

Trojan Playground: A Reinforcement Learning Framework for Hardware Trojan Insertion and Detection

Amin Sarihi¹, Ahmad Patooghy², Peter Jamieson³, and Abdel-Hammed A. Badawy¹

¹Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM

²Department of Computer Systems Technology, North Carolina A&T State University, Greensboro, NC

³Department of Electrical and Computer Engineering, Miami University, Oxford, OH

E-mail: sarihi@nmsu.edu

Abstract—Current Hardware Trojan (HT) detection techniques are mostly developed based on a limited set of HT benchmarks. Existing HT benchmark circuits are generated with multiple shortcomings, *i.e.*, i) they are heavily biased by the designers' mindset when they are created, and ii) they are created through a one-dimensional lens, mainly the signal activity of nets. To address these shortcomings, we introduce the first automated reinforcement learning (RL) HT insertion and detection framework. In the insertion phase, an RL agent explores the circuits and finds different locations that are best for keeping inserted HTs hidden. On the defense side, we introduce a multi-criteria RL-based detector that generates test vectors to discover the existence of HTs. Using the proposed framework, one can explore the HT insertion and detection design spaces to break the human mindset limitations as well as the benchmark issues, ultimately leading toward the next-generation of innovative detectors. Our HT toolset is open-source to accelerate research in this field and reduce the initial setup time for newcomers. We demonstrate the efficacy of our framework on ISCAS-85 benchmarks and provide the attack and detection success rates and define a methodology for comparing our techniques.

Index Terms—Hardware Trojan, Hardware Security, Reinforcement Learning, Open-Source.

I. INTRODUCTION

PER a DoD report [1] released in 2022, 88% of the production and 98% of the assembly, packaging, and testing of microelectronic chips are performed outside of the US. The growing multi-party production model has significantly raised security concerns about malicious modifications in the design and fabrication of chips, *i.e.*, Hardware Trojan (HT) insertion. HTs are defined as any design/manufacturing violations in an integrated circuit (IC) with respect to the intent of the IC. Upon activation, an HT may lead to erroneous outputs (an example is seen in Figure 1) and/or leak of information [2]. According to the adversarial model introduced by Shakya *et al.* [3], HTs can be inserted into target ICs according to the following scenarios:

- Design source code or netlist can be infected with HTs by compromised employees.
- Third-party intellectual properties (IPs) like processing cores, memory modules, I/O components, and network-on-chip [4] are often purchased and incorporated into a

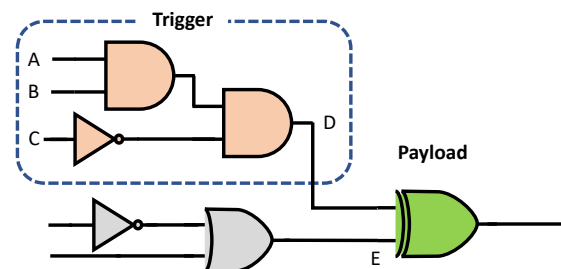


Fig. 1: An HT with a trigger and payload. Whenever $A=1$, $B=1$, $C=0$, the trigger is activated ($D=1$) and the XOR payload inverts the value of E .

design to speed up time-to-market and lower design expenses. However, integrating IPs from untrusted vendors can pose a risk to the security and integrity of the IC.

- An untrusted foundry may reverse-engineer the GDSII physical layout to obtain the netlist and insert HTs inside them.
- Malicious third-party CAD tools may also insert HTs into designs

We believe that HTs can be inserted into designs in any of the discussed adversarial models.

Researchers have been mostly using established benchmarks reported by Shakya *et al.* and Salmani *et al.* [3], [5] as a reference to study the impact of HTs¹. Subsequently, various HT detection approaches have been developed based on these benchmarks over the past decade [6]–[9]. Despite the valuable effort to create HT benchmarks for the community, these benchmarks are limited in terms of size and variety that are needed to push detection tools into more realistic modern scenarios. For instance, the small set of benchmarks means it is hard to leverage and train machine learning (ML) HT detectors, where insufficient training data negatively impact classification accuracy. Some research studies have tried to alleviate this problem by using techniques to shuffle data for ML-based detectors, *e.g.*, the leave-one-out cross-validation method [7]; however, it does not solve the problem entirely. Additionally, the existing HT benchmarks suffer from an

¹These benchmarks are available on trust-hub.org.

inherent human bias in the insertion phase, since they are tightly coupled with the designer’s mindset. For instance, the HT benchmarks in [10] only consider signal activity for HT insertion, *i.e.*, HTs are inserted into a pool of available rare nets of the circuit in a random fashion. The flaws in the insertion phase simplify the problem’s complexity, leading security researchers to develop HT detectors finely tuned to flawed scenarios [9], [11]. In contrast, adversaries devise new HT attacks that combine different ideas where detectors fall short to expose them. Another equally important problem in this domain is having almost no HT detectors publicly available. This deprives other researchers of accessing these tools and imposes a considerable latency for newcomers to hardware security.

This work attempts to move this research space forward by developing next-generation HT insertion and detection methods based on reinforcement learning (RL). The developed RL-based HT insertion tool creates new HT benchmarks according to the criteria passed to the tool by the user. The insertion criteria is an RL rewarding function modified by a user that relies on the RL agent to automatically insert HTs into designs. The netlist is considered an environment in which the RL agent tries to insert HTs to maximize a gained reward. The rewarding scheme of the proposed insertion tool is tunable, which can push the agent toward a specific goal in the training session. We believe that our insertion tool is a step towards preparing the community for future HTs inserted by non-human agents, *e.g.*, AI agents.

We also propose an RL-based HT detector with a tunable rewarding function that helps detect inserted HTs based on various strategies. We have studied three different detection rewarding functions for the RL detector agent to explore this space. The agent finds test vectors that yield the highest rewards per each reward function. Then, the generated test vectors are used to activate and find HTs in the IC. The test engineer passes the test vectors to the chip and monitors the output for any deviations from the golden model.

Our proposed toolset enables the researchers to experience both HT insertion and detection within a unified framework. The framework only requires users to set the parameters to insert and detect HTs without human intervention. There have been previous efforts to automate the HT insertion and detection process [10], [12], [13]; however, they are either not open-source tools or need an intermediate effort hindering us from creating a vast quantity of HTs (more explanation in Section II).

We make the following contributions in the paper with respect to our previous publications ([14], [15]) noting that all of the work will be released open-source:

- We developed a tunable RL-based HT insertion tool free of human bias, capable of automatic HT insertion and creating a large population of valid HTs for each design
- We introduce a tunable RL-based multi-criteria HT detection tool that helps a security engineer to better prepare for different HT insertion strategies.
- We introduce and use a generic methodology to make fair comparisons between HT detectors. The methodology is based on a metric called the confidence value that helps

the security engineer to select the proper detector based on the chip’s application and security requirements.

