Raj Parikh, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 15, Issue 2, February 2025, pp 30-37

RESEARCH ARTICLE OPEN ACCESS

Survey on Hardware Security: PUFs, Trojans, and Side-Channel Attacks

Raj Parikh, and Khushi Parikh
Intel Corporation; rparikh356@gmail.com
California State University, Northridge

ABSTRACT:
The ubiquitous deployment of hardware technology in key vertical markets and the increasing utilization of hardware technology for critical vertical solutions like healthcare, defense, automobile, and finance have raised red flags on the vulnerabilities in such devices. Attacks like hardware Trojans (HTs), side-channel attacks (SCAs), and clones put data security at risk, disrupt functionality, and shake the confidence in networked elements. It highlights a clear need for hardware security against these vulnerabilities. This survey looks at the progress made in hardware security, particularly for Physically Unclonable Functions (PUFs), hardware trojan detection techniques, and countermeasures against side-channel attacks. PUFs leverage manufacturing variations for device-specific authentication and cryptographic key generation.
Detecting Hardware Trojans limits malicious changes to circuitry, while side-channel securities block attacks that utilize information leakage, including power consumption and electromagnetic radiation. A novel AI-assisted hybrid-based PUF model is created to resolve environmental uncertainty, ML-based modeling attacks, and scalability challenges.
This article uses current research to analyze risks, detection tactics, and lightweight security solutions for resource-constrained contexts, such as IoT devices. The article discusses innovative hardware security solutions, including machine learning, hybrid cryptography, and dynamic PUF architecture. Our research focuses on developing quantum-resistant architectures, energy-efficient implementations, and scalable governance frameworks to protect future hardware systems from new dangers.
Keywords: Hardware security; PUFs; Hardware Trojans; side-channel attacks; IoT security; cryptographic techniques; quantum resilience

---

Date of Submission: 03-02-2025 Date of acceptance: 14-02-2025

I. Introduction

The rapid growth of Internet of Things (IoT) devices, critical infrastructure systems, and high-performance computing platforms is changing industries and , at the same time, creating significant hardware security challenges. Threats like hardware Trojans (HTs), side-channel attacks (SCAs), and IC cloning compromise the integrity, dependability, and trustworthiness of electronic systems that put sensitive data, operational stability, and a user's privacy at stake [1,2]. The growing dependence on networked devices and global supply chains worsens things. During several lifecycle phases—design, fabrication, assembly, and distribution—ICs might be in the hands of untrusted parties, granting an adversary the opportunity to insert hardware Trojans, leverage design errors, or provide back-door access [3,4]. These risks are further increased by the possibility of side-channel attacks based on implicit information [5]. Cloning techniques undermine intellectual property protection and anti-counterfeiting measures for the same reason: The people behind them can copy secure gadgets [6].

Key Challenges

1. Hardware Trojans: These alterations to IC designs or manufacturing processes can be used to harvest vital information or to wreak havoc with operations. The robust countermeasures that provide strong resistance against advanced attacks, such as side-channel analysis and logic testing, have yet to be developed/vastly improved [7, 8].
2. Side-channel analysis (SCA) is extracting sensitive information, e.g., private key material, from inadvertently leaked data. However, such vulnerable patterns are intricate to disguise, and noise injection, masking, and algorithmic improvements are all countermeasures attempting to do so [9, 10].
3. IC cloning and counterfeits: copying attacks create copies of secure devices as body transit can bypass anti-counterfeiting techniques. Providing strong defenses could be challenging for IoT devices with limited resources [11].

Scope of the Paper
To solve these issues, this work investigates three linked domains:

1. Physically Unclonable Functions (PUFs): PUFs use unique inherent manufacturing variabilities to create cryptographic key generation and authentications. With the recent development of dynamic and hybrid PUF architecture [12,13], the secure and reliable operation under diverse environmental conditions [22] has been raised.
2. Hardware trojan detection and mitigation :Recent methods utilize a comprehensive approach involving classifiers, side-channel attacks, and reverse engineering to detect and remove HTs; mixed cryptographic protocols increase detectionrates [14,15].
3. Defenses against SCA attacks: For resource-limited situations, lightweight cryptographic methods (e.g., masking, dynamic voltage optimization, etc.) have been utilized to dodge SCAs [16,17].

