Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(4), 197-209
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Survey on AI-Augmented Secure RTL Design for Hardware Trojan Prevention

Raj Parikh, Khushi Parikh

Altera Corporation, San Jose, USA
Email: rparikh356@gmail.com

How to cite this paper: Parikh, R. and Parikh, K. (2025) A Survey on AI-Augmented Secure RTL Design for Hardware Trojan Prevention. *Journal of Computer and Communications*, **13**, 197-209.
https://doi.org/10.4236/jcc.2025.134013

Received: March 18, 2025
Accepted: April 25, 2025
Published: April 28, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Once, discreet circuit elements, called components, were heaped up on boards inside steel cages using wire-lead technology in just five short years. Fast forward to today, and your computer CPU fits about half an inch square on a chip. Both this constant miniaturization of electronic circuits and the rapid growth in the prevalence of third-party intellectual property parts have made hardware protection more worrisome than ever. Among all these issues, Hardware Trojans (HTs)—which represent corrupted or harmful additions during various design and fabrication stages—pose significant threats to system integrity, privacy of data, and essential infrastructure. This survey gives an in-depth look at how AI can enhance RTL security. It classifies these AI-based techniques into four main categories: GNNs, for instance, can be used to estimate the topology of circuits, extract structural characteristics, and thus find where some corruption has occurred. The SALTY framework applies Jumping-Knowledge GNNs to improve the accuracy location for hardware Trojans. Deep Learning in Side-Channel and Power-Analysis Techniques: Deep learning methods—such as Siamese Neural Networks (SNNs) and Long Short-Term Memory (LSTM) models—have been developed to detect abnormalities brought about by Trojans in power consumption or electromagnetic (EM) radiation, granting non-invasive practices clear security benefits. In conjunction with AI, research teams are now building nearest-neighbor classifiers and decision trees and using reinforcement learning (RL) to recognize occurrences of Trojans inside RTL code. Some research uses Verilog/VHDL conditional statements as features for ML, making it possible for early warning signals to be effectively detected and introducing a proactive security mechanism during the design phase. A step-by-step methodology has evolved for prevention measures such as logic locking and layout hardening, which aims against a splendid prospect within reach. The TroLLoc framework uses logic obfuscation combined with security-aware placement and routing, thus mitigating security exposures post-design.

Keywords

Logic Locking, Deep Learning in Power Analysis, Siamese Neural Networks (SNNs), Jumping-Knowledge GNNs, Verilog/VHDL Code Analysis

1. Introduction

The globalization of the integrated circuit (IC) supply chain has brought significant challenges to the security and trustworthiness of hardware. Adopting the fabless semiconductor model, in which companies outsource design, fabrication, and verification to third parties, further increases the risk of malicious alterations in the form of hardware Trojans (HTs) [1].

Hardware Trojans are low-profile changes to circuit design that can infiltrate sensitive data, sabotage system performance, or, in extreme cases, endanger the security of vital national infrastructure such as defense, health, traffic, and finance [2].

The complexity of modern IC designs and the widespread use of third-party IP cores pose further difficulties in detecting hardware Trojans. Traditional methods such as rule-based design verification (e.g., LVS and DRC checks), side-channel analysis, and functional testing have limitations: scalability issues and high false positives or negatives rates. They are also ill-equipped to deal with continuously evolving attack vectors [3].

Researchers are now using AI and machine learning (ML) techniques to generate new tools for design verification. Among these are Graph Neural Networks (GNNs), Siamese Neural Networks (SNNs), reinforcement learning (RL), and explainable AI (XAI), all to identify and mitigate Trojans [4].

This paper divides the AI-based RTL Security Methodology into four broad camps, each with its vigorously implemented badge:

Graph-based detection techniques, which identify vulnerabilities from signal power levels.

Power side-channel analysis featuring opportunities for greater power use.

RTL machine learning models are designed to find and model new threats before they become real.

Proactive logic locking mechanisms, as well as encrypting and decrypting keys.

Through a thorough investigation and comparison of existing research on AI-based detection frameworks for Trojans, this paper aims to highlight some key difficulties, discuss recent advances in research, and suggest future research directions for buttressing data-security methods in upcoming generations of semiconductors.