Our results show that our developed detection tool with all three of our detection approaches has a 90.54% detection rate on average for our HT-inserted benchmarks. We compare these detection results to existing state-of-the-art detection methods and show how our techniques find previously unidentifiable HTs. As we believe that HT detection will be implemented as a variety of different detection strategies, the uniquely identified HTs suggest that our detection techniques and framework are important contributions to this space.

The remainder of this paper is organized as follows: Section II reviews the related work and explains the fundamentals of RL. The mechanics of our proposed HT insertion and detection approaches are presented in Sections III and IV, respectively. We introduce our HT comparison methodology in Section V. Section VI demonstrates the experimental results and Section VII concludes the paper.

II. RELATED WORK

This section reviews the previous studies in HT insertion and detection.

A. Hardware Trojan Insertion and Benchmarks

The first attempts to gather benchmarks with hard-to-activate HTs were made by Shakya *et al.* and Salmani *et al.* [3], [5]. A set of 96 trust benchmarks with different HT sizes and configurations are available at Trust-Hub [16]. While these benchmarks are a valuable contribution for the research community, they have three drawbacks: (1) The limited number of Trojan circuits represents only a subset of the possible HT insertion landscape in digital circuits, which hampers the ability to develop diverse HT countermeasures, (2) they lack incorporating state-of-the-art Trojan attacks and (3) they fail to populate a large enough HT dataset that is required for ML-based HT detection.

Various approaches since have attempted to insert HTs. Jyothi *et al.* [17] proposed a tool called TAINT for automated HT insertion into FPGAs at the RTL level, gate-level netlist, and post-map netlist. The tool also allows the user to insert HTs in FPGA resources such as Look-Up Tables (LUTs), Flip Flops (FFs), Block Random Access Memory (BRAM), and Digital Signal Processors (DSP). Despite the claimed automated process, the user is expected to select the trigger nets based on suggestions made by the tool. The results section shows that the number of available nodes in post-map netlists drops significantly, leaving less flexibility for Trojan insertion compared to RTL codes.

Reverse engineering tools can also be used to identify security-critical circuitry in designs that can direct attackers to insert efficient HTs. Fyrbial *et al.* [18] introduced HAL, a gate-level netlist reverse engineering tool that offers both offensive reverse engineering strategies and defensive measures, such as developing arbitrary Trojan detection techniques. The authors believe that adversaries are more likely to insert HTs through reverse engineering techniques and are less likely to have direct access to the original HDL codes. A hardware

Trojan that leaks cryptographic keys has been inserted with the tool; nonetheless, it requires human effort for insertion, which hinders the process of producing a large HT dataset [19].

Cruz *et al.* [10] tried to address the benchmark shortcomings by presenting a toolset capable of inserting a variety of HTs based on the parameters passed to the toolset. Their software inserts HTs with the following configuration parameters: the number of trigger nets, the number of rare nets among the trigger nodes, a rare-net threshold (computed with functional simulation), the number of the HT instances to be inserted, the HT effect, the activation method, its type, and the choice of payload. Despite increasing the variety of inserted HTs, there is no solution for finding the optimal trigger and payload nets. The TRIT benchmark set generated by this tool is available on Trust-Hub [16].

Cruz *et al.* [19] propose MIMIC, an ML framework for automatically generating Trojan benchmarks. The authors extracted 16 functional and structural features from existing Trojan samples. Then, they trained ML models and generated a large number of hypothetical Trojans called *virtual Trojans* for a given design. The virtual Trojans are then compared to a reference Trojan model and ranked. Finally, the selected Trojan will be inserted into the target circuit using suitable trigger and payload nets. The HT insertion process is extremely convoluted, requiring multiple stages and expertise. MIMIC is not released to the public and rebuilding the tool from their work is an extensive process. MIMIC’s HT insertion criteria are very similar to [10] and it suffers the same shortcomings in [10].

In an attempt to deceive machine learning HT detection approaches, Nozawa *et al.* [20] have devised adversarial examples. Their proposed method replaces the HT instance with its logically equivalent circuit so that the classification algorithm erroneously disregards it. To design the best adversarial example, the authors have defined two parameters: Trojan-net concealment degree (TCD) which is tuned to maximize the loss function of the neural network in the detection process, and a modification evaluating value (MEV) that should be minimized to have the least impact on circuits. These two metrics help the attacker to look for more effective logical equivalents and diversify HTs. The equivalent HTs are inserted in trust-hub benchmarks, and they decrease accuracy significantly.

Sarihi *et al.* [14] (our own work) insert a large number of HTs into ISCAS-85 benchmarks with Reinforcement Learning (RL). The HT circuit is an agent that interacts with the environment (the circuit) by taking 5 different actions (next level, previous level, same level up, same level down, no action) for each trigger input. Level denotes the logic level in the combinational circuits. The agent moves the Trojan inputs throughout the circuit and explores various locations suitable for embedding HTs. Triggers are selected according to a set of SCOAP (Sandia Controllability/Observability Analysis Program [21]) parameters, *i.e.*, a combination of controllability and observability. The agent is rewarded in proportion to the number of circuit inputs it can engage in the HT activation process.

Gohil *et al.* [22] proposed ATTRITION, another RL-based HT insertion platform where signal probability is the target

TABLE I: Survey of previous HT insertion tools.

Tool	Domain	Insertion Criteria	Automate	Open-Source
Trust-Hub [3]	ASIC/FPGA	Secret Leakage, Signal Prob.	✗	✗
HAL [18]	ASIC/FPGA	Neighborhood Control Value	✗	✓
TAINT [17]	FPGA	Not Mentioned	✗	✗
TRIT [10]	ASIC	Signal Prob.	✗	✗
Yu <i>et al.</i> [13]	ASIC	Transition Prob.	✓	✗
Nozawa <i>et al.</i> [20]	ASIC	Same as [3]	✗	✗
MIMIC [19]	ASIC	Struct. & Funct. Features	✓	✗
Sarihi <i>et al.</i> [14]	ASIC	SCOAP parameters	✓	✗
ATTRITION [22]	ASIC	Signal Prob.	✓	✗

upon which the trigger nets are selected. The agent tries to find a set of so-called *compatible* rare nets, *i.e.*, a group of rare nets that can be activated together with an input test vector. The test vector is generated using a SAT-solver. The authors also propose a pruning technique to limit the search space for the agent to produce more HTs in a shorter period. The tool is claimed to be open-source, but only the source code was released..

