SYNOPSIS

A **hardware Trojan** is a type of malicious modification made to the hardware components of a computer system, during the manufacturing process. These modifications can be difficult to detect and can have serious consequences, including data theft, system malfunction, or providing unauthorized access to attackers as a result, it is of paramount importance to detect such malicious modifications before use.

Logic Testing:

This involves running a series of tests on the IC's logic circuits to see if they behave differently than expected. It can help spot hidden Trojans by comparing with normal operations.

Issues in Logic Testing:

Logic testing has a few key challenges when it comes to finding hardware Trojans. First, some Trojans are very stealthy—they stay hidden during normal tests and only show up under rare conditions, making them hard to detect. Another issue is that it's difficult to create test patterns that cover every possible way a circuit might behave, especially in complicated designs. Also, creating and running all these tests takes a lot of time and computer power, which can be a problem, especially for large circuits. Some Trojans are designed to blend in with normal circuit behaviour, so they don't change the outputs in a noticeable way, leading to missed detections. These challenges make it tough to find all the Trojans through logic testing alone.

Existing Approaches:

1. MERO (Multiple Excitation of Rare Occurrence) Approach:

This approach [1] focuses on generating test patterns that activate rare conditions in a circuit, which are more likely to trigger hidden Trojans. By targeting these rare logic states multiple times, MERO increases the chances of detecting Trojans while minimizing the number of test patterns needed.

2. Genetic Algorithm Approach:

Genetic Algorithms (GAs) [2] use principles of natural selection to optimize test generation for Trojan detection. GAs start with a set of random test patterns and evolve them over multiple iterations, selecting the most effective ones for Trojan detection.

Project Focus:

Reinforcement Learning (RL) Approach:

In light of the above discussion, we have opted for reinforcement learning (RL) [3] for our hardware Trojan detection project, leveraging its significant advantages over traditional methods. RL offers high adaptability, continuously learning and refining its strategies based on ongoing feedback, which enhances its accuracy in detecting hidden Trojans. This is a major improvement over traditional methods. RL excels in identifying rare and subtle conditions, which is crucial since hardware Trojans are often designed to be triggered only under very specific. By automatically optimizing test pattern generation, RL streamlines the detection process, saving both time and effort which is required to test large benchmarks such a ISCAS 85 [4]. Furthermore, RL's ability to explore a wide range of scenarios and adjust its approach dynamically makes it particularly effective for managing the complexity of modern integrated circuit (IC) designs. This flexibility and scalability positions RL as a powerful and innovative approach to advancing hardware security in increasingly sophisticated environments.

References:

[1] Chakraborty, Rajat Subhra, et al. "MERO: A statistical approach for hardware Trojan detection." International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[2] Nourian, M. A., Mahdi Fazeli, and David Hély. "Hardware trojan detection using an advised genetic algorithm based logic testing." Journal of Electronic Testing 34 (2018): 461-470.

[3] Lyu, Yangdi, and Prabhat Mishra. "Automated test generation for Trojan detection using delay-based side channel analysis." 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2020.

[4] ISCAS benchmarks. Available at https://www.pld.ttu.ee/~maksim/benchmarks/iscas85/bench/.