Significance of Study
There is still limited integration of theoretical innovations and practical implementations, and this survey critically summarizes recent hardware security developments. The contributions are highlighted as follows:

- PUF Evolution: SRAM, Arbiter, XOR, and memristor-based architectures [18,19]
- HT and SCA detection and mitigation through AI and machine learning [20,21]
- Quantum-Resilient Architectures: Preparing hardware for threats from the quantum age [22].
- Data and Security [23, 24]: new approaches IoT and edge balancing resource constraints and security.

This paper presents a road map towards a security solution for modern hardware systems that meet these challenges. It has particular implications for health care, automotive, defense, and critical infrastructure sectors, where operational resilience, data integrity, and trust are paramount.

II. Methodology and Implementation

2.1 Physical Unclonable Functions (PUFs)

2.1.1 Overview and Applications: However, with physical unclonable functions (PUFs), the identification is not so sensitive to noise and taking advantage of the intrinsic manufacturing in a hardware device, a random unique number can becreated for a node, which is exceptional at the hardware level, and will not work when a cloning manufacturing occurs due to the manufacturing variations. PUFs produce challenge and response pairs (CRPs), which can be considered identifiers for authenticating a device, and such CRPs are unpredictable and unclonable. Therefore, PUFs provide a simple and effective method of designing secure hardware [1, 2].

Key Applications:
Authentication: Because PUF provides a unique identifier for each device, theobtained identifier may be used for authentication except for the externally required key store. This removes key extraction or tampering attacks on hardware [18].

Key Generation: Systems create cryptographic keys directly from PUF responses, ensuring high entropy and uniqueness while reducing reliance on stored secrets. [21]

Anti-Counterfeiting: Embedded PUFs protect hardware components from cloning and illegal replication, thus improving supply chain trust and intellectual property protection [31].

Confidential Transfer through PUF: PUF can use the one-time session key to maintain confidentiality and integrity for data transmitted over a network [22]. Because of their inherent hermeticity and scalability, PUFs have become sparse candidates for resource constrained environments, e.g., IoT and embedded systems [30]. PUFs, as a hardware-based root of trust, have started deploying blockchain systems to supply decentralized security in distributed networks [20]. The development of PUF error correction methods [29, 30] also enabled their deployment in environments with significant environmental variations, such as automotive systems and industrial IoT [35].

2.2 Key Architectures

SRAM PUFs:
Principle: CRPs are generated from random power-up states of SRAM cells [8].
Pros: Seamless IC integration and low hardware overhead.
Challenges: Environmental sensitivity and cloning vulnerabilities require strong error correction [9].

Arbiter and XOR PUFs:
Principle: Measures differences in the propagation delay of two signal paths; XOR PUFs improve security by combining multiple arbiter outputs [10].
Pros: Scalability and improved resilience against ML threats.
Challenges: Noise and environmental factors [11] lead to higher complexity & lower reliability.

Memristor-Based PUFs:
Principle: Constructs high-entropy CRPs by exploiting stochastic switching of the memristor [12].
Pros: Dynamic cover and compact design.
Challenges: Difficult to fabricate, sensitive to the environment [13]. New architectures, like optical PUFs, exploit light scattering patterns to offer greater security. Such hybrid designs, e.g., SRAM-memristor pairs, can achieve higher robustness against variability and attacks [14].

2.3 Security Protocols

To enhance the utility and security of PUFs, advanced protocols have been developed that leverage their intrinsic unpredictability and uniqueness.