Table I summarizes the existing artifacts and research in the HT insertion space. It represents the target technology (2nd column); summarizes the insertion criteria (3rd column); shows if the tool is automated (4th column), and if the tool or its artifacts are openly released (5th column).

B. Hardware Trojan Detection

Chakraborty *et al.* [23] introduced MERO, a test vector generator that tries to trigger possible HTs by exciting rare-active nets multiple times. The algorithm’s efficacy is tested against randomly generated HTs with rare triggers. MERO’s detection rate significantly shrinks as circuit size grows.

Hasegawa *et al.* [7] have proposed a machine-learning method for HT detection. The method extracts 51 circuit features from the trust-hub benchmarks to train a random forest classifier that eventually decides whether a design is HT-free or not. The HT classifier is trained on a limited HT dataset with an inherent bias during its insertion phase.

Lyu *et al.* [11] proposed TARMAC to map the trigger activation problem to the clique cover problem, *i.e.*, treating the netlist as a graph. They utilized a SAT-solver to generate the test vector for each maximal satisfiable clique. The method lacks scalability as it should run on each suspect circuit separately. Also, the achieved performance is not stable [2]. Implementation of the method is neither trivial nor available online for researchers [22].

TGRL is an RL framework used to detect HTs [2]. The agent decides whether to flip a bit in the test vector according to an observed probability distribution. The reward function, which is a combination of the number of activated nets and their SCOAP [24] parameters, pushes the agent to activate as many signals as possible. Despite its higher HT detection rate than MERO and TARMAC, the algorithm was not tested on any HT benchmarks [22].

DETERRENT, an RL-based detection method [9], finds the smallest set of test vectors to activate multiple combinations of trigger nets. The RL state is a subset of all possible rare nets, and actions are appending other rare nets to this subset. The authors used a SAT-solver to determine if actions are

TABLE II: Survey of Previous HT Detection Tools.

Study	Detection Basis	Open-Source
MERO [23]	Switching Activity	✗
Hasegawa <i>et al.</i> [7]	Netlist Features	✗
TARMAC <i>et al.</i> [11]	Switching Activity	✗
TGRL <i>et al.</i> [2]	Switching Activity	✗
DETERRENT <i>et al.</i> [9]	Switching Activity	✗
HW2VEC [25]	Graph Structural Info.	✓

compatible with the rare nets in the subsets and they only focus on signal-switching activities as their target.

The HW2VEC tool [25] converts RTL-level and gate-level designs into a dataflow graph and abstract syntax tree to extract a feature set that represents the structural information of the design. Extracted features are used to train a graph neural network to determine whether a design is infected with HTs or not. The authors test the tool with 34 circuits infected by in-house generated HTs.

It is very important to note that out of the methods reviewed above (and others studied but not discussed here), the only publicly available tool is HW2VEC. Table II summarizes the previous works in HT detection where researchers have used various criteria in detecting HTs (2nd column), and the open-source state of the work (3rd column).

III. THE PROPOSED HT INSERTION

Figure 2 shows the flow of the proposed HT insertion tool. The first step creates a graph representation of the flattened netlist from the circuit. Yosys Open Synthesis Suite [26] translates the HDL (Verilog) source of the circuit into a JSON (JavaScript Object Notation) [27] netlist which enables us to parse the internal graph representation of the circuit. Next, the tool finds a set of rare nets to be used as HT trigger nets (this step is described in details in Subsection III-A). Finally, an RL agent uses the rare net information and attempts to insert an HT to maximize a rewarding function as described in section III-B.

A. Rare Nets Extraction

We use the parameters introduced in [8] to identify trigger nets. These parameters are defined as functions of net *controllability* and *observability*. Controllability measures the difficulty of setting a particular net in a design to either '0' or '1'. Observability, on the other hand, is the difficulty of propagating a net value to at least one of the circuit's primary outputs [21].

The first parameter is called the HT trigger susceptibility parameter, and it is derived from the fact that low-switching nets have mainly a high difference between their controllability values. Equation 1 describes this parameter:

$$HTS(Net_i) = \frac{|CC1(Net_i) - CC0(Net_i)|}{Max(CC1(Net_i), CC0(Net_i))} \quad (1)$$

where *HTS* is the HT trigger susceptibility parameter of the net; *CC0*(*Net_i*) and *CC1*(*Net_i*) are the combinational controllability 0 and 1 of *Net_i*, respectively. The *HTS* parameter

ranges between [0, 1) such that higher values correlate with lower activity on the net.

The other parameter, specified in Equation 2, measures the ratio of observability to controllability:

$$OCR(Net_i) = \frac{CO(Net_i)}{CC1(Net_i) + CC0(Net_i)} \quad (2)$$

where *OCR* is the observability to controllability ratio. This equation requires that the HT trigger nets must be very hard to control, but not so hard to observe. Unlike the *HTS* parameter, *OCR* is not bounded, and it belongs to the interval of [0, ∞). We will specify thresholds (see Section VI) for each parameter and use them as filters to populate the set of rarely-activated nets for our tool.

B. RL-Based HT Insertion

The RL environment is, in fact, the circuit in which the agent is trying to insert HTs. The agent's action is to insert combinational HTs where trigger nets are ANDED, and the payload is an XOR gate (same as Figure 1). The RL agent starts from a reset condition where it takes a series of actions that eventually insert HTs in the circuit. Different HT insertion options are represented with a state vector in each circuit. For a given HT, the state vector is comprised of $s_t = [s_1, s_2, \dots, s_{n-2}, s_{n-1}, s_n]$ where s_1 through s_{n-2} are the logic-levels of the HT inputs, and s_{n-1} and s_n are the logic-levels of the target net and the output of the XOR payload, respectively. Figure 3 shows an example of how we conduct the circuit levelization. Here, the circuit Primary Inputs (PIs) are considered level 0. The output level of each gate is computed by Equation 3:

$$Level(output) = MAX(Level(in_1), Level(in_2)) + 1 \quad (3)$$

As an example, the HT in Figure 4 (in yellow) has the state vector $s_t = [2, 1, 3, 4]$. The action space of the described HT agent is multi-discrete, *i.e.*, each input of the HT may choose an action from a set of five available actions. These actions are:

- **Next level:** the input of the HT moves to one of the nets that are one level higher than the current net level.
- **Previous level:** the input of the HT moves to one of the nets that is one level lower than the current net level.
- **Same level up:** the input of the HT will move to one of the nets at the same level as the current net level. The net is picked by pointing to the next net in the ascending list of net ids for the given level.
- **Same level down:** the input of the HT will move to one of the nets at the same level as the current net level. The net is picked by pointing to the previous net in the ascending list of nets for the given level.
- **No action:** the input of the HT will not move. If an action leads the agent to step outside the circuit boundaries, it is substituted with a "No action".