1.1. Key Challenges

Scalability and Complexity: It's impractical to verify modern ICs with billions of transistors manually. Many AI methods are not very good at this scale, mainly

when they rely on deep neural networks as the learning models and graph theory as a coordination mechanism.

False Positives and Detection Accuracy: Traditional functional verification methods, such as those used in side-channel analysis, are no guide for distinguishing between benign circuit variation and real Trojans because of the broad range of disturbances caused by today's design techniques. If AI fraud measures are to work, they can have just two attribute sensitivity, or operational drawbacks.

Golden Model Dependency: Many current approaches assume you always have a 'golden' reference IC. However, COTS components off the shelf do not provide global wiring as stated. Colleagues are testing AI methods using self-referencing side-channel analysis and dynamic post-processing ML models.

Adaptive Hardware Attacks: Evading Trojans are forever improving. They repeatedly fool detection systems using low-power triggers, dynamic activation schemes, and hidden gates, requiring AI models to adjust in real-time for even the tiniest alteration or distortion.

Security of Logic Locking Techniques: There are specific difficulties with existing logic locking and layout hardening methods. They preclude the insertion of Trojans directly into a chip. Still, according to recent research uncovered by some of our colleagues here at Columbia University, such chips have proven leaky in an embarrassingly short time. Furthermore, an AI-based testing framework should evaluate how well these protective devices operate and what can be done to improve them.

1.2. Scope of Paper

These methods contain a class of techniques based on AI content examination, including the following few:

Graph-Based Hardware Trojan Detecting Method

For (Jumping Knowledge) GNN-SALTY is a programmable RTL security model relying on Graph Neural Networks [2]. Graph-based features represent the geographical orientation of infected nodes in IC layouts and network volumes [5].

AI and Side-Channel Analysis for Hardware Security

Deep learning techniques, such as Siamese Neural Networks and LSTMs (Long Short-Term Memories), are deployed in compromised ICs to identify power or EM signal anomalies [6] [7]. Methods using self-reference to lessen the reliance on the Golden chip [3].

Machine Learning for RTL Code Analysis Programs

Machine Learning performed RTL verifying based on various principles, such as K-nearest neighbor classifiers, decision trees, and reinforcement learning [6]. In feature engineering, IP verification methods with Verilog/VHDL code scanning are also known as Hardware Trojan Detection [8].

Logic Locking and Secure ICs

Logic obscuration and security-aware placement/routing combined in the TroLLoc Framework [9]. AI-powered vulnerability assessments can help locate

the weak points in locked circuits and exposed data hazards [5].

1.3. Significance of Study

This research results are significant for trust, data integrity, and business continuity. Therefore, it is essential to improve this technology in industries concerned with these problems—automobile manufacturing, aerospace, healthcare information systems (for both general practitioners and family planning secrets), etc.—as well as government organizations such as intelligence departments and the NSA.

Significant contributions of this report included:

Combining new theory with concrete applications

This article unifies some of the basic research on PUF that has been done in recent years. It also examines how to implement practical security in this new era with artificial intelligence and related technology and realize and realize quantum-resistant architectures [10].

Promoting AI-driven security solutions

The paper is testing the performance of AI-based detection algorithms. It examines the effectiveness of machine learning defense models for things like protecting against side-channel attack satellite transmissions or hardware Trojan horses [6]. It also considers how monitoring equipment can best combat the problem of pirates stealing your intellectual property.

2. Content Reviewed and Recent Works

As for the methods of Hardware Trojans detection

Researchers have made innumerable attempts to detect and remedy hardware trojans (HTs). The earliest methods attempted to use are functional verification, circuit design analysis, and formal verification. Each of these had limitations:

A. They could not find non-functional trojans, B. needed exhaustive manual analysis to get program information and relied upon frame models [11].

Although this resulted in efficiency improvements and greatly enhanced scalability, machine learning (ML) and artificial intelligence (AI) are still evolving.

A typical early AI-based detection model, GNN4, used Graph Neural Networks (GNNs) to automatically extract RTL security and targeting features, etc. [12]. Other works used deep learning techniques, such as Siamese Neural Networks (SNNs) associated with Side Channel Analysis, plus the use of Long Short-Term Memory (LSTM) Models to track power and EM signatures corresponding to hardware trojans [6].

More recently, GNN4HT has extended its range from FPGAs to gate-level and RTL designs. This addressed situations where class similarity was significant, and data augmentation was limited [13].