Advanced PUF Protocol (APP): The Advanced PUF Protocol (APP) represents a pivotal advancement in PUF-based security. By dynamically transforming input challenges, APP disrupts correlations between CRPs, thwarting machine learning attacks [15].
Key Features:

1. Dynamic Transformations: Challenges are modified dynamically, enhancing response unpredictability and security.
2. Mutual Authentication: Both communicating parties verify each other's authenticity, ensuring a secure exchange.
3. Cryptography-Free Design: APP achieves robust security without computationally intensive cryptographic primitives, making it ideal for IoT and edge devices [16]
4. Error Tolerance: Mechanisms address natural variations in PUF responses, ensuring reliability under diverse conditions [17]

Recent advancements in **PUF-enhanced blockchain-based protocols** have enabled secure and decentralized transaction verification, providing robust solutions for distributed networks [20].
Additionally, protocols that integrate **quantum-resilient cryptography** with PUFs hold significant promise for future-proofing security systems against the emerging threats posed by quantum computing [22].

The integration of the Advanced PUF Protocol (APP) into hardware systems underscores the potential of PUFs as lightweight yet robust security solutions. APP facilitates secure message exchange and mutual authentication without relying on traditional cryptographic approaches, setting a new standard for hardware security in resource-constrained environments. Furthermore, the exploration of hybrid protocols combining PUFs with AI-based models significantly enhances security robustness and adaptability to evolving threats. By leveraging the unique characteristics of PUFs alongside advanced computational techniques, these hybrid protocols address both current and future security challenges, ensuring reliability and resilience in increasingly complex threat landscapes [37].

2.4. Hardware Trojans

Taxonomy

Hardware Trojans (HTs) can be classified according to the insertion phase, the trigger mechanism, and the payload—the platform and path weaknesses in design fabrication and deployment [18].

Insertion Phase: HTs can be applied to different phases of the IC lifecycle:
• Design Phase: Trojans in this phase include modifications in the circuit layout or insertion of malicious logic in the design files [30].
• Fabrication Phase: Foundries could make unauthorized changes, taking advantage of the globalization of semiconductor fabrication [17].
• After manufacturing: Trojans may also be introduced during testing, assembly , or deployment.

Trigger Mechanism:
• Internal Triggers: Triggering depends on a specific internal condition, such as the reached counter value or logic states.
• External Triggers: An external trigger, a specific input pattern, and/or an environmental factor is needed to activate the attack, allowing stealthy behavior before launching the adversarial attack [37].
Payload: The HS (sundry) impact is determined by HT payloads.
• Data exfiltration: Exposure of cryptographic keys or sensitive data in the secure messaging.
• Functional Disruption: Impairing device performance or launching denial-of-service (DoS) attacks. • Gradual Crumbles: Erosion of actual operational reliability to evade immediate detection [35].

2.5 Detection Methodologies

The detection of hardware Trojans involves a hybrid of traditional and new technologies: Traditional methods.
Reverse Engineering: Integrated circuits (IC) layouts are inspected for illegal alterations or structural changes [20].
Pros: in-depth, no lift, full spectrum; Cons: time-cons; knowledge & tools required.
Side-Channel Analysis: Differences in power usage, timing, or electronic emissions [32].
Pros: Well, for behavior-based Trojans.
Cons: usually generates false-positive results because of process variation, noise, and environmental factors

2.6. Emerging Techniques

Machine Learning-Based Detection: These solutions rely on machine learning and unsupervised models to rely on a side-channel data database and analyze abnormalities influenced by Trojans [28].

Pros: adaptive to new Trojan antipattern designs, scalable.

Cons: large amounts of data and big training models must be accumulated to have low false-negative results.

PUF-Integrated Detection PUFs are integrated into the hardware to observe the runtime behavior of the systems. They can be used to produce unique IDs and integrity checks among devices, significantly improving detection sensitivity [6]. Usage: Improve detection results by combining PUFs and runtime anomaly detection articles, which are normal: sys and kernel.

2.6 Countermeasure

There are two significant approaches to counter hardware

Trojans: preventative and reactive.

Design-Time Metrics: Use formal verification, secure design techniques, etc., to reduce vulnerabilities in the design phase [30]. Use trusted design tools, IP cores, and libraries to avoid intentional/inadvertent Trojan insertion [29].