The action space is also represented by a vector where its size is equal to the number of the HT inputs, and each action can be one of the five actions above, e.g., for the HT in Figure 4, the action space would be $a_t = [a_1, a_2]$ since it has

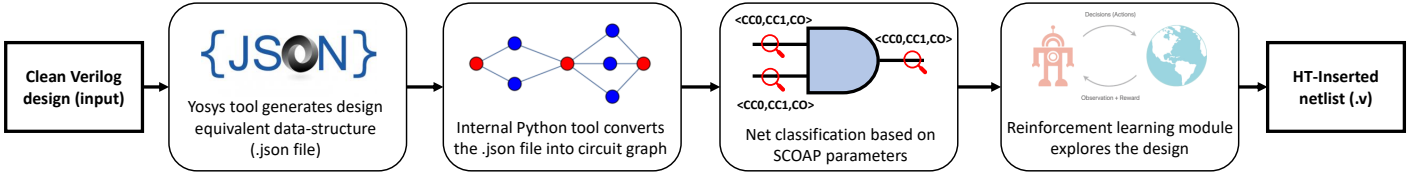


Fig. 2: The proposed RL-based HT insertion tool flow.

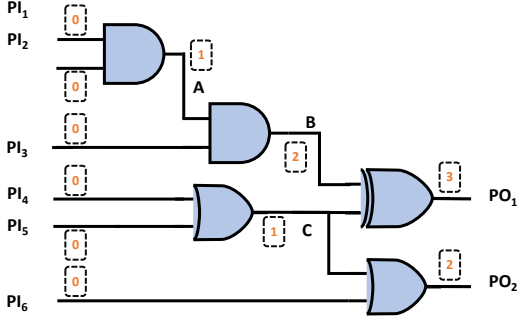


Fig. 3: Levelizing a circuit. The output level of each digital gate is computed by $\max(\text{Level}(in1), \text{Level}(in2)) + 1$.

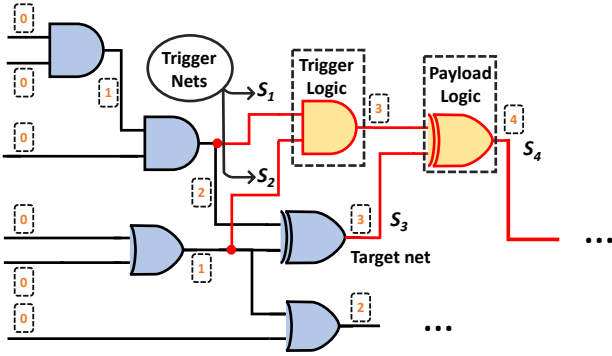


Fig. 4: Obtaining the state vector in the presence of an HT in the circuit.

two inputs. Hypothetical actions for the first and the second inputs can be the same level up/down and next/previous level, respectively.

The flow of our RL inserting agent is described in Algorithm 1. The SCOAP parameters are first computed (line 1). We specify two thresholds T_{HTS} and T_{OCR} and require our algorithm to find nets that have higher HTS values than T_{HTS} and lower OCR values than T_{OCR} (line 2). These nets are classified as rare nets. The algorithm consists of two nested while loops that keep track of the terminal states and the elapsed timesteps. The latter defines the total number of samples the agent trains on. We have used the OpenAI Gym [28] environment to implement our RL agent.

The first used method is called `reset_environment()` which resets the environment before each episode and returns the initial location of the agent HT (line 5). The HT is randomly inserted within the circuit according to the following set of rules.

- Rule 1) Trigger nets are selected randomly from the list

Algorithm 1 Training of the HT inserting Reinforcement Learning Agent

Input: Graph G , HTS Threshold T_{HTS} , OCR Threshold T_{OCR} , Circuit Inputs in_ports , State Space s_t , Terminal State $Terminal_state$, Total Timesteps j ;
Output: HT Benchmark $HT_{Benchmark}$;

```

1: Compute SCOAP parameters:
    $\langle CC0, CC1, CO \rangle = \text{computeSCOAP}(G)$ ;
2: Get the set of rare nets:
    $rare\_nets = \text{Compute\_Rare\_Nets}(G, T_{HTS}, T_{OCR})$ ;
3:  $counter = 0$ ;
4: while ( $counter < j$ ) do
5:    $HT = \text{reset\_environment}()$ ;
6:    $Terminal\_state = \text{false}$ ;
7:   while  $!(Terminal\_state)$  do
8:      $G, s_t, Terminal\_state, HT_{triggers} = \text{action}(HT)$ ;
9:      $HT\_activated = \text{PODEM}(G)$ ;
10:     $temp\_reward = (HT_{triggers} \cap rare\_nets).count()$ ;
11:    if ( $HT\_activated$ ) then
12:      if ( $temp\_reward == 1$ ) then
13:         $reward = 8$ ;
14:      else if ( $temp\_reward == 2$ ) then
15:         $reward = 16$ ;
16:      else if ( $temp\_reward == 3$ ) then
17:         $reward = 100$ ;
18:      else if ( $temp\_reward == 4$ ) then
19:         $reward = 1000$ ;
20:      else if ( $temp\_reward == 5$ ) then
21:         $reward = 10000$ ;
22:      else
23:         $reward = -1$ ;
24:      end if
25:    end if
26:     $\text{update\_PPO}(\text{action}, s_t, \text{reward})$ ;
27:     $counter + = 1$ ;
28:  end while
29: end while
30:  $HT_{Benchmark} = \text{Graph\_to\_netlist}(G)$ 

```

of the total nets.

- Rule 2) Each net can drive a maximum of one trigger net.
- Rule 3) Trigger nets cannot be assigned as the target.
- Rule 4) The target net is selected with respect to the level of trigger nets. To prevent forming combinational loops, we specify that the level of the target net should

be greater than that of the trigger nets.

In each episode of the training process, we keep the target net unchanged to help the RL algorithm converge faster. Instead of manually specifying a target net, we let the algorithm explore the environment and choose target net. The terminal state variable TS is set to *False* to check the termination condition for each episode. When the level of the trigger nets reaches the level of the target net, or the number of steps per episode reaches an allowed maximum (lines 6-7), TS becomes *True* which terminates the episode.