New AI-augmented Safety in RTL and Gate-Level Designs

Explainable AI (XAI) is a recently developed technology with promise, especially in hardware Trojan localization and security-aware anomaly detection.

Some results under the SALTY framework use Jumping-Knowledge (JK) GNNs to extract patterns, thereby improving resolution for trojans [2].

ML-based detection frameworks, such as SVM, decision trees, and reinforcement learning (RL), have applied RTL-level verification, extracting security-sensitive patterns from conditional statements in Verilog/VHDL [11].

Another advancement is ML models' self-referencing and dynamic post-processing, substituting for golden reference chips, thus allowing non-destructive Trojan detection in commercial off-the-shelf (COTS) components [3].

New Methods of Hybrid Cryptography: Various methods are now being researched to protect secure silicon architectures from attacks such as authentication tricks or Trojans. These include physically unclonable function-based encryption (PUFs).

Logic Locking and Hardware Security Reinforcement: To counteract hardware Trojan insertion or other invasive methods of attack from attackers, trickery during the design stage increases the difficulty for them [3]. The TroLLoc framework integrates secure placement/routing with logic obfuscation to reduce on-die security traps after design [4].

Recent studies note potential flaws in logic locking techniques, such as key recovery attacks and accidental data leakage risks [5].

AI-assisted vulnerability assessments are being developed to evaluate the effectiveness of logic-locking mechanisms.

AI-Based Hardware Security's Challenges

Despite advances, several challenges remain:

Scalability: Existing models must scale to large IC designs with billions of transistors [14].

False Positives: High detection model sensitivity causes false alarms, complicating the differentiation between benign and malicious changes [11].

Adaptive Hardware Attack: Evolving stealthy Trojan designs demand adaptive, self-learning AI models [13].

AI Model Safety: AI-based security mechanisms are vulnerable to attacks, highlighting the need for robust, attack-resilient AI frameworks [15].

3. Methodology and Implementation

Actionable Implementation Guidelines

Graph-Based Hardware Trojan Detection: Convert RTL designs into netlists and extract structural features such as gate connectivity and logic dependencies. Train GNN-based models using labeled datasets containing both Trojan-infected and clean circuits. Compare detection performance using accuracy, precision, and false positive rate metrics. Integrate the trained model into electronic design automation (EDA) tools for continuous RTL security monitoring.

AI and Side-Channel Analysis: Capture power traces and electromagnetic emissions from ICs during operation. Use Siamese Neural Networks (SNNs) to distinguish between Trojan-infected and standard power signatures. Validate de-

tection accuracy through statistical analysis and ROC curves.

Machine Learning for RTL Code Verification: Extract features from Verilog/VHDL code, including conditional statements and signal dependencies. Train classifiers such as decision trees and nearest-neighbor algorithms for RTL anomaly detection. Integrate ML-based verification into RTL synthesis workflows to detect modifications early in the design phase.

Logic Locking and Secure IC Design: Use XOR-based logic locking to prevent unauthorized modifications. Securely store encryption keys to avoid key-recovery attacks. Assess resistance to Boolean SAT-based attacks using sensitivity analysis.

1. Applying GNN to Hardware Trojan Detection Techniques

Machine learning techniques, such as graph neural networks (GNNs), have been widely acclaimed for their effectiveness in HT detection due to their ability to simulate complex interactions in a circuit netlist. [9] To uncover potential Trojan occurrences, GNN effectively represents the circuit as a graph—where nodes are circuit components (e.g., gates, registers) and edges are the connections between them. Typical structures linking activities indicative of Trojan behavior can be captured almost effortlessly.

A. **Representation of Circuits Based on GNN:** Because netlists have a non-2D structure, traditional Convolutional Neural Networks (CNNs) can find this difficult. By constructing a graph-based representation for circuit layout, GNNs can overcome this problem. The gate-level netlist is first translated into a graph with attributes such as gate connectivity, signal path, logic allocation, etcetera. The graph construction proceeds in these steps:

- Extract all individual parts of the circuit and their interconnections.
- Represent the gates as nodes v and connections between them as edges e.
- Assign the node attribute values: gate kind, fan-in/out ratios, and logic depth.

