Review

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

Raj Parikh * and Khushi Parikh

Posted Date: 21 January 2025

doi: 10.20944/preprints202501.1559.v1

Keywords: hardware security; PUFs; hardware Trojans; side-channel attacks; IoT security; cryptographic techniques; quantum resilience

Review

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

Raj Parikh [1,*] and Khushi Parikh [2]

[1] Intel Corporation

[2] California State University, Northridge

* Correspondence: rparikh356@gmail.com; Tel.: +1-6692044858

Abstract: The increasing reliance on hardware technologies across critical sectors such as healthcare, defense, automotive, and finance has raised awareness of vulnerabilities in these systems. Threats like hardware Trojans (HTs), side-channel attacks (SCAs), and cloning compromise data security, disrupt operations and jeopardize trust in interconnected systems. Addressing these risks requires robust hardware security mechanisms. This survey provides a comprehensive analysis of advancements in hardware security, focusing on Physically Unclonable Functions (PUFs), hardware Trojan detection techniques, and defenses against side-channel attacks. PUFs leverage manufacturing variations for device-specific authentication and cryptographic key generation. Hardware Trojan detection mitigates malicious modifications in integrated circuits, while side-channel defenses counteract attacks exploiting information leakage like power consumption and electromagnetic emissions. A novel AI-driven hybrid PUF model is proposed to address environmental variability, machine learning-based modeling attacks, and scalability challenges. Drawing from recent studies, this paper categorizes threats, explores detection methodologies, and evaluates lightweight security protocols for resource-constrained environments like IoT devices. Emphasizing machine learning-enhanced detection, hybrid cryptographic techniques, and dynamic PUF designs, it highlights innovations for enhancing hardware security. Future directions include quantum-resilient architectures, energy-efficient implementations, and scalable regulatory frameworks, offering a roadmap to secure next-generation hardware systems against evolving threats.

Keywords: hardware security; PUFs; hardware Trojans; side-channel attacks; IoT security; cryptographic techniques; quantum resilience

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices, critical infrastructure systems, and high-performance computing platforms has transformed industries but introduced significant hardware security challenges. Threats such as hardware Trojans (HTs), side-channel attacks (SCAs), and IC cloning compromise the integrity, reliability, and trustworthiness of electronic systems, posing significant risks to sensitive data, operational stability, and user privacy [1,2].

The increasing reliance on interconnected devices and globally distributed supply chains exacerbates these vulnerabilities. At various stages—design, fabrication, assembly, and distribution—ICs may pass through untrusted entities, creating opportunities for malicious actors to introduce hardware Trojans, exploit design flaws, or enable unauthorized access [3,4]. Side-channel attacks amplify these risks by leveraging unintentional information leakage, such as power consumption or electromagnetic emissions, to extract sensitive data, including cryptographic keys [5]. Similarly, cloning techniques undermine intellectual property protection and anti-counterfeiting measures by replicating secure devices [6].

 doi:10.20944/preprints202501.1559.v1

Key Challenges

1. **Hardware Trojans**: Malicious modifications during IC design or manufacturing can disrupt functionality or extract sensitive information. Advanced detection methods, including logic testing and side-channel analysis, show promise but require further refinement to address sophisticated attacks [7,8].
2. **Side-Channel Attacks (SCAs)**: SCAs exploit unintended data leakage to infer critical information like cryptographic keys. Countermeasures such as masking, noise injection, and algorithmic optimizations aim to obscure exploitable patterns, but balancing security with performance remains challenging [9,10].
3. **IC Cloning and Counterfeiting**: Cloning techniques replicate secure devices, undermining anti-counterfeiting measures. This is especially concerning resource-constrained IoT devices, where robust defenses are difficult to implement [11].

Scope of the Paper

This study explores three interrelated domains to address these challenges:

1. **Physically Unclonable Functions (PUFs)**: PUFs leverage intrinsic manufacturing variations to generate unique identifiers for authentication and cryptographic key generation. Recent innovations, such as dynamic and hybrid PUF architectures, enhance security and reliability under varying environmental conditions [12,13].
2. **Hardware Trojan Detection and Mitigation**: Modern techniques integrate reverse engineering, side-channel analysis, and machine learning to detect and neutralize HTs, with hybrid cryptographic protocols improving accuracy [14,15].
3. **Side-Channel Attack Defenses**: Lightweight cryptographic methods, such as masking and dynamic voltage scaling, are explored to counter SCAs in resource-constrained environments [16,17].