The training process of the agent takes place in a loop where actions are being issued, rewards are collected, the state is updated, and eventually, the updated graph is returned. To test the value of an action taken by the RL agent (meaning if the HT can be triggered with at least one input pattern), we use *PODEM* (Path-Oriented Decision Making), an automatic test pattern generator [29] (line 9). This algorithm uses a series of backtracing and forward implications to find a vector that activates the inserted HT. If the HT payload propagates through at least one of the circuit outputs, the action gains a reward proportional to the number of rare triggers on the HT. After the number of rare triggers is counted in line 10, the agent is rewarded in lines 11 through 25. The rewarding scheme is designed such that the agent would start finding HTs with 1 rare trigger net and adds more rare while exploring the environment. Additionally, the exponential reward increase in each case ensures that the agent is highly encouraged to find HTs that have at least 3 or more rare trigger nets. In case an HT is not activated with *PODEM* or no rare nets are among the HT triggers, the agent will be rewarded -1 . Since the agent is unlikely to find high-reward HTs at the beginning of the exploration stage, the first two rewarding cases ($temp_{reward} = 1$ and $temp_{reward} = 2$) should be set such that the agent sees enough positive rewarding improvements, yet be more eager to find more HTs that yield higher rewards. The reward values are assigned to different cases after conducting extensive experiments with the RL agent.

To train the RL agent, we use the *PPO* (Proximal Policy Optimization) [30] RL algorithm. PPO can train agents with multi-discrete action spaces in discrete or continuous spaces. The main idea of PPO is that the new updated policy (which is a set of actions to reach the goal) should not deviate too far from the old policy following an update in the algorithm. To avoid substantial updates, the algorithm uses a technique called clipping in the objective function [30]. By using a clipped objective function, PPO restricts the size of policy updates to prevent them from deviating too much from the previous policy. This constraint promotes stability and ensures that the updates are controlled within a certain range, which helps to avoid any abrupt changes that may negatively affect the performance of the agent. At last, when the HTs are inserted, the toolset outputs Verilog gate-level netlist files that contain the malicious HTs (line 30).

IV. THE PROPOSED HT DETECTION

From a detection perspective, we must determine whether a given circuit is clean or Trojan-infected. To achieve this

goal, an RL agent is defined that applies its generated test vectors to circuits and checks for any deviation at the circuits' primary outputs with respect to the expected outputs (golden model). The agent interacts with the circuit (performs actions) by flipping the vector values aiming to activate certain internal nets. The action space is an n -dimensional binary array where n is the number of circuit primary inputs. The action space vector a_t is defined as $a_t = [a_1, a_2, \dots, a_n]$. The agent decides to toggle each a_i to transition to another state or leave them unchanged. $a_i = 0$ denotes that the value of the i^{th} bit of the input vector should remain unchanged from the previous test vector. In contrast, $a_i = 1$ means that the i^{th} input bit should flip. The RL agent follows a π policy to decide which actions should be commenced at each state. The π policy is updated using a policy gradient method [31] where the agent commences actions based on probability distribution from π policy. The assumption is that attackers are likely to choose trigger nets that have a consistent value (0 or 1) most of the time. Thus, a detector aims to activate as many of these dormant nets as possible. We consider two different approaches for identifying such rare nets:

1) Dynamic Simulation: We feed each circuit with 100K random test vectors and record the value of each net. Then, we populate the switching activity statistics during the simulation time and set a threshold θ for rare nets where the switching activity for a net below θ denotes that the net is rare. θ is in the range of $[0, 1]$.

2) Static Simulation: We use the *HTS* parameter in Equation 1 and a threshold to find rare nets. Categorizing rare nets with this approach provides the security engineer with an extra option for detection.

In a circuit with m rare nets, the state space is defined as $State_t = [s_1, s_2, \dots, s_m]$ where s_i is associated with the i^{th} net in the set. If an action (a test vector) sets the i^{th} net to its rare value, s_i will be 1; otherwise, s_i stays at 0. As can be inferred, the action and state spaces are multi-binary.

Attackers tend to design multi-trigger HTs [10] and this should be considered when HT detectors are designed. The final purpose of our detector is to generate a set of test vectors that can trigger as many rare nets as possible. To achieve this goal, a part of the rewarding function should enumerate rare nets. However, we should avoid over-counting the situations in which a rare net has successive dependent rare nets. An example case is shown in Figure 5 where four nets net_1 , net_2 , net_3 , and net_4 (with their switching probabilities and their rare values) are all dependent rare nets. Instead of including all four nets in the state space, we choose the rarest net as the representative net since activating the rarest net ensures the activation of the others as well. In this example, net_4 is

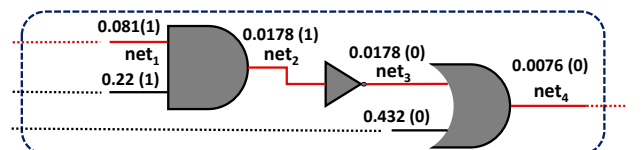


Fig. 5: State pruning identifies nets in the same activation path.

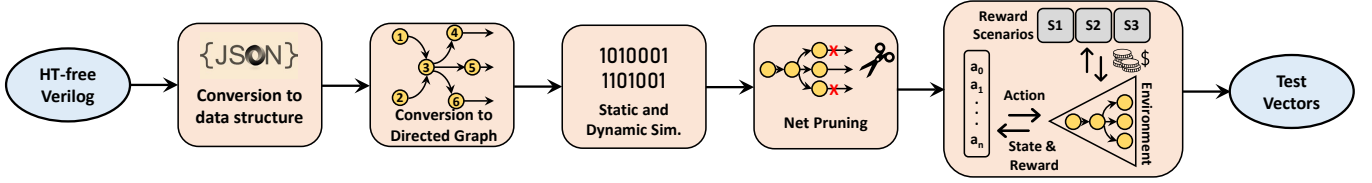


Fig. 6: The proposed detection flow.

selected as the set representative. This policy helps accelerate the RL agent to converge on the global minima faster. Figure 6 summarizes our proposed detection flow.

As for rewarding the agent, we consider three rewarding functions, which we explain here. Our multi-rewarding detector enables security engineers to better prepare for attackers with different mindsets.

A. Rewarding function D1

In our first rewarding function (Algorithm 2), we push the RL agent to build on its current state. We use a copy of the previous state and encourage the agent to generate state vectors that differ from the previous one. The hypothesis is to push the agent toward finding test vectors that lead to various unseen states. The pruned current and previous state vectors and its length are passed as inputs to Algorithm 2 to compute the reward. The rewarding function is composed of an *immediate* and a *sequential* part, which are initialized to 0 in lines 1 and 2, respectively. Whenever the state transitions, we iterate through the loop K times. We calculate the sequential reward by making a one-to-one comparison between the nets in the old and new states. According to lines 5 – 11, the highest reward is given when an action can trigger a net that was not triggered in the previous state, *i.e.*, +40. If a rare net is still activated in the current state, the agent will still get rewarded +20. The worst state transition is whenever an action leads to a rare net losing its rare value, which is rewarded -3 . Lastly, if the agent cannot activate a rare net after a state transition, it will be rewarded -1 . The immediate award is simply the number of activated rare nets in the new state. The ultimate reward value is a linear combination of the immediate and sequential rewards with coefficients λ_1 and λ_2 , respectively, which are tunable parameters to be set by the user. Note that we build the state vector with the obtained rare nets from functional simulation.

