCC19947.2020.9062997.
[264] N. Miura, D. Fujimoto, M. Nagata, N. Homma, Y. Hayashi, and T. Aoki, "EM attack sensor: Concept, circuit, and design-automation methodology," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2015, pp. 1–6, doi: 10.1145/2744769.2747923.
[265] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Dresden, Germany, Mar. 2014, pp. 1–6, doi: 10.7873/DATE.2014.216.
[266] D.-H. Seo, M. Nath, D. Das, B. Chatterjee, S. Ghosh, and S. Sen, "PG-CAS: Patterned-ground co-planar capacitive asymmetry sensing for mm-range EM side-channel attack probe detection," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021, pp. 1–5, doi: 10.1109/ISCAS51556.2021.9401580.
[267] A. Ghosh, M. Nath, D. Das, S. Ghosh, and S. Sen, "Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection," *IEEE Microw. Wireless Compon. Lett.*, vol. 32, no. 6, pp. 784–787, Jun. 2022, doi: 10.1109/LMWC.2022.3161001.
[268] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022, doi: 10.1109/JSSC.2021.3113335.
[269] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Mclean, VA, USA, May 2017, pp. 62–67, doi: 10.1109/HST.2017.7951799.
[270] K. Wei, J. W. Kwak, and D. B. Ma, "An encrypted on-chip power supply with random parallel power injection and charge recycling against power/EM side-channel attacks," *IEEE Trans. Power Electron.*, vol. 38, no. 1, pp. 500–509, Jan. 2023, doi: 10.1109/TPEL.2022.3206182.
[271] E. Katz, M. Avital, Y. Weizman, and I. Levi, "Analytical side channel EM models, extending simulation abilities for ICs, and linking physical-models to cryptographic metrics," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 12, pp. 4463–4476, Dec. 2023, doi: 10.1109/TCAD.2023.3289310.
[272] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for IC chip level hardware security," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 1, pp. 5–14, Jan. 2022, doi: 10.1109/TVLSI.2021.3073946.
[273] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, "Checking robustness against EM side-channel attacks prior to manufacturing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 5, pp. 1264–1275, May 2022, doi: 10.1109/TCAD.2021.3092297.
[274] A. Dehbaoui, V. Lomne, T. Ordas, L. Torres, M. Robert, and P. Maurine, "Enhancing electromagnetic analysis using magnitude squared incoherence," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 3, pp. 573–577, Mar. 2012, doi: 10.1109/TVLSI.2011.2104984.
[275] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "EM-X-DL: Efficient cross-device deep learning side-channel attack with noisy EM signatures," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 18, no. 1, pp. 1–17, Jan. 2022, doi: 10.1145/3465380.
[276] A. T. Markettos and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," in *Proc. Int. Workshop Cryptographic Hardw. Embedded Syst.*, Lausanne, Switzerland. Berlin, Germany: Springer, 2009, pp. 317–331, doi: 10.1007/978-3-642-04138-9_23.

[277] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *Proc. 3rd Int. Constructive Side-Channel Anal. Secure Design*, Darmstadt, Germany. Berlin, Germany: Springer, May 2012, pp. 151–166, doi: 10.1007/978-3-642-29912-4_12.

[278] P. Haddad, C. Kasmi, J. Esteves, and V. Houchouas, "Electromagnetic harmonic attack on transient effect ring oscillator based true random number generator," in *Proc. Hardwear IO Conf.*, The Hague, The Netherlands, 2016. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0 and https://www.youtube.com/watch?v=mTZYwCTDL7c&t=74s

[279] S. Osuka, D. Fujimoto, Y.-I. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "EM information security threats against RO-based TRNGs: The frequency injection attack based on IEMI and EM information leakage," *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 4, pp. 1122–1128, Aug. 2019, doi: 10.1109/TEMC.2018.2844027.

[280] S. Osuka, D. Fujimoto, S. Kawamura, and Y. Hayashi, "Electromagnetic side-channel analysis against TERO-based TRNG," *IEEE Trans. Electromagn. Compat.*, vol. 64, no. 5, pp. 1288–1295, Oct. 2022, doi: 10.1109/TEMC.2022.3189372.

[281] J. He, H. Ma, M. Panoff, H. Wang, Y. Zhao, L. Liu, X. Guo, and Y. Jin, "Security oriented design framework for EM side-channel protection in RTL implementations," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 8, pp. 2421–2434, Aug. 2022, doi: 10.1109/TCAD.2021.3112884.