Significance of Study

This paper synthesizes advancements in hardware security, bridging theoretical innovations and real-world applications. It emphasizes:

- PUF Evolution: Advancements in SRAM, Arbiter, XOR, and memristor-based designs [18,19]
- AI Integration: Machine learning for HT detection and SCA mitigation [20,21]
- Quantum-Resilient Architectures: Preparing hardware for quantum-era threats [22].
- Energy Efficiency: Solutions balancing security and resource constraints for IoT and edge devices [23,24].

By addressing these challenges, this study provides a roadmap for securing modern hardware systems. Its findings are particularly relevant to industries where trust, data integrity, and operational resilience are paramount, such as healthcare, automotive, defense, and critical infrastructure.

2. Methodology and Implementation

2.1. Physical Unclonable Functions (PUFs)

2.1.1. Overview and Applications:

Physical Unclonable Functions (PUFs) have emerged as a cornerstone of hardware security, exploiting inherent manufacturing variations to produce unique, device-specific identifiers. These identifiers, represented as challenge-response pairs (CRPs), are inherently unpredictable and unclonable, making PUFs an efficient and lightweight solution for secure hardware design [1,2].

 doi:10.20944/preprints202501.1559.v1

Key Applications:

1. Authentication: PUFs enable secure device-specific authentication without requiring external key storage, minimizing risks of key theft or tampering [18].
2. Key Generation: By deriving cryptographic keys directly from PUF responses, systems achieve high entropy and uniqueness, reducing dependency on stored secrets. [21]
3. Anti-Counterfeiting: Embedded PUFs safeguard hardware components from cloning and unauthorized replication, enhancing supply chain integrity and intellectual property protection [31].
4. Secure Communication: PUFs facilitate one-time session key generation, ensuring data confidentiality and integrity during transmission [22].

The simplicity and scalability of PUFs make them particularly suitable for resource-constrained environments, including IoT devices and embedded systems [30]. PUFs are increasingly integrated into blockchain systems to act as hardware-based roots of trust, enabling decentralized security in distributed networks [20]. Moreover, advancements in PUF error correction techniques have enabled their deployment in environments with significant environmental variability, such as automotive systems and industrial IoT [35].

2.2. Key Architectures

1. **SRAM PUFs:**

   Principle: Utilizes the random power-up states of SRAM cells to generate CRPs [8].

   Advantages: Seamless IC integration and minimal hardware overhead.

   Challenges: Environmental sensitivity and cloning vulnerabilities require robust error correction [9].
2. **Arbiter and XOR PUFs**

   Principle: Measures delay differences in signal paths; XOR PUFs enhance security by combining multiple Arbiter outputs [10].

   Advantages: Scalability and improved resistance to machine learning attacks.

   Challenges: Increased complexity and reduced reliability due to noise and environmental factors [11].
3. **Memristor-Based PUFs**

   Principle: Leverages stochastic switching behavior of memristors for high-entropy CRPs [12].

   Advantages: Dynamic concealment and compact design.

   Challenges: Complex fabrication and environmental sensitivity [13].

Emerging architectures, such as optical PUFs, leverage light scattering patterns for enhanced security. Hybrid designs, like SRAM-memristor combinations, improve 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].

 doi:10.20944/preprints202501.1559.v1

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) are classified by insertion phase, trigger mechanism, and payload. They exploit vulnerabilities across design, fabrication, and deployment stages [18].

1. **Insertion Phase**

HTs can be introduced at various stages of the IC lifecycle:

- Design Phase: Trojans at this stage involve altering the circuit layout or introducing malicious logic within the design files [30].
- Fabrication Phase: Foundries may introduce unauthorized modifications, exploiting the globalization of semiconductor manufacturing [17].
- Post-Manufacturing Phase: Trojans can also be added during testing, assembly, or deployment.

2. **Trigger Mechanism**

- Internal Triggers: Activation is based on specific internal conditions, such as reaching a counter value or particular logic states.
- External Triggers: Activation occurs through external stimuli like specific input patterns or environmental factors, ensuring stealthy behavior until the attack is launched [37].