B. Rewarding function D2

Algorithm 3 describes our second rewarding function. In this case, the agent gains rewards proportional to the difficulty of the rare nets triggered. First, the reward vector is initiated with a length equal to the state vector (line 1). Each element in the reward vector has a one-to-one correspondence with rare nets on the state vector. The reward for each rare net is computed by taking the inverse of the net switching activity rate (line 4). There are cases where a net might have a switching probability of 0. In such cases, activating the net would be rewarded 10X times the greatest reward in the vector

Algorithm 2 Rewarding Function 1

Input: $State_{pre}$, $State_{cur}$, State Vector Length K
Output: $Reward_{final}$

```

1:  $Reward_{Imd} = 0$ ;
2:  $Reward_{Seq} = 0$ ;
3: for  $k \in \{0, \dots, K - 1\}$  do
4:   if ( $State_{cur}[k] = 0$  and  $State_{pre}[k] = 0$ ) then
5:      $Reward_{Seq} += -1$ ;
6:   else if ( $State_{cur}[k] = 0$  and  $State_{pre}[k] = 1$ ) then
7:      $Reward_{Seq} += -3$ ;
8:   else if ( $State_{cur}[k] = 1$  and  $State_{pre}[k] = 0$ ) then
9:      $Reward_{Seq} += 40$ ;
10:  else if ( $State_{cur}[k] = 1$  and  $State_{pre}[k] = 1$ ) then
11:     $Reward_{Seq} += 20$ ;
12:  end if
13: end for
14:  $Reward_{Imd} = State_{cur}.count(1)$ 
15:  $Reward_{final} = \lambda_1 \times Reward_{Seq} + \lambda_2 \times Reward_{Imd}$ 

```

(line 12). Thus, upon the observance of every new state, the agent will be rewarded based on the nets that were activated and the reward vector (line 18). If a rare net was not activated, -1 will be added to the final reward (line 20). The algorithm aims to encourage the agent to directly trigger the rarest nets in the circuit.

C. Rewarding function D3

In the third rewarding function, described in Algorithm 4, rare nets are populated based on the threshold of the *HTS* parameter computed during the static simulation using Equation 1. When a rare net in the set is activated, the agent is rewarded with the controllability of the rare value (line 4). Otherwise, it will receive -1 from the environment (line 6). This scenario aims to investigate controllability-based HT detection with the RL agent.

V. THE PROPOSED GENERIC HT-DETECTION METRIC

We propose the following methodology to the community to make fair and repeatable comparisons among HT detection methods. In addition, our methodology can help compare different HT insertion techniques for a given HT detector. This methodology obtains a confidence value that one can use to compare different HT detection methods.

Figure 7 shows four possible outcomes when an HT detection tool studies a given circuit. From the tool user's perspective, the outcomes are probabilistic events. For example,

Algorithm 3 Rewarding Function 2

Input: Net switching vector $Switching_{vector}$,
 Current state vector $State_{vector}$, State Vector Length K
Output: Final reward $Reward_{final}$

```

1:  $Reward_{vector} = [0] * K$ 
2: for  $k \in \{0, \dots, K - 1\}$  do
3:   if ( $Switching_{vector}[k] \neq 0$ ) then
4:      $Reward_{vector}[k] = Switching_{vector}[k]^{-1}$ 
5:   else
6:      $Reward_{vector}[k] = 0$ 
7:   end if
8: end for
9:  $reward_{max} = max(Reward_{vector}[\ ])$ 
10: for  $k \in \{0, \dots, K - 1\}$  do
11:   if ( $Switching_{vector}[k] == 0$ ) then
12:      $Reward_{vector}[k] = 10 * reward_{max}$ 
13:   end if
14: end for
15:  $Reward_{final} = 0$ 
16: for  $k \in \{0, \dots, K - 1\}$  do
17:   if ( $State_{vector}[k] == 1$ ) then
18:      $Reward_{final} += Reward_{vector}[k]$ 
19:   else
20:      $Reward_{final} += -1$ 
21:   end if
22: end for

```

Algorithm 4 Rewarding Function 3

Input: Controllability reward vector $Reward_{vector}$,
 Current state vector $State_{vector}$, State Vector Length K
Output: Final reward $Reward_{final}$

```

1:  $Reward_{final} = 0$ 
2: for  $k \in \{0, \dots, K - 1\}$  do
3:   if  $State_{vector}[k] == 1$  then
4:      $Reward_{final} += Reward_{vector}[k]$ 
5:   else
6:      $Reward_{final} += -1$ 
7:   end if
8: end for

```

when an HT-free circuit is being tested, the detection tool may either classify it as an infected or a clean circuit, *i.e.*, $Prob(FP) + Prob(TN) = 1$ where FP and TN stand for *False Positive* and *True Negative* events. Similarly, for HT-infected circuits, we have $Prob(FN) + Prob(TP) = 1$. FN and FP are two undesirable outcomes at which detectors misclassify the given circuit. However, the FN cases pose a significantly greater danger as they result in a scenario where we rely on an HT-infected chip, whereas an FP case means wasting a clean chip by either not selling or not using it. So, we need to know how the user (might be a security engineer or a company representative) of HT detection tools prioritizes FN and FP cases. We define a parameter α as the ratio of the undesirability of FN over FP . The tool user determines

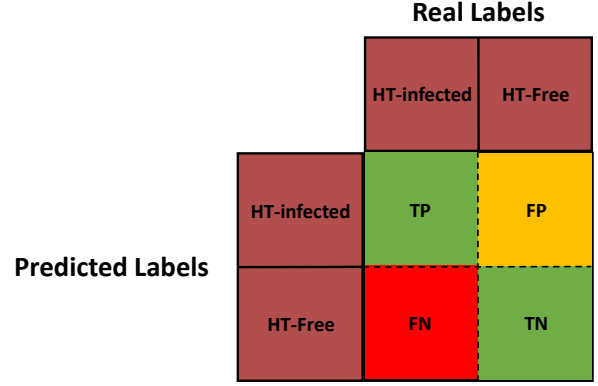


Fig. 7: Possible outcomes of an HT detection trial.