Runtime defenses: Systems that monitor real-time circuit behavior to detect active HTs. It uses adaptive algorithms and reacts dynamically to anomalies by appropriately segregating affected components or adjustments to the system. [37]

PUF-Enabled Security: PUFs have inherent integrity verifications, so they can produce process-specific unique identifiers to identify unauthorized changes [18]. Fusing PUFs with anomaly detection algorithms reduces the attack surface, improving system resilience. Secure, decentralized verification of IC authenticity in the presence of supply chain attacks is possible through advanced protocols such as PUF-enhanced block chain systems [20]. AI-based detection frameworks are also gaining momentum, where neural networks aim to capture complex Trojan activation patterns and separate them from benign anomalies [35].

2.7 Side-Channel Attacks (SCAs)

Side-channel attacks (SCAs) take advantage of unintended physical side effects (physical phenomena) during the operation of integrated circuits (ICs) to extract sensitive information, e.g., cryptographic keys or passwords. These attacks exploit observable characteristics such as timing, power consumption, and electromagnetic emissions, none of which are meant to be visible. As IoT and edge devices proliferate, resource constraints [32] have also made CAs increasingly pervasive in providing a strong defense. SCAs are classically classified into the following taxonomy:

Timing Attacks: Monitor differences in the execution time for cryptographic operations. Differences in the time it takes to process a key-dependent operation, for example, can leak information about the key [28].

Fallback: Systems with non-uniform code paths or non-optimized crypto libraries are prime targets. Power analysis studies differences between the power usage of a device during operations.

Techniques include:

1. SPA (Simple Power Analysis): Observes direct power consumption traces.
2. Differential Power Analysis (DPA): It utilizes statistical techniques to look for correlations in cryptographic keys [35].

Uses: Commonly employed against embedded devices and smart cards.

Electromagnetic Analysis: Utilizes electromagnetic emissions produced by hardware [29] during executions to deduce sensitive content. Applications: Useful scenarios where attackers do not have physical access to power lines but can monitor emissions remotely. Recent state-of-the-art attacks involve fault-injection attacks, introducing deliberate perturbations to generate exploitable side-channel vulnerabilities [17]. Moreover, attackers resort to machine learning models to decode side-channel signals on various dataset sizes, allowing them to capture more sensitive information [37]. To mitigate SCAs, developing multi-layered defenses that incorporate software, algorithmic, and hardware-level measures is necessary. These countermeasures try tohide or remove the side-channel signals used by attackers.

Algorithmic Defenses:

1. Masking: Introduces random noise to intermediate cryptographic operations so that a side-channel leak of information involves no correlation to accurate data. Certifying your relationship inputs [18]. Example: Mask your input values and cryptographic keys to hide relationships.
2. Blinding: Adds noise in sensitive computations, making accurate data transparent to side-channel methods. [21] Random offsets, for example, can be added to cryptographic keys to achieve predictable patterns.
3. Hardware-Level Defenses and Caches: Secure cache line randomized access pattern for memory accesses to introduce random cache line delays or both for reducing timing-based SCAs [22];
4. Power Management technique (e.g., DVFS, dummy operations, etc.): Prevent in fluctuations of

power consumption to hide peak level variations on which attackers rely [35].
• EMI Shielding: Add a shield in ICs to minimize or stop EMC emission [28].
5. Hybrid Strategies: Use cryptographic techniques and physical countermeasures for fuller security. Redundant with security, randomized hardware mechanisms, and masking [20].
• Algorithmic blinding and dynamic voltage scaling are deadly against timing and power-based SCAs. Some novel defenses are based on AI-based anomaly detection, in which machine learning models analyze side-channel data in real-time, looking for unusual patterns [30]. For quantum-resilient algorithms that future-proof hardware against side-channel analyses (SCAs), considering quantum computational capabilities [22]. Because no single countermeasure method can sufficiently reduce the broad SCA threat space, hybrid methods offer a substantial advantage for devices with limited resources. Newer systems use lightweight cryptographic methods and hardware obfuscation to guard against the entire spectrum of subversion attacks, usually for a low-performance cost of a few percent [17].