[282] M. M. M. Rahman, M. S. Rahman, R. Kibria, M. Borza, B. Reddy, A. Cron, F. Rahman, M. Tehranipoor, and F. Farahmandi, "CAPEC: A cellular automata guided FSM-based IP authentication scheme," in *Proc. IEEE 41st VLSI Test Symp. (VTS)*, Farah, CA, USA, Apr. 2023, pp. 1–8, doi: 10.1109/VTS56346.2023.10140093.

[283] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001, doi: 10.1109/43.952740.

[284] G. Qu, J. L. Vvong, and M. Potkonjak, "Fair watermarking techniques," in *Proc. Design Autom. Conf.*, Yokohama, Japan, Jan. 2000, pp. 55–60, doi: 10.1109/ASPDAC.2000.835070.

[285] H. J. Patel, J. W. Crouch, Y. C. Kim, and T. C. Kim, "Creating a unique digital fingerprint using existing combinational logic," in *Proc. IEEE Int. Symp. Circuits Syst.*, Taipei, Taiwan, May 2009, pp. 2693–2696, doi: 10.1109/ISCAS.2009.5118357.

[286] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardware-Oriented Secur. Trust*, Jun. 2008, pp. 51–57, doi: 10.1109/HST.2008.4559049.

[287] S. L. P. S. K. Patanjali, A. A. Nair, C. Rebeiro, and S. Bhunia, "SIGNED: A challenge-response scheme for electronic hardware watermarking," *IEEE Trans. Comput.*, vol. 72, no. 6, pp. 1763–1777, Jun. 2023, doi: 10.1109/TC.2022.3223304.

[288] U. Das, M. S. Rahman, N. Nalla Anandakumar, K. Z. Azar, F. Rahman, M. Tehranipoor, and F. Farahmandi, "PSC-watermark: Power side channel based IP watermarking using clock gates," in *Proc. IEEE Eur. Test Symp. (ETS)*, Farah, Italy, May 2023, pp. 1–6, doi: 10.1109/ETS56758.2023.10174052.

[289] A. Cui, C.-H. Chang, S. Tahar, and A. T. Abdel-Hamid, "A robust FSM watermarking scheme for IP protection of sequential circuit design," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 30, no. 5, pp. 678–690, May 2011, doi: 10.1109/TCAD.2010.2098131.

[290] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "FSM inspired unconventional hardware watermark using field-assisted SOT-MTJ," *IEEE Access*, vol. 11, pp. 8150–8158, 2023, doi: 10.1109/ACCESS.2023.3238807.

[291] Sonam, K. Sehra, R. P. Singh, S. Singh, S. Wadhera, P. Kasturi, G. J. Saxena, and M. Saxena, "Secure digital image watermarking using memristor-based hyperchaotic circuit," *Vis. Comput.*, vol. 39, no. 10, pp. 4459–4485, Oct. 2023, doi: 10.1007/s00371-022-02601-3.

[292] A. Tiwari and V. K. Srivastava, "Novel schemes for the improvement of lifting wavelet transform-based image watermarking using Schur decomposition," *J. Supercomput.*, vol. 79, no. 12, pp. 13142–13179, Aug. 2023, doi: 10.1007/s11227-023-05167-6.

[293] F. Koushanfar, I. Hong, and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," *ACM Trans. Design Autom. Electron. Syst.*, vol. 10, no. 3, pp. 523–545, Jul. 2005, doi: 10.1145/1080334.1080338.

[294] A. Sengupta, D. Roy, and S. P. Mohanty, "Triple-phase watermarking for reusable IP core protection during architecture synthesis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 4, pp. 742–755, Apr. 2018, doi: 10.1109/TCAD.2017.2729341.

[295] M. Rathor, A. Anshul, K. Bharath, R. Chaurasia, and A. Sengupta, "Quadruple phase watermarking during high level synthesis for securing reusable hardware intellectual property cores," *Comput. Electr. Eng.*, vol. 105, Jan. 2023, Art. no. 108476, doi: 10.1016/j.compeleceng.2022.108476.

[296] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2015, pp. 137–143, doi: 10.1109/HST.2015.7140252.

[297] Y. Xie and A. Srivastava, "Anti-SAT: Mitigating SAT attack on logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 2, pp. 199–207, Feb. 2019, doi: 10.1109/TCAD.2018.2801220.