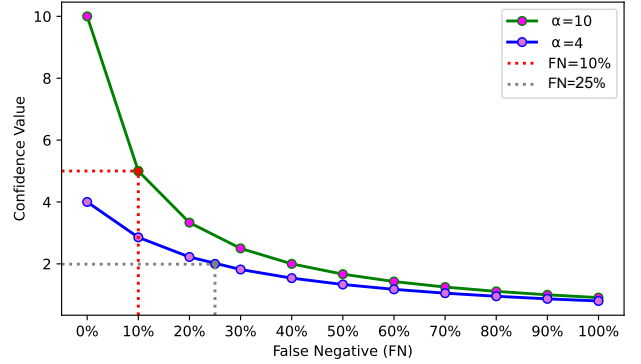


Fig. 8: Confidence value vs. the percentage of FN in our detectors assuming $\alpha = 10$ and $\alpha = 4$

α based on characteristics and details of the application that eventually chips will be employed in, *e.g.*, the risks of using an infected chip in a device with a sensitive application versus using a chip for home appliances. Note that this value is set by the user and not derived from the actual FP and FN . After α is set, it is plugged in Equation 4 and a general confidence basis $Conf.Val$ is computed.

$$Conf.Val = \frac{(1 - FP)}{(1/\alpha + FN)} \quad (4)$$

Using this metric, a fair comparison between HT detection methods can be made regardless of their detection criteria and implementation methodology. The defined confidence metric combines the two undesirable cases with respect to their severity from the security engineer's point of view. The $Conf.Val$ ranges between $[\frac{0.5\alpha}{1+0.5\alpha} .. \alpha]$. The closer the value is to α is equivalent to more confidence in the detector. The absolute minimum of the $Conf.Val = 1/3$ that happens when $\alpha = 1$ and $FP = FN = 50\%$. Note that in this analysis, we assume that FN and FP are independent probabilities. We note that, for some detection methods, FP is always 0. For instance, test-based HT detection methods that apply a test vector to excite HTs use a golden model (HT-free) circuit for comparison and decision-making, and it is impossible for a non-infected circuit to have a mismatch with the golden model (from the perspective of functional simulation). It is impossible

TABLE III: Characteristics of different circuits from ISCAS-85 benchmark

Benchmark	# of Inputs	# of Levels	# of nodes	# of nets	T_{OCR}	T_{HTS}	Description
c432	36	40	352	492	14	0.85	27-Channel Interrupt Controller
c880	60	43	607	889	15	0.82	8-Bit ALU
c1355	41	44	957	1416	20	0.75	32-Bit SEC Circuit
c1908	33	52	868	1304	14	0.90	16-bit SEC/DED Circuit
c2670	233	28	1323	1807	20	0.83	12-bit ALU and Controller
c3540	50	60	1539	2527	15	0.84	8-bit ALU
c5315	178	63	2697	4292	21	0.79	9-bit ALU
c6288	32	240	4496	6801	18	0.8	16x16 Multiplier
c7552	207	53	3561	5433	20	0.8	32-Bit Adder/Comparator

for such methods to falsely detect an HT in a clean circuit. However, our metric is general and captures such cases.

Figure 8 shows the relation between the confidence value and the FN percentage for $\alpha = 10$ and $\alpha = 4$ for a test-based detector. As can be observed, the slopes of the graphs are different when FN approaches zero. The maximum tolerable FN is defined as an upper bound for the FN value at which we gain at least half the maximum confidence. As shown with the dashed lines in Figure 8, the maximum tolerable FN for $\alpha = 4$ and $\alpha = 10$ is, respectively, $FN = 25\%$ and $FN = 10\%$. Based on the figure, it can be inferred that choosing a higher base α will make it more challenging to attain higher confidence values. This fact should be considered when choosing α and interpreting the confidence values.

We believe that, in addition to the detection quality, which can be measured by the proposed confidence value, HT detection methods should also be compared from a computational cost point of view. In particular, we encourage researchers to report the run-time of their methods and the training time, if applicable.

VI. EXPERIMENTAL RESULTS AND DISCUSSION

This section demonstrates the efficiency of the developed HT insertion and detection framework. For our experiments, we use an AMD EPYC 7702P 64-Core CPU with 512GB of RAM to train and test our agents. The training of the RL agents is done using the Stable Baselines library [32] with MLP (multi-layer perceptron) as the PPO algorithm policy [30]. The benchmark circuits are selected from ISCAS-85 [33], which are converted into equivalent circuit graphs using NetworkX [34]. Our toolset is developed in Python to 1) easily adopt available libraries, 2) facilitate future expansions and integration with other tools that researchers may develop.

Table III provides details of the benchmark circuits used in our experiments. The table represents the number of primary inputs (2^{nd} column), logic levels (3^{rd} column), number of nodes including inputs, outputs, and logic gates (4^{th} column), and nets (5^{th} column). We have specified T_{OCR} and T_{HTS} such that 5% of all nets in each circuit are considered as *rare nets* (6^{th} and 7^{th} columns, respectively). This was done to enable a fair comparison between the circuits. Finally, the circuit functionality is listed in the 8^{th} column.

A. Timing Complexity

Table IV provides timing information spent on training the HT insertion and detection agents per circuit. The 2^{nd} column

TABLE IV: Mean HT detection/insertion training time of the RL algorithm for different ISCAS-85 benchmarks

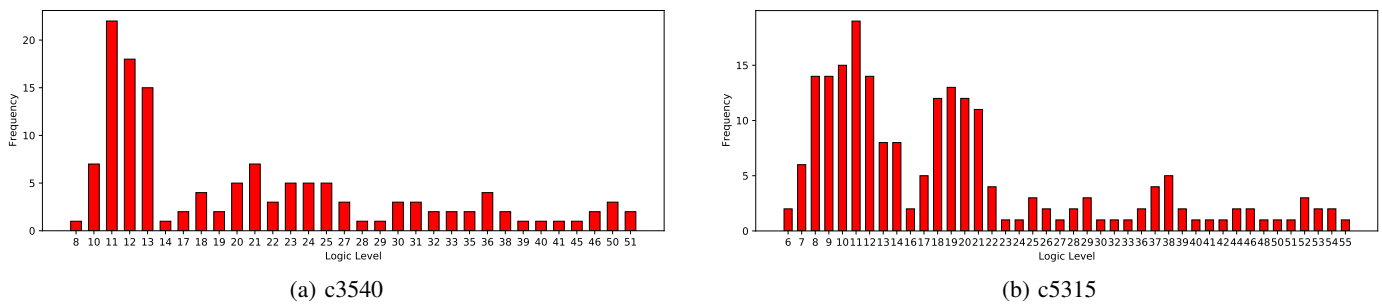
Benchmark	Insertion/Detection Timesteps	Insertion/Detection Training Time
c432	120K / 450K	1 hr 40 m / 1 hr 7 m
c880	132K / 495K	2 hr 36 m / 2 hr 7 m
c1355	145K / 550K	3 hr 10 m / 2 hr 27 m
c1908	160K / 605K	5 hr 25 m / 2 hr 40 m
c2670	175K / 665K	8 hr 1 m / 7 hr 23 m
c3540	192K / 731K	12 hr 1 m / 5 hr 24 m
c5315	211K / 800K	23 hr 16 m / 15 hr 36 m
c6288	232K / 880K	57 hr 18 m / 59 hr 16 m
c7552	255K / 970K	26 hr 15 m / 44 hr 15 m