3. **Payload**

HT payloads determine their impact, which can include:

- Data Exfiltration: Leakage of cryptographic keys or sensitive information during secure communication.
- Functional Disruption: Degrading device performance or causing denial-of-service (DoS) attacks.

 doi:10.20944/preprints202501.1559.v1

- Subtle Malfunctions: Gradual deterioration of operational reliability to avoid immediate detection [35].

2.5. Detection Methodologies

Detecting hardware Trojans requires a combination of traditional and emerging techniques:
Traditional Approaches

1. **Reverse Engineering:** Analyzing IC layouts to identify unauthorized modifications or structural anomalies [20].

Challenges: Time-intensive and resource-heavy, requiring specialized expertise and equipment.

2. **Side-Channel Analysis:** Monitors power consumption, timing variations, or electromagnetic emissions to detect anomalies [32].
   Strengths: Effective for behavior-based Trojans.
   Limitations: Prone to false positives due to process variations and noise.

2.6. Emerging Techniques

1. **Machine Learning-Based Detection:** Utilizes supervised and unsupervised learning models to analyze side-channel data and detect Trojan-induced anomalies [28].
   Advantages: Adapts to evolving Trojan designs and offers scalable detection.
   Challenges: Requires large datasets and robust training models to minimize false negatives.
2. **PUF-Integrated Detection:** Embeds PUFs into hardware to monitor real-time behavior. PUFs generate unique device identifiers and act as integrity checks, enhancing Trojan detection [6].
   Applications: Combining PUFs with runtime anomaly detection offers robust, lightweight solutions for IoT and edge devices [22].

2.7. Countermeasure

Counteracting hardware Trojans involves preventive and reactive measures:

Design-Time Measures: Employ formal verification and secure design practices to minimize vulnerabilities during the development phase [30].

Use trusted design tools, IP cores, and libraries to prevent intentional or unintentional Trojan insertion [29].

Runtime Defenses: Real-time monitoring systems analyze circuit behavior to detect active HTs. Incorporates adaptive algorithms that respond dynamically to anomalies, such as isolating compromised components or reconfiguring the system. [37]

PUF-Enhanced Security: PUFs provide intrinsic integrity checks, generating unique identifiers that highlight unauthorized modifications [18]. Combining PUFs with anomaly detection algorithms further reduces the attack surface and enhances system resilience. Advanced protocols like PUF-enhanced blockchain systems enable secure, decentralized verification of IC authenticity, counteracting supply chain attacks [20]. AI-driven detection frameworks are also gaining traction, employing neural networks to identify complex Trojan activation patterns and distinguish them from benign anomalies [35].

2.8. Side-Channel Attacks (SCAs)

Side-channel attacks (SCAs) exploit unintended physical phenomena during the operation of integrated circuits (ICs) to infer sensitive information, such as cryptographic keys or passwords. These attacks leverage characteristics like timing, power consumption, and electromagnetic emissions, which are not intended to be observable. CAs have become increasingly prevalent with

 doi:10.20944/preprints202501.1559.v1

the growth of IoT and edge devices, where resource constraints often limit the implementation of robust defenses [32]. The taxonomy of SCAs can be classified as follows:

Timing Attacks: Analyze variations in the execution time of cryptographic operations. For instance, differences in processing times for key-dependent operations can reveal information about the key [28]. Challenges: Systems with inconsistent execution paths or poorly optimized cryptographic libraries are particularly vulnerable.

Power Analysis Observes variations in the power consumption of a device during operations. Techniques include:

- Simple Power Analysis (SPA): Observes direct power usage patterns.
- Differential Power Analysis (DPA): Uses statistical methods to identify correlations with cryptographic keys [35].

- Applications: Widely used against embedded devices and smart cards.

Electromagnetic Analysis: Exploits electromagnetic emissions generated by hardware during operations to infer sensitive information [29]. Applications: Useful scenarios where attackers cannot physically access power lines but can monitor emissions from a distance.

Recent advancements include fault-injection attacks, where deliberate perturbations, such as voltage or clock glitches, are introduced to create exploitable side-channel vulnerabilities [17]. Machine learning models are also increasingly used by attackers to analyze large datasets of side-channel signals, enhancing their ability to extract sensitive information [37].