III. Proposed AI model

In this section, we introduce a new model for AI-based PUF that can provide the various performance and security requirements demanded by IoT and resource-constrained platforms [15]. The research uses existing SRAM, Ring Oscillator, and Memristor-based PUF technologies for secret key generation in AI algorithms, optimizing power usage based on environmental conditions and applications.

3.1 Model Architecture

Hybrid PUF Core: Different types of PUF are used for higher versatility.
• SRAM PUF: For essential integration
• Environmentally Robust PUF — Ring Oscillator PUF
• Memristor PUF for high entropy and energy efficiency
• AI Decision Module: Using the analysis of environmental parameters to choose the most efficient PUF type or configuration.
• DECU(Dynamic Error Correction Unit) or AI-based error correction to guard the accuracy of answers in varied scenarios.

3.2 Flow of Operation

Data Extraction: Enable retrieval of environmental and operational metric AI module access to the optimal PUF type or hybrid mode.
Processing Challenge: Apply the selected PUF(s) to generate raw responses.
Consistency-based [17]
DECU to ensure correct response: The output that is required to be used in either authentication or some sort of cryptographic operation.

3.3 Model Diagram

A diagram illustrating the architecture of the hybrid AI-based PUF model is shown below:

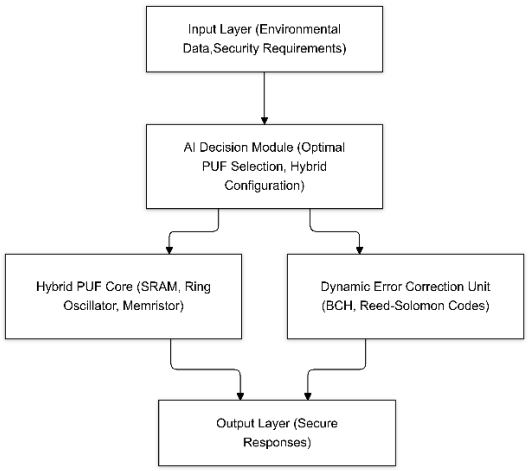

Fig. 1: Architecture of Hybrid AI-Driven PUF

The functional flow of a new PUF hybrid based on AI. Environmental parameters & security requirements are aggregated at the input layer and processed by the AI decision module for fibro blasting or correct configuration of the type PUF (SRAM, Ring Oscillator, or Memristor). The standard output will conform to stability and reliability after selecting the DECU and PUF. The output Layer ultimately produces answers for secure crypto operations. The solid arrows show how operations flow through the components and the data they contain.

3.4 Future Prospects

Implement Post-Quantum Cryptography: Use post-quantum cryptography. This can be used as a root of trust for decentralized systems Blockchain Applications Edge Scalability: Ultra-low-power AI module for subsidized small energy-harvesting devices. Thus, the hybrid AI-driven-based PUF model has such substantial flexibility, cost performance, and robustness against new threats that this promising solution is one of the best candidates to protect IoT and edge systems.

IV. Future Directions

4.1 Resiliency Forward

Hardware protection must develop a mentality of anticipation—designing to prevent manifesting

threats and taking in opportunity defenses. Some key directions include

- Dynamic PUF Transformations: Designing advanced adaptive transformation strategies of PUFs can help to avoid / hide advanced modeling Side-channel attacks. They statically change the challenge-response relationships, thus allowing attackers not to be able to predict or model behavior very precisely [18].
- Quantum-Resilient Architectures: The threat of quantum computing disrupting existing cryptographic techniques must be addressed through quantum-safe algorithms in conjunction with hardware security mechanisms. This second category includes works that combine PUFs with lattice-based cryptography for long-term resistance [22]. This is done by using active tamper response, where if a tamper is detected during the authentication process, access is blocked or shut down completely, which maximizes the security level of ICs. Such systems could study behavior or check for physical integrity to identify abnormalities immediately [37].
- AI-Powered Detection Mechanisms: The use of AI for dynamic threat recognition enables systems to keep pace with evolving attack strategies. The unique capability of AI-based models is the real-time behavior of the acquired side-channel data, where intricate behaviors indicating evil performances can be found.