Mathematically, the propagation rules of a GNN layer can be described as:

$$h_i^{(l+1)} = \sigma\left(W^{(l)} \sum_{j \in N_{(i)}} \alpha_{ij} h_i^{(l)}\right) \tag{1}$$

where:

$h_i^{(l)}$ represents the node feature at layer l,

$W^{(l)}$ is the learnable weight matrix,

σ is the activation function,

$N_{(i)}$ is the neighborhood of node iii,

α_{ij} is the attention coefficient computed as:

$$\alpha_{ij} = \exp\left(\text{LeakyRe}\left(v^{\mathrm{T}}\left[Wh_i \,\|\, Wh_j\right]\right)\right) \Big/ \sum_{k \in N_{(i)}} \exp\left(\text{LeakyReLU}\left(v^{\mathrm{T}}\left[Wh_i \,\|\, Wh_k\right]\right)\right) \tag{2}$$

This approach enables **feature propagation across circuit elements**, aiding **efficient anomaly detection** in netlists [2].

2. Side-Channel and Power Analysis-Based Detection

In addition to these traditional approaches, deep learning models like Siamese Neural Networks (SNNs) and Long Short-Term Memory (LSTM) networks are used more frequently for Side-Channel Analysis (SCA). These technologies devi-

ate from normal circuit behavior by analyzing power consumption and electromagnetic (EM) emissions, which might as well be on their radar screen.

B. Signal Processing and Feature Extraction: During regular operations and with a Trojan infection, these power traces from a circuit are collected. After that, statistical and machine learning algorithms are used to extract all sorts of features related to abnormal activity.

$$P(t) = V(t) \cdot I(t) \tag{3}$$

where:

$V(t)$ is the instantaneous voltage,

$I(t)$ is the instantaneous current.

C. Machine Learning-Based Power Classification: After extracting features, one may train a Siamese Neural Network to classify Trojan and non-Trojan power patterns. The SNN objective function is Siamese Neural Network Objective Function.

$$L = \sum_{i=1}^{n} y_i \left\| f(x_i) - f(x_j) \right\|^2 + (1 - y_i) \max\left(0, m - \left\| f(x_i) - f(x_j) \right\|\right)^2 \tag{4}$$

where:

x_i, x_j are input feature vectors,

y_i is the similarity label,

$f(x)$ is the feature extractor,

m is a margin parameter.

This method achieves high accuracy in detecting power anomalies caused by Trojan insertions [11].

3. Logic Locking and Secure RTL Design

To prevent hardware Trojan insertion, logic locking and layout hardening techniques are used [9]. The TroLLoc framework integrates logic obfuscation with secure placement and routing, making it difficult for attackers to insert malicious modifications post-design [5].

A. **XOR-Based Logic Locking**: One widely used type of logic locking is XOR/XNOR-based obfuscation. Under this technique inserts key-controlled gates into a design so only the correct key can give forth normal behavior. The logic equation for a locked gate is as follows.

$$Y = (A \oplus K_1) \cdot (B \oplus K_2) \tag{5}$$

where:

K_1, K_2 are secret keys, A, B are logic inputs, & Y is the locked output.

3.1. Path Sensitization for Security Evaluation Path sensitization techniques

are used to evaluate the security of logic locking. Through ATPG the secure outputs of a locked circuit will remain unpredictable unless the correct key is put in [8]. Not all locked circuits will be this secure, however.

$$D = \sum_{i=1}^{n} S_i P_i \tag{6}$$

where:

S_i is the sensitivity function, & P_i is the probability of leakage for key bit *i*.

Security evaluations determine the resilience of locked circuits against key-recovery attacks by analyzing these constraints [10].

4. AI-Driven Security Enhancements

4.1. Federated Learning for Secure IC Verification

Federated learning allows AI models to be trained across multiple fabs without exposing proprietary design data [15]. The federated learning model aggregation rule is

$$\theta_t = \sum_{i=1}^{n} \left(m_i / M \right) \theta_i \tag{7}$$

where:

θ_t is the global model, m_i is the number of samples at fabrication site *i*, & M is the total dataset size.

This guarantees secure and private updates for AI-driven Trojan detection, allowing continuous safety improvement without losing data confidentiality.