Mitigating SCAs requires implementing multi-layered defenses that integrate software, algorithmic, and hardware-level strategies. These countermeasures aim to obscure or eliminate the side-channel signals that attackers exploit.

Algorithmic Defenses:

1. **Masking:** Introduces random noise into intermediate cryptographic computations, ensuring that leaked side-channel information is uncorrelated with actual data. [18]

   Example: Masking input values and cryptographic keys to obscure relationships.
2. **Blinding:** Adds random values to sensitive computations, hiding real data from side-channel analysis. [21]

   Example: Adding random offsets to cryptographic keys disrupts predictable patterns.

Hardware-Level Defenses:

- **Randomized Caches:** Obfuscate memory access patterns by randomizing cache lines or introducing unpredictable delays, mitigating timing-based SCAs [22]
- **Power Management Techniques:** Implement dynamic voltage scaling or dummy operations to smooth power consumption patterns, masking variations attackers rely on [35].
- **Electromagnetic Shielding:** Incorporate shielding layers into ICs to minimize or render electromagnetic emissions meaningless [28].

Hybrid Approaches:

- Combine cryptographic techniques with hardware defenses for comprehensive protection. Employing masking alongside randomized hardware mechanisms ensures redundancy in security [20].
- Dynamic voltage scaling coupled with algorithmic blinding disrupts both timing and power-based SCAs.

Emerging defenses integrate AI-driven anomaly detection, where machine learning models analyze side-channel data in real-time to identify suspicious patterns [30]. Quantum-resilient algorithms are also being explored to future-proof hardware against SCAs that exploit quantum computational capabilities [22].

 doi:10.20944/preprints202501.1559.v1

Implications: Hybrid approaches are especially valuable for resource-constrained devices, where a single countermeasure may not suffice to address the diverse SCA threat landscape. By leveraging lightweight cryptographic techniques and hardware obfuscation, modern systems can achieve robust security with minimal performance overhead [17].

3. Proposed AI model

Hybrid AI-Driven PUF Model for Context-Aware Security

This section introduces an innovative AI-driven PUF model designed to address the diverse security demands of IoT and resource-constrained systems. By integrating SRAM, Ring Oscillator, and Memristor-based PUFs with AI algorithms, this model adapts dynamically to environmental conditions and specific application scenarios, ensuring optimal performance and security.

3.1. Model Architecture

- Hybrid PUF Core: Combines different PUF types for enhanced versatility.
  - SRAM PUF ensures ease integration.
  - Ring Oscillator PUF provides environmental robustness.
  - Memristor PUF offers high entropy and energy efficiency.
- AI Decision Module: Analyzes real-time environmental data to select or configure the optimal PUF type.
- Dynamic Error Correction Unit (DECU): Employs AI-enhanced error correction, ensuring stable responses under diverse conditions.

3.2. Flow of Operation

1. Input Processing: Collect environmental data and operational parameters.
2. PUF Selection: AI module selects the optimal PUF type or hybrid configuration.
3. Challenge Processing: Generate raw responses via selected PUF(s).
4. Error Correction: DECU ensures response consistency.
5. Response Generation: Final output used for authentication or cryptographic tasks.

3.3. Model Diagram

- The architecture of the hybrid AI-driven PUF model is illustrated in the diagram below:

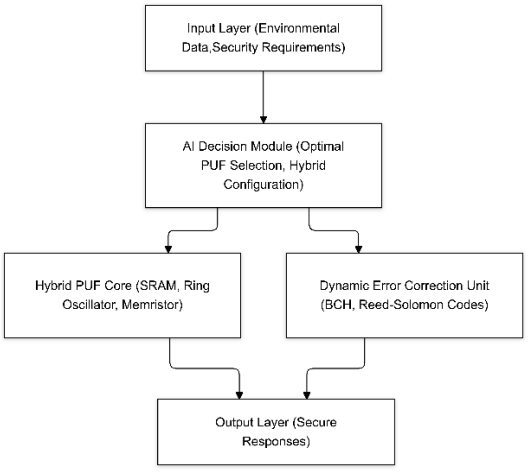

Figure 1. Hybrid AI-Driven PUF Model Architecture.

 doi:10.20944/preprints202501.1559.v1

The diagram illustrates the functional flow of the AI-driven hybrid PUF model. The Input Layer collects environmental parameters and security requirements, which are processed by the AI Decision Module to select or configure the optimal PUF type (SRAM, Ring Oscillator, or Memristor). The selected PUF processes input challenges, while the Dynamic Error Correction Unit (DECU) ensures stable and reliable responses. Finally, the Output Layer generates secure responses for cryptographic operations. Solid arrows indicate the data and operational flow between the components.