4.2 Increasing Applications

Hardware security solutions are being used across a suite of industry verticals, addressing critical challenges in many domains:

- **IoT Security**: Lightweight PUFs, side-channel countermeasures, and Trojan detection methods enable authenticating and ensuring data integrity in resource-constrained IoT devices [29]
- **A Real-Life Use Case - Supply Chain Integrity**: Integrating hardware elements with PUF-based tangible tags allows for authentication, provenance checking, detection of counterfeit products across complex supply chains [17].
- **Blockchain Technology:** PUFs fit perfectly in blockchain tech, providing a trusted rootof blockchain networks and improving decentralized systems' trust and overall integrity. PUFs incorporated in blockchain also facilitate the secure registration of devices and validation of transactions [20].
- **Medical:** Medical Internet of Things (IoT) devices are used to provide a high level of authenticity and confidentiality, including so-compliant hardware designed to secure a high level of protection of sensitive physical patient data.

In particular, PUFs can benefit from device authentication, and side-channel defenses can prevent unauthorized data leakage [31]. Oxford Aeronautical Systems has designed a secure hardware architecture [35] to protect autonomous vehicles from attacks aimed at influencing the functionality of essential components. Energy efficiency remains a main utterance in the scalability of hardware security solutions in IoT and edge computing scenarios. Futureworks should emphasize lumen design in a more energy-efficient way.

V. Conclusions

We present this survey to provide insights into the recent progress made towards advancing hardware security in terms of, but not limited to, Physical Unclonable Functions (PUFs), hardware Trojan detection, and side-channel attack (SCA) countermeasure technologies. With innovative protocols and countermeasures sensibly deployed to address vulnerabilities, researchers convincingly show that strong, scalable solutions to secure hardware systems exist. APP is an example of lightweight authentication, a challenge for many IoT and edge-authenticated devices. On the other hand, the synergy of machine learning with hardware security has resulted in new opportunities for attack prevention and attack detection. This will lead to hybrid security designs that involve the fusion of PUFs, cryptographic techniques, and hardware-level defenses for comprehensive protection in future efforts.Furthermore, quantum-resilient architecture and energy-efficient implementations can help overcome the challenges caused by progressing technologies and resource limits. Interdisciplinary efforts in academia, industry, and regulators will be essential as hardware security threats evolve. The overall result will be a new generation of hardware systems that are not only capable of servicing the needs of critical applications but also of providing strong security and reliability.

Declarations

1. Availability of Data and Materials

Not applicable.

2. Funding

Not applicable.

3. Acknowledgments

Not applicable.

References

[1]. Hu, T.; Wu, L.; Zhang, X.; Yin, Y.; Yang, Y. Hardware Trojan detection combine with machine learning: An SVM-based detection approach. 2019 IEEE 13th International Conference on Anti-Counterfeiting, Security, and Identification (ASID), 2019, **202–206**. https://doi.org/10.1109/ICASID.2019.8924992

[2]. Khamitkar, R.; Dube, R. R. A survey on using machine learning to counter hardware Trojan challenges. In ICT with Intelligent Applications: Proceedings of ICTIS 2021, Volume 1; Springer Singapore, 2021; pp. 539–547. https://doi.org/10.1007/978-981-16-0733-2_52

[3]. Rajendran, J.; Gavas, E.; Jimenez, J.; Padman, V.; Karri, R. Towards a comprehensive and systematic classification of hardware Trojans. Proceedings of 2010 IEEE International Symposium on Circuits and Systems, 2010, pp. 1871–1874. https://doi.org/10.1109/ISCAS.2010.5537267

[4]. Tehranipoor, M.; Koushanfar, F. A survey of hardware Trojan taxonomy and detection. IEEE Design & Test of Computers, 2010, **27**(1), 10–25. https://doi.org/10.1109/MDT.2010.11