5. AI-Augmented Routing Security

To suppress crosstalk, electromagnetic (EM) leakage, and side-channel attacks on the system, a constrained shortest-path algorithm is employed for secure routing driven by AI.

$$C = \sum_{(u,v)\in P} w(u,v) \tag{8}$$

where:

P represents all possible paths, & $w(u,v)$ is the routing cost, considering wirelength, congestion, and security risks.

The security-aware routing optimization function is:

where:

$$S = \min\left(\alpha C + \beta S \right) \tag{9}$$

S represents side-channel vulnerability, & α, β are weighting coefficients that balance performance and security.

This AI-driven routing framework ensures secure signal transmission while minimizing susceptibility to hardware Trojans and side-channel attacks [7].

Evaluation and Performance Analysis

A. Performance Metrics of the Model: The effectiveness of AI-based hardware Trojan (HT) detection models can be assessed by a range of classification metrics, including accuracy, precision, recall (true positive rate—TPR), false positive rate (FPR), F1-score, and area under the curve (AUC) [1]. The expressions for these are:

Accuracy:

Accuracy = (TP + TN)/(TP + TN + FP + FN).

Precision:

Precision = TP/(TP + FP).

Recall (TPR):

Recall = TP/(TP + FN).

False Positive Rate (FPR):

FPR = FP/(FP + TN).

F1-Score:

$$\mathrm{F1} = 2 \times \left(\mathrm{Precision} \times \mathrm{Recall}\right) / \left(\mathrm{Precision} + \mathrm{Recall}\right) \tag{10}$$

For the efficiency of Graph Neural Networks (GNNs) and machine learning detection models, these metrics were applied to multiple datasets from Trust-Hub benchmarks [2] [11].

Evaluation of Strategy of Cases

A three-tiered strategy was adopted in the evaluation process of AI-powered detection models:

Case I: Machine Learning-Based Classification

The decision tree model was trained on the netlist features extracted and employs an approach based on the nearest neighboring [1]. The expression represents it:

$$y(x) = \mathrm{DECISION\ TREE}\left(x, \mathrm{Nearest\ Neighbour}\left(x, D\right)\right) \tag{11}$$

This case showed an improvement of ~5% in accuracy over traditional feature-based classification methods [3].

Case II: Graph-Based Trojan Detection

In RTL designs, Graph Neural Network (GNN) classification was employed to analyze circuit relationships and to detect malicious tampering [13]. We have:

$$y = f\theta(x) \tag{12}$$

where y denotes the predicted output, $f\theta$ represents the deep learning model, and x is the extracted netlist feature vector.

This method improved false positive reduction by 12% and significantly enhanced detection sensitivity for unknown Trojan types [12] [14].

Case III: Node-Level Classification with GNNs

With the development of this method, instead of classifying entire netlists, it is now possible to identify each infected node based on its power characteristics. As a result, we see that in the SoftMax activation function employed here with Graph Convolutional Network (GCN), the classification can be expressed as follows:

$$\hat{y} = \mathrm{GCN}(x) \tag{13}$$

where $\hat{y}$ is the classified node label and x represents node embeddings.

This approach successfully identified Trojan locations within netlists with an accuracy of ~98%, making it superior to traditional machine learning-based detection techniques [5] [15].

Side-Channel and Power Analysis Evaluation

Siamese Neural Networks (SNNs) were used for side-channel and power analysis. While they do not directly attack the chip, rather than their physical effects on power consumption cycles, one useful thing about SNN is that it is free from computationally intensive calculations to generate power cycle versions of on-chip waveforms. The classification function is:

$$IG_x(x) = \left(x_{fi} - x'_{fi}\right) \times \int_0^1 \partial F\left(x' \times \alpha\left(x - x'\right)\right) / \partial x_{fi} \, \mathrm{d}\alpha \tag{14}$$

where $F(x)$ **is** the model output and α is a scaling factor.

This method achieved:

- **98% accuracy in power-based anomaly detection**
- **Reduced dependency on golden-chip models** [11].

Logic Locking Security Assessment

The security of different logic-locking technology, such as XOR-based obfuscation, was evaluated in light of how resistant they were to key recovery attacks. Path sensitization techniques were also used when assessing the extent to which there was a danger of leakage from a key:

$$D = \sum_1^n S_i P_i \tag{15}$$

where S_i is the security sensitivity function and P_i is the probability of a successful attack [5].