[298] M. Yasin, B. Mazumdar, J. J. V. Rajendran, and O. Sinanoglu, "SARLock: SAT attack resistant logic locking," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, McLean, VA, USA, May 2016, pp. 236–241, doi: 10.1109/HST.2016.7495588.

[299] M. Yasin, A. Sengupta, B. C. Schafer, Y. Makris, O. Sinanoglu, and J. Rajendran, "What to lock? Functional and parametric locking," in *Proc. Great Lakes Symp. VLSI*, May 2017, pp. 351–356, doi: 10.1145/3060403.3060492.

[300] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal attacks on logic locking and camouflaging techniques," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, no. 2, pp. 517–532, Apr. 2020, doi: 10.1109/TETC.2017.2740364.

[301] X. Xu, B. Shakya, M. M. Tehranipoor, and D. Forte, "Novel bypass attack and BDD-based tradeoff analysis against all known logic locking attacks," in *Proc. 19th Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, Taipei, Taiwan. Berlin, Germany: Springer, Sep. 2017, pp. 189–210, doi: 10.1007/978-3-319-66787-4_10.

[302] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, and Y. Jin, "AppSAT: Approximately deobfuscating integrated circuits," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Mclean, VA, USA, May 2017, pp. 95–100, doi: 10.1109/HST.2017.7951805.

[303] J. Zhou and X. Zhang, "Generalized SAT-attack-resistant logic locking," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2581–2592, 2021, doi: 10.1109/TIFS.2021.3059271.

[304] B. Shakya, X. Xu, M. Tehranipoor, and D. Forte, "CAS-Lock: A security-corruptibility trade-off resilient logic locking scheme," *IACR Trans. Cryptograph. Hardware Embedded Syst.*, vol. 2020, pp. 175–202, Nov. 2020, doi: 10.13154/tches.v2020.i1.175-202.

[305] R. Hassan, G. Kolhe, S. Rafatirad, H. Homayoun, and S. M. Dinakarrao, "SATConda: SAT to SAT-hard clause translator," in *Proc. 21st Int. Symp. Quality Electron. Design (ISQED)*, Santa Clara, CA, USA, Mar. 2020, pp. 155–160, doi: 10.1109/ISQED48828.2020.9137052.

[306] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-secure logic locking: From theory to practice," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1601–1618, doi: 10.1145/3133956.3133985.

[307] H. Zhou, Y. Shen, and A. Rezaei, "Vulnerability and remedy of stripped function logic locking," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 139, 2019. [Online]. Available: https://eprint.iacr.org/2019/139.pdf

[308] H. M. Kamali, K. Z. Azar, H. Homayoun, and A. Sasan, "Full-lock: Hard distributions of SAT instances for obfuscating circuits using fully configurable logic and routing blocks," in *Proc. 56th ACM/IEEE Design Autom. Conf. (DAC)*, Las Vegas, NV, USA, Jun. 2019, pp. 1–6.

[309] M. Yasin, J. J. Rajendran, O. Sinanoglu, and R. Karri, "On improving the security of logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 35, no. 9, pp. 1411–1424, Sep. 2016, doi: 10.1109/TCAD.2015.2511144.

[310] K. Juretus and I. Savidis, "Increased output corruption and structural attack resilience for SAT attack secure logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 1, pp. 38–51, Jan. 2021, doi: 10.1109/TCAD.2020.2988629.

[311] P. Chakraborty, J. Cruz, A. Alaql, and S. Bhunia, "SAIL: Analyzing structural artifacts of logic locking using machine learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3828–3842, 2021, doi: 10.1109/TIFS.2021.3096028.

[312] A. Alaql and S. Bhunia, "SARO: Scalable attack-resistant logic locking," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3724–3739, 2021, doi: 10.1109/TIFS.2021.3092135.