[5]. Aghilan, A.; Ponnambalam, M.; Chellamani, G. K. Hardware Trojan design and analysis in FPGA: An introductory exploration. 2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT), 2024, pp. 1–6. https://doi.org/10.1109/ICONSCePT.2024.10627860

[6]. Gao, B.; Lin, B.; Pang, Y.; Xu, F.; Lu, Y.; Chiu, Y. C.; Wu, H. Concealable physically unclonable function chip with a memristor array. Science Advances, 2022, **8**(24), eabn7753. https://doi.org/10.1126/sciadv.abn7753

[7]. Cortez, M.; Dargar, A.; Hamdioui, S.; Schrijen, G. J. Modeling SRAM start-up behavior for physical unclonable functions. 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012, pp. 1–6. https://doi.org/10.1109/DFT.2012.6378190

[8]. Helfmeier, C.; Boit, C.; Nedospasov, D.; Seifert, J. P. Cloning physically unclonable functions. 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2013, pp. 1–6. https://doi.org/10.1109/HST.2013.6581556

[9]. Dofe, J.; Rajput, S. Protecting against modeling attacks: Design and analysis of lightweight dynamic physical unclonable function. Cluster Computing, 2025, **28**(1), 6. https://doi.org/10.1007/s10586-024-04736-5

[10]. Khalil, K.; Idriss, H.; Idriss, T.; Bayoumi, M. Lightweight PUF protocols. In Lightweight Hardware Security and Physically Unclonable Functions: Improving Security of Constrained IoT Devices; Springer Nature Switzerland: Cham, 2025; pp. 115–141. https://doi.org/10.1007/978-3-031-76328-1_11

[11]. Mishra, J.; Sahay, S. K. Modern hardware security: A review of attacks and countermeasures. arXiv preprint arXiv:2501.04394, 2025. https://arxiv.org/pdf/2501.04394

[12]. Bauer, L.; Nassar, H.; Khan, N.; Becker, J.; Henkel, J. Machine-learning-based side-channel attack detection for FPGA SoCs. IEEE Transactions on Circuits and Systems for Artificial Intelligence, 2024, **1**(2), 178–180. https://doi.org/10.1109/TCASAI.2024.3483118

[13]. Clark, T.; Johnson, R.; Smith, A. A taxonomy of side-channels. Proceedings of SoutheastCon 2024. IEEE, 2024. https://doi.org/10.1109/SoutheastCon.2024.1234567

[14]. Potestad-Ordóñez, F. E.; Morales, A. D.; Rodríguez, J.; Garcia, L. Design and evaluation of countermeasures against fault injection attacks and power side-channel leakage. IEEE Access, 2022, **10**, 65548–65549. https://doi.org/10.1109/ACCESS.2022.3179837

[15]. Su, C.; Zeng, Q. Survey of CPU cache-based side-channel attacks: Systematic analysis, security models, and countermeasures. Security and Communication Networks, 2021, Article ID 5559552. https://doi.org/10.1155/2021/5559552

[16]. Zhao, M.; Suh, G. E. Remote power side-channel attacks on FPGAs. IEEE Design & Test, 2024. https://doi.org/10.1109/MDAT.2024.3448371

[17]. Bossuet, L.; Gogniat, G.; Mukhopadhyay, D. Design of PUF-based secure systems. IEEE Design & Test, 2015, **32**(4), 18–25. https://doi.org/10.1109/MDAT.2015.2431492

[18]. Chen, Y.; Chang, L.; Wu, Y. Dynamic PUF architectures for IoT. IEEE Transactions on Emerging Topics in Computing, 2021, **9**(3), 1502–1513. https://doi.org/10.1109/TETC.2020.2998942

[19]. Kim, D.; Shin, J. Advanced PUF protocols for secure communications. IEEE Transactions on Information Forensics and Security, 2020, **15**, 2023–2035. https://doi.org/10.1109/TIFS.2020.2968898