3.4. Future Prospects

1. Quantum-Resilient Integration: Incorporate post-quantum cryptography.
2. Blockchain Applications: Use as a root of trust for decentralized systems.
3. Edge Scalability: Design ultra-low-power AI modules for energy-harvesting devices.

The hybrid AI-driven PUF model shows exceptional adaptability, efficiency, and resistance to modern threats, making it ideal for securing IoT and edge systems.

4. Future Directions

4.1. Enhancing Resilience:

The evolution of hardware security must anticipate and address emerging threats through innovative design and proactive countermeasures. Key directions include:

- **Dynamic PUF Transformations:** Developing complex, adaptive transformation mechanisms for PUFs can combat advanced modeling and side-channel attacks. These transformations dynamically alter challenge-response relationships, making it exceedingly difficult for attackers to predict or model behavior [18].
- **Quantum-Resilient Architectures:** As quantum computing becomes a tangible threat to cryptographic systems, integrating quantum-safe algorithms with hardware security mechanisms is critical. Hybrid designs combining PUFs with lattice-based cryptography ensure long-term resilience [22].
- **Integrated Tamper Detection:** Embedding active monitoring systems within ICs to detect and respond to physical tampering in real-time enhances security. Such systems could utilize behavioral analysis or physical integrity checks to flag anomalies immediately [37].
- **AI-Driven Detection Mechanisms:** Incorporating AI for dynamic threat detection enables systems to adapt to evolving attack strategies. AI-based models can analyze side-channel data in real-time to identify complex patterns indicative of malicious activities. [30]

4.2. Expanding Applications

The applications of hardware security solutions continue to grow, addressing critical needs across diverse domains:

IoT Security: Lightweight implementations of PUFs, side-channel defenses, and Trojan detection mechanisms ensure secure authentication and data integrity in resource-constrained IoT devices [29]

Supply Chain Integrity: Embedding PUF-based tags in hardware components authenticates devices, verifies provenance, and prevents counterfeiting across complex supply chains [17].

Blockchain Technology: PUFs can serve as secure roots of trust within blockchain networks, enhancing the integrity and reliability of decentralized systems. Combining PUFs with blockchain also facilitates secure device registration and transaction validation [20].

 doi:10.20944/preprints202501.1559.v1

Healthcare: In medical IoT devices, hardware security mechanisms protect sensitive patient data, ensuring both authenticity and confidentiality. For example, PUFs can verify device identities, while side-channel defenses prevent unauthorized data access [31].

Automotive Systems: Secure hardware architectures are essential for protecting autonomous vehicles from malicious intrusions, ensuring the safety and reliability of critical components [35].

Energy efficiency remains a critical challenge in scaling hardware security solutions for IoT and edge computing environments. Future research must prioritize energy-optimized designs:

5. Conclusions

This survey highlights significant advancements in the field of hardware security, focusing on Physical Unclonable Functions (PUFs), hardware Trojan detection, and side-channel attack (SCA) countermeasures. By addressing vulnerabilities through innovative protocols and countermeasures, researchers have demonstrated that robust, scalable solutions for securing hardware systems are achievable.

Protocols such as the Advanced PUF Protocol (APP) exemplify the potential for lightweight yet secure authentication mechanisms, particularly for IoT and edge devices. Meanwhile, the integration of machine learning with hardware security has opened new avenues for detecting anomalies and preventing sophisticated attacks.

Future efforts should prioritize hybrid security designs that integrate PUFs, cryptographic techniques, and hardware-level defenses to offer comprehensive protection. Additionally, quantum-resilient architecture and energy-efficient implementations are essential to address the challenges posed by emerging technologies and resource constraints.

As hardware security threats evolve, interdisciplinary collaboration between academia, industry, and regulatory bodies will be crucial. This collective effort will ensure that the next generation of hardware systems is equipped to meet the demands of critical applications while maintaining robust security and reliability.

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