[313] Y. Xie and A. Srivastava, "Delay locking: Security enhancement of logic locking against IC counterfeiting and overproduction," in *Proc. 54th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Austin, TX, USA, Jun. 2017, pp. 1–6, doi: 10.1145/3061639.3062226.
[314] A. Chakraborty, Y. Liu, and A. Srivastava, "Evaluating the security of delay-locked circuits," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 4, pp. 608–619, Apr. 2021, doi: 10.1109/TCAD.2020.3008843.
[315] Y. Zhong and U. Guin, "Complexity analysis of the SAT attack on logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 10, pp. 3143–3156, Oct. 2023, doi: 10.1109/TCAD.2023.3240933.
[316] R. Hassan, G. Kolhe, S. Rafatirad, H. Homayoun, and S. M. P. Dinakarrao, "A neural network-based cognitive obfuscation toward enhanced logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 11, pp. 4587–4599, Nov. 2022, doi: 10.1109/TCAD.2021.3138686.
[317] M. S. Rahman, R. Guo, H. M. Kamali, F. Rahman, F. Farahmandi, and M. Tehranipoor, "ReTrustFSM: Toward RTL hardware obfuscation—A hybrid FSM approach," *IEEE Access*, vol. 11, pp. 19741–19761, 2023, doi: 10.1109/ACCESS.2023.3244902.
[318] L. Mankali, L. Alrahis, S. Patnaik, J. Knechtel, and O. Sinanoglu, "Titan: Security analysis of large-scale hardware obfuscation using graph neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 304–318, 2023, doi: 10.1109/TIFS.2022.3218429.
[319] J. Gandhi, D. Shekhawat, M. Santosh, and J. G. Pandey, "Logic locking for IP security: A comprehensive analysis on challenges, techniques, and trends," *Comput. Secur.*, vol. 129, Jun. 2023, Art. no. 103196, doi: 10.1016/j.cose.2023.103196.
[320] M. Yasin, B. Mazumdar, J. Rajendran, and O. Sinanoglu, "Hardware security and trust: Logic locking as a design-for-trust solution," in *The IoT Physical Layer: Design and Implementation*. Cham, Switzerland: Springer, 2019, pp. 353–373, doi: 10.1007/978-3-319-93100-5_20.
[321] M. Yasin, B. Mazumdar, J. Rajendran, and O. Sinanoglu, "Hardware security and trust: Logic locking as a design-for-trust solution," in *The IoT Physical Layer: Design and Implementation*, 2019, pp. 353–373, doi: 10.1007/978-3-319-93100-5_20.
[322] S. Dupuis and M.-L. Flottes, "Logic locking: A survey of proposed methods and evaluation metrics," *J. Electron. Test.*, vol. 35, no. 3, pp. 273–291, Jun. 2019, doi: 10.1007/s10836-019-05800-4.
[323] D. Sisejkovic, F. Merchant, L. M. Reimann, H. Srivastava, A. Hallawa, and R. Leupers, "Challenging the security of logic locking schemes in the era of deep learning: A neuroevolutionary approach," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 17, no. 3, pp. 1–26, Jul. 2021, doi: 10.1145/3431389.
[324] D. Sisejkovic, F. Merchant, L. M. Reimann, and R. Leupers, "Deceptive logic locking for hardware integrity protection against machine learning attacks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 6, pp. 1716–1729, Jun. 2022, doi: 10.1109/TCAD.2021.3100275.
[325] A. Sengupta and R. Chaurasia, "Securing IP cores for DSP applications using structural obfuscation and chromosomal DNA impression," *IEEE Access*, vol. 10, pp. 50903–50913, 2022, doi: 10.1109/ACCESS.2022.3174349.
[326] A. Sengupta and M. Rathor, "Enhanced security of DSP circuits using multi-key based structural obfuscation and physical-level watermarking for consumer electronics systems," *IEEE Trans. Consum. Electron.*, vol. 66, no. 2, pp. 163–172, May 2020, doi: 10.1109/TCE.2020.2972808.
[327] S. Patnaik, M. Ashraf, O. Sinanoglu, and J. Knechtel, "A modern approach to IP protection and trojan prevention: Split manufacturing for 3D ICs and obfuscation of vertical interconnects," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1815–1834, Oct. 2021, doi: 10.1109/TETC.2019.2933572.
[328] T. Nigussie, J. C. Schabel, S. Lipa, L. McIlrath, R. Patti, and P. Franzon, "Design obfuscation through 3-D split fabrication with smart partitioning," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 9, pp. 1230–1243, Sep. 2022, doi: 10.1109/TVLSI.2022.3179304.
[329] A. Suresh, S. N. Dhanuskodi, and D. Holcomb, "A secure design methodology to prevent targeted trojan insertion during fabrication," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jun. 2023, pp. 1–6, doi: 10.1109/ISVLSI59464.2023.10238490.