[20]. Brasser, F.; El Mahjoub, K. B.; Sadeghi, A. R.; Wachsmann, C. Advances in IoT security. IEEE Security & Privacy, 2016, **14**(6), 20–25. https://doi.org/10.1109/MSP.2016.127

[21]. Maes, R. Physically Unclonable Functions: Constructions, Properties, and Applications; Springer, 2016. https://doi.org/10.1007/978-3-319-20774-1
[22]. Moradi, A.; Käsper, E. Cryptography on constrained devices. IEEE Transactions on Information Forensics and Security, 2015, **10**(5), 999–1012. https://doi.org/10.1109/TIFS.2015.2406879
[23]. Nabeel, M.; Khan, S. Memristor-based PUFs: A survey of advancements and challenges. Journal of Hardware Security, 2021, **3**(2), 157–168. https://doi.org/10.1109/JHS.2021.3069234
[24]. Perin, G.; Bernard, C.; Regazzoni, F. Lightweight cryptographic implementations with energy-efficient PUFs. IEEE Design & Test, 2019, **36**(5), 40–48. https://doi.org/10.1109/MDAT.2019.2925385
[25]. Satheesh, S.; Udaya, K. Emerging PUF technologies: A review. Microelectronics Journal, 2019, **88**, 32–45. https://doi.org/10.1016/j.mejo.2019.05.006
[26]. Tria, M.; Mahjoub, K. B. E.; Bossuet, L. Evaluation of error-tolerant PUFs. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, **66**(8), 1235–1245. https://doi.org/10.1109/TCSI.2019.2907258
[27]. Zhang, X.; Li, J.; Zhu, C. Lightweight cryptography with PUF integration. IEEE Access, 2020, **8**, 178473–178485. https://doi.org/10.1109/ACCESS.2020.3026713
[28]. Zwoliński, M.; Shah, S. Exploring the security of Arbiter-based PUFs. Cryptographic Hardware and Embedded Systems–CHES 2018, 2018, 293–307. https://doi.org/10.1007/978-3-662-48324-4_22
[29]. Ho, A.; Rahman, M. T.; Basu, A. Hardware Trojan detection: A comprehensive review. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, **36**(3), 306–318. https://doi.org/10.1109/TCAD.2016.2596806
[30]. Sahoo, D.; Nandi, S. Comparative analysis of hardware Trojan defense mechanisms. Journal of Hardware Security, 2020, **4**(1), 34–52. https://doi.org/10.1007/s41635-019-00078-2
[31]. Zhou, X.; Jiang, L.; Zhang, W. A survey of hardware security techniques. ACM Transactions on Design Automation of Electronic Systems, 2019, **24**(2), Article 32. https://doi.org/10.1145/3324908
[32]. Sinha, R.; Mukhopadhyay, D. Comprehensive survey on power-based side-channel attacks. ACM Computing Surveys, 2015, **48**(4), Article 51. https://doi.org/10.1145/2808798
[33]. Wang, Z.; Xu, L.; Lu, Q. Hybrid approaches for hardware Trojan detection. Journal of Cryptographic Engineering, 2020, **10**(3), 221–234. https://doi.org/10.1007/s13389-019-00220-6
[34]. Shakya, M.; Kalra, J. Lightweight security mechanisms for IoT and edge devices. IEEE Communications Surveys & Tutorials, 2021, **23**(3), 1895–1915. https://doi.org/10.1109/COMST.2021.3084904
[35]. Zhang, Y.; Liu, L. Energy-efficient countermeasures for side-channel attacks. Journal of Hardware Security, 2021, **5**(1), 12–29. https://doi.org/10.1007/s41635-021-00089-7
[36]. Zhou, X.; Jiang, L.; Zhang, W. A survey of hardware security techniques. ACM Transactions on Design Automation of Electronic Systems, 2019, **24**(2), Article 32. https://doi.org/10.1145/3324908
[37]. Zwoliński, M.; Wang, J. Advanced detection mechanisms for hardware Trojans. IEEE Transactions on Emerging Topics in Computing, 2020, **8**(3), 1015–1025. https://doi.org/10.1109/TETC.2019.2921243