This study found that traditional XOR-based methods were vulnerable to Boolean SAT-based attacks, while TroLLoc (Logic Locking + Layout Hardening) improved security resilience by 43% [9].

Secure AI-Driven Routing Optimization

In this research, to prevent signal leakage and Trojan insertion in IC routing, an AI-driven constrained shortest-path optimization was put:

$$C = \sum_{(u,v)\in P} w(u,v) \tag{16}$$

where P represents possible paths, and $w(u,v)$ accounts for wire length, congestion, and security risks.

Results showed:

- 27% improvement in security-aware routing efficiency.
- Lower susceptibility to electromagnetic (EM) side-channel attacks [7].

4. Limitations and Constraints

Vulnerability to Adversarial Attacks: AI models can be misled by carefully crafted adversarial inputs. Robust techniques, such as adversarial training, must be explored to enhance resilience.

Computational Overhead: Deep learning-based security measures introduce significant computational requirements, increasing verification time and hardware complexity.

Dependency on Golden Models: Many detection approaches assume the availability of a trusted reference IC, which is often impractical for commercial off-the-shelf (COTS) components.

Scalability Challenges: AI-driven security frameworks must scale effectively for large IC designs containing billions of transistors.

Trade-Offs and Pitfalls

Accuracy vs. Performance: More complex AI models generally yield higher accuracy but at the cost of increased latency and computational power.

False Positive Rates: Overly sensitive models may flag benign variations as potential threats, necessitating extensive validation to reduce false alarms.

Energy Consumption: AI-enhanced verification methods can impose higher power consumption during training and deployment phases.

5. Conclusions

This paper introduces an artificial intelligence-driven method for locating and preventing hardware Trojans at the various phases of IC design. The main findings are as follows:

Graph Neural Networks (GNNs): Offer Trojan-infected node localization capabilities with an accuracy of as high as 98%, making them superior to all types of machine learning models temporarily used for other purposes [13].

AI-assisted side-channel analysis: Utilizing Siamese Neural Networks (SNNs) can sense power leakage and electromagnetic radiation produced by HTs. The True Positive Rate (TPR) of the anomaly detected in this way is 98 percent [6].

Logic Locking Techniques: TroLLoc (Dual Technique for Logic Locking and Layout Hardening) can raise the average success rate by 43% compared to prevention [9].

AI-embedded routing optimization: Can lower susceptibility to signal leakage while making these systems more resistant to electromagnetic side-channel attacks than ever [7].

Federated Learning-based Security frameworks: Allow secure multi-party IC verification without sacrificing design confidentiality, thus showing up supply chain security [16].

This paper offers:

A comprehensive hardware Trojan detection scheme based on artificial intelligence, incorporating AI to deliver low-cost detection and location results.

An in-depth evaluation of these latest AI models, giving their comparative accuracy, scalability, and robustness against adversarial attacks.

A hardware security strategy for the future based on AI, including its concentration on architectures immune to quantum attacks, the use of adversarial training methods, and approaches to federated learning.

Future Horizons

For the next phase of research, we should take account of the following trends:

1. A cryptographic architecture combining post-quantum encryption with PUFs.

2. Real-time AI adversarial training to counteract covert Trojan attacks.

Integration with cloud-based EDA platforms for scalable and distributed security verification.

3. Establish a framework for detecting AI-powered anomalous behavior on a post-silicon level.

This research lays the foundation for next-generation hardware security solutions, built on the latest advances in AI and cryptography. These advancements

contribute to the credibility of semiconductor security, making them viable for critical applications such as defense and healthcare. Instead, they will be equally worthy today in autonomous cars tomorrow, serving on all fronts!

Acknowledgements

I would like to acknowledge the authors of the numerous research papers referenced in this paper, whose contributions have significantly advanced the field of RTL design in FPGA and ASIC.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Chattopadhyay, A., Bisariya, S. and Sutrakar, V.K. (2025) Identification of Hardware Trojan Locations in Gate-Level Netlist Using Nearest Neighbour Approach Integrated with Machine Learning Technique. arXiv: 2501.16347. https://doi.org/10.48550/arXiv.2501.16347

[2] Mahfuz, T., Gaikwad, P., Suha, T., Bhunia, S. and Chakraborty, P. (2025) SALTY: Explainable Artificial Intelligence Guided Structural Analysis for Hardware Trojan Detection. arXiv: 2502.14116. https://doi.org/10.48550/arXiv.2502.14116