[330] S. Patnaik, M. Ashraf, H. Li, J. Knechtel, and O. Sinanoglu, "Concerted wire lifting: Enabling secure and cost-effective split manufacturing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 2, pp. 266–280, Feb. 2022, doi: 10.1109/TCAD.2021.3056379.
[331] H. Li, S. Patnaik, M. Ashraf, H. Yang, J. Knechtel, B. Yu, O. Sinanoglu, and E. F. Y. Young, "Deep learning analysis for split-manufactured layouts with routing perturbation," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 10, pp. 1995–2008, Oct. 2021, doi: 10.1109/TCAD.2020.3037297.
[332] S.-H. Lin, J.-Y. Lee, C.-C. Chuang, N.-Y. Lee, P.-Y. Chen, and W.-L. Chin, "Hardware implementation of high-throughput S-box in AES for information security," *IEEE Access*, vol. 11, pp. 59049–59058, 2023, doi: 10.1109/ACCESS.2023.3284142.
[333] R. Román, R. Arjona, and I. Baturone, "A lightweight remote attestation using PUFs and hash-based signatures for low-end IoT devices," *Future Gener. Comput. Syst.*, vol. 148, pp. 425–435, Nov. 2023, doi: 10.1016/j.future.2023.06.008.
[334] A. A. Khan, S. Bourouis, M. M. Kamruzzaman, M. Hadjouni, Z. A. Shaikh, A. A. Laghari, H. Elmannai, and S. Dhahbi, "Data security in healthcare industrial Internet of Things with blockchain," *IEEE Sensors J.*, vol. 23, no. 20, pp. 25144–25151, Oct. 2023, doi: 10.1109/JSEN.2023.3273851.
[335] T. Zeb, M. Yousaf, H. Afzal, and M. R. Mufti, "A quantitative security metric model for security controls: Secure virtual machine migration protocol as target of assessment," *China Commun.*, vol. 15, no. 8, pp. 126–140, Aug. 2018, doi: 10.1109/CC.2018.8438279.
[336] "Intel demos first 3D stacked CMOS transistors combined with backside power and direct backside contact," in *Proc. 69th Annu. IEEE Int. Electron Devices Meeting (IEDM)*, Santa Clara, CA, USA, Dec. 2023. [Online]. Available: https://videocardz.com/press-release/intel-showcases-3d-stacked-cmostransitor-with-backside-power-and-direct-backside-contact
[337] C. K. H. Suresh, B. Mazumdar, S. S. Ali, and O. Sinanoglu, "A comparative security analysis of current and emerging technologies," *IEEE Micro*, vol. 36, no. 5, pp. 50–61, Sep. 2016, doi: 10.1109/MM.2016.87.
[338] F. Rahman, B. Shakya, X. Xu, D. Forte, and M. Tehranipoor, "Security beyond CMOS: Fundamentals, applications, and roadmap," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 12, pp. 3420–3433, Dec. 2017, doi: 10.1109/TVLSI.2017.2742943.
[339] M. R. Mahmoodi, D. B. Strukov, and O. Kavehei, "Experimental demonstrations of security primitives with nonvolatile memories," *IEEE Trans. Electron Devices*, vol. 66, no. 12, pp. 5050–5059, Dec. 2019, doi: 10.1109/TED.2019.2948950.
[340] T. B. Singha, R. P. Palathinkal, and S. R. Ahamed, "Securing AES designs against power analysis attacks: A survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14332–14356, Aug. 2023, doi: 10.1109/JIOT.2023.3265683.
[341] A. Javeed, C. Yilmaz, and E. Savas, "Microarchitectural side-channel threats, weaknesses and mitigations: A systematic mapping study," *IEEE Access*, vol. 11, pp. 48945–48976, 2023, doi: 10.1109/ACCESS.2023.3275757.
[342] S. Hemavathy and V. S. K. Bhaaskaran, "Arbiter PUF—A review of design, composition, and security aspects," *IEEE Access*, vol. 11, pp. 33979–34004, 2023, doi: 10.1109/ACCESS.2023.3264016.

MAMIDIPAKA B. R. SRINIVAS received the B.Tech. degree in electronics and communication engineering from JNTU Kakinada, India, in 2012, and the M.Tech. degree in VLSI design from the Vignan's Foundation for Science Technology and Research, Andhra Pradesh, in 2016. He is currently pursuing the Ph.D. degree in VLSI design with VIT, Vellore, India.

KONGUVEL ELANGO (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from the Karpagam College of Engineering, Anna University, Chennai, India, in 2010, and the M.E. degree in communication and network engineering and the Ph.D. degree in information and communication engineering from Madras Institute of Technology, Anna University, in 2013. He is currently an Assistant Professor with the School of Electronics Engineering, Vellore Institute of Technology, Vellore, India. His main research interests include VLSI design, signal processing, the Internet of Things, and embedded systems.