[3] Parikh, R. and Parikh, K. (2025) Survey on Hardware Security: PUFs, Trojans, and side-Channel Attacks. Preprints. https://doi.org/10.20944/preprints202501.1559.v1

[4] Sengupta, A., Anshul, A., Chourasia, V. and Bhui, N. (2025) Security Vulnerability (Backdoor Trojan) during Machine Learning Accelerator Design Phases. *IT Professional*, **27**, 65-72. https://doi.org/10.1109/mitp.2024.3519632

[5] Reimann, L.M., Rezunov, E., Germek, D., Collini, L., Pilato, C., Karri, R. and Leupers, R. (2025) The Impact of Logic Locking on Confidentiality: An Automated Evaluation. arXiv: 2502.01240. https://doi.org/10.48550/arXiv.2502.01240

[6] Nasr, A., Mohamed, K., Elshenawy, A. and Zaki, M. (2024) A Siamese Deep Learning Framework for Efficient Hardware Trojan Detection Using Power Side-Channel Data. *Scientific Reports*, **14**, Article No. 13013. https://doi.org/10.1038/s41598-024-62744-2

[7] Parikh, R., & Parikh, K. (2025) AI-Driven Security in Streaming Scan Net-Works (SSN) for Design-for-Test (DFT). Preprints. https://doi.org/10.20944/preprints202503.0503.v1

[8] Fan, R., Tang, Y., Sun, H., Liu, J. and Li, H. (2024) An Efficient ML-Based Hardware Trojan Localization Framework for RTL Security Analysis. 2024 *ACM/IEEE 6th Symposium on Machine Learning for CAD* (*MLCAD*), Salt Lake City, 9-11 September 2024, 1-7. https://doi.org/10.1109/mlcad62225.2024.10740223

[9] Wang, F., Wang, Q., Alrahis, L., Fu, B., Jiang, S., Zhang, X., Sinanoglu, O., Ho, T.-Y., Young, E.F.Y. and Knechtel, J. (2024). TroLLoc: Logic Locking and Layout Hardening for IC Security Closure against Hardware Trojans. arXiv:2405.05590. https://doi.org/10.48550/arXiv.2405.05590

[10] Hemavathy, S., Jagadeesh, K. and Bhaaskaran, V.S.K. (2025) Unified Security Framework Using Device-Specific Fingerprint: Mitigating Hardware Trojans and Authenticating Firmware Updates. *IEEE Access*, **13**, 26897-26914. https://doi.org/10.1109/access.2025.3538936

[11] Sutikno, S., Putra, S.D., Wijitrisnanto, F. and Aminanto, M.E. (2023) Detecting Unknown Hardware Trojans in Register Transfer Level Leveraging Verilog Conditional Branching Features. *IEEE Access*, **11**, 46073-46083. https://doi.org/10.1109/access.2023.3272034

[12] Su, H., Hu, W., Zhang, X., Zhu, D. and Wu, L. (2025) Towards Precise and Explainable Hardware Trojan Localization at LUT Level. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. https://doi.org/10.1109/tcad.2025.3527377

[13] Ma, P., Li, J., Liu, H., Shi, J., Zhang, S., Pan, W. and Hao, Y. (2023) Hardware Trojan Detection Methods for Gate-Level Netlists Based on Graph Neural Networks. *IEEE Transactions on Computers*, **74**, 1470-1481. https://doi.org/10.1109/TC.2025.3533085

[14] Parikh, R. and Parikh, K. (2025) Mathematical Foundations of AI-Based Secure Physical Design Verification. Preprints. https://doi.org/10.20944/preprints202502.1831.v1

[15] Tauhid, A., Xu, L., Rahman, M. and Tomai, E. (2023) A Survey on Security Analysis of Machine Learning-Oriented Hardware and Software Intellectual Property. *High-Confidence Computing*, **3**, Article 100114. https://doi.org/10.1016/j.hcc.2023.100114

[16] Ghimire, A., Alkurdi, M., Amsaad, F., Rahman, M.T. and Jhanjhi, N.Z. (2024) AI-Enabled Hardware Trojan Detection for Secure and Trusted Context-Aware Embedded Systems. Preprints. https://doi.org/10.36227/techrxiv.170630749.99115711/v1