shows the total timesteps for insertion/detection, and the 3^{rd} column shows the total spent time. We initialize training the inserting agent in c432 with 120K timesteps and an episode length of 450. We increase both values by 10% for each succeeding circuit to ensure enough exploration is made in each circuit as their size grows. As for detection, we start with 450K timesteps and increase it by 10% for subsequent circuits and we keep the episode length at 10. The short episode length allows the agent to experience different states, thereby increasing the chances of exploration. In the testing phase, the test vectors are collected after running the agent for 20K episodes.

In our experiments, c6288 takes the most time in both insertion and detection scenarios (2.5 days) which we argue is reasonable for an attacker and the defense engineer. Note that we have not used any optimization techniques to reduce the number of gates and nets in the benchmarks. Such techniques can notably decrease the RL environment size, and subsequently, the training time. That being said, the impact of optimization techniques on detection/insertion quality should be investigated, but it is not within the scope of this paper.

B. Insertion, Detection, and Confidence Value Figures

Figure 9 illustrates the logical depth distribution of rare nets in c3540 and c5315 circuits. Despite the fact that rare nets are mostly found in the lower logic levels, there are still a significant number of rare nets in the higher levels, which could potentially contribute to the creation of stealthier hardware Trojans. As explained in section III-B, the level of the HT trigger nets is limited by the payload’s level. If a payload is not selected from the higher-level nets, the agent has less opportunity to explore higher-level trigger nets

Fig. 9: Distribution of rare nets in $c3540$ and $c5315$

which might harm the insertion exploration of new HTs. To enable more exploration, we define the following two payload selection scenarios: 1) P_{rand} in which the agent selects payloads randomly, and 2) P_{high} where payload net is selected such that at least 80% of rare nets are within the agent’s sight.

Table V provides information about the number of inserted HTs using P_{rand} and P_{high} scenarios for each benchmark circuit. The 2nd and 3rd columns show the total number of HTs successfully inserted by the agent. The numbers followed by each insertion scenario in the remaining columns show the number of rare nets among the 5-input triggers. For instance, in $c432$, 1866 HTs were inserted under P_{rand} where 1688 of those had 3 rare nets, 160 of those had 4 rare nets, and only 18 of those had 5 rare nets. As can be observed, in most cases, the number of inserted HTs under P_{high} is higher than P_{rand} with the exception of $c6288$ and $c7552$. Also, as the number of rare triggers increases, fewer HTs are inserted. In other words, it becomes more difficult for the RL agent to find HTs with higher rare nets. There are some cases under $P_{rand} - 5$ and $P_{high} - 5$ that the agent could not insert any HTs. These rows in the table are shown as 0, e.g. in $c2670$.

Figure 10 displays the HT detection accuracy percentages for the studied circuits under P_{rand} and P_{high} insertion scenarios. Besides $D1$, $D2$, and $D3$, there is an extra detection scenario called *Combined* where all the test vectors produced by $D1$, $D2$, and $D3$ are consolidated and applied to the circuits for HT detection. No detection rates are reported in cases that no HTs were inserted. It can be observed from both Table V and Figure 10 that despite more inserted HTs in the P_{high} scenario, they do not evade detection any better than the random payload selection scenario and the detection rates are almost the same. Nevertheless, the extra inserted HTs

under P_{high} can be used to train better ML HT detectors. Figure 10 also suggests that the existence of $D1$, $D2$, and $D3$ is vital to providing better HT detection coverage. Figure 11 displays the number of times each detector was ranked first in 9 benchmark circuits under our two insertion strategies. While $D3$ ties with $D2$ under P_{rand} , it becomes the best detector under P_{high} . $D1$ only outperforms in 1 benchmark circuit in both scenarios. The figure suggests that developing HT detectors solely based on signal activity might not achieve the expected outcomes. Nevertheless, $D2$ still plays an essential role in overall HT detection accuracy. The impact of the *Combined* scenario is vital as it improves the overall detection accuracy in most cases. For instance, in $c3540$, none of the detectors can perform better than 60% in the P_{rand} scenario while the *Combined* detection accuracy is nearly 75%. It also can be seen that adding more rare nets to the HT trigger does not necessarily lead to stealthier HTs. For example, in $c880$, $c1355$, and $c1908$, there are HTs with 5 trigger nets that were 100% detected while the detection accuracy was less for HTs with fewer rare triggers in the same circuits.

Another important observation is the different magnitude of detection accuracy among the benchmark circuits. While we achieve, 100% accuracy in $c6288$, the same figure is about 25%-30% lower in $c3540$ and $c6288$. We know from Table III that $c6288$ is a multiplier circuit. It contains 240 full and half adders arranged in a 15×16 matrix [35]. $c3540$, on the other hand, has 14 control inputs for multiplexing and masking data. $c7552$ also contains multiple control signals and bit masking operations. Our hypothesis is that the detection accuracy is higher in $c6288$ due to having fewer control signals that disable circuit components and signals. Accordingly, they get more frequently activated in $c6288$ compared to $c3540$ and $c7552$. **In other words, these results imply that inserting**

TABLE V: Number of inserted HTs under P_{rand} and P_{high} scenarios for ISCAS-85 benchmark circuits

Benchmark	$P_{rand} - Total$	$P_{high} - Total$	$P_{rand} - 3$	$P_{high} - 3$	$P_{rand} - 4$	$P_{high} - 4$	$P_{rand} - 5$	$P_{high} - 5$
c432	1866	2788	1688	2331	160	453	18	4
c880	1954	2116	1595	1736	327	373	32	7
c1355	921	1400	815	1116	86	268	20	16
c1908	1247	1576	1121	1240	126	321	0	15
c2670	206	434	188	406	18	28	0	0
c3540	410	767	367	703	41	64	2	0
c5315	434	797	406	719	28	77	0	1
c6288	531	475	459	426	67	46	5	3
c7552	769	683	704	615	64	67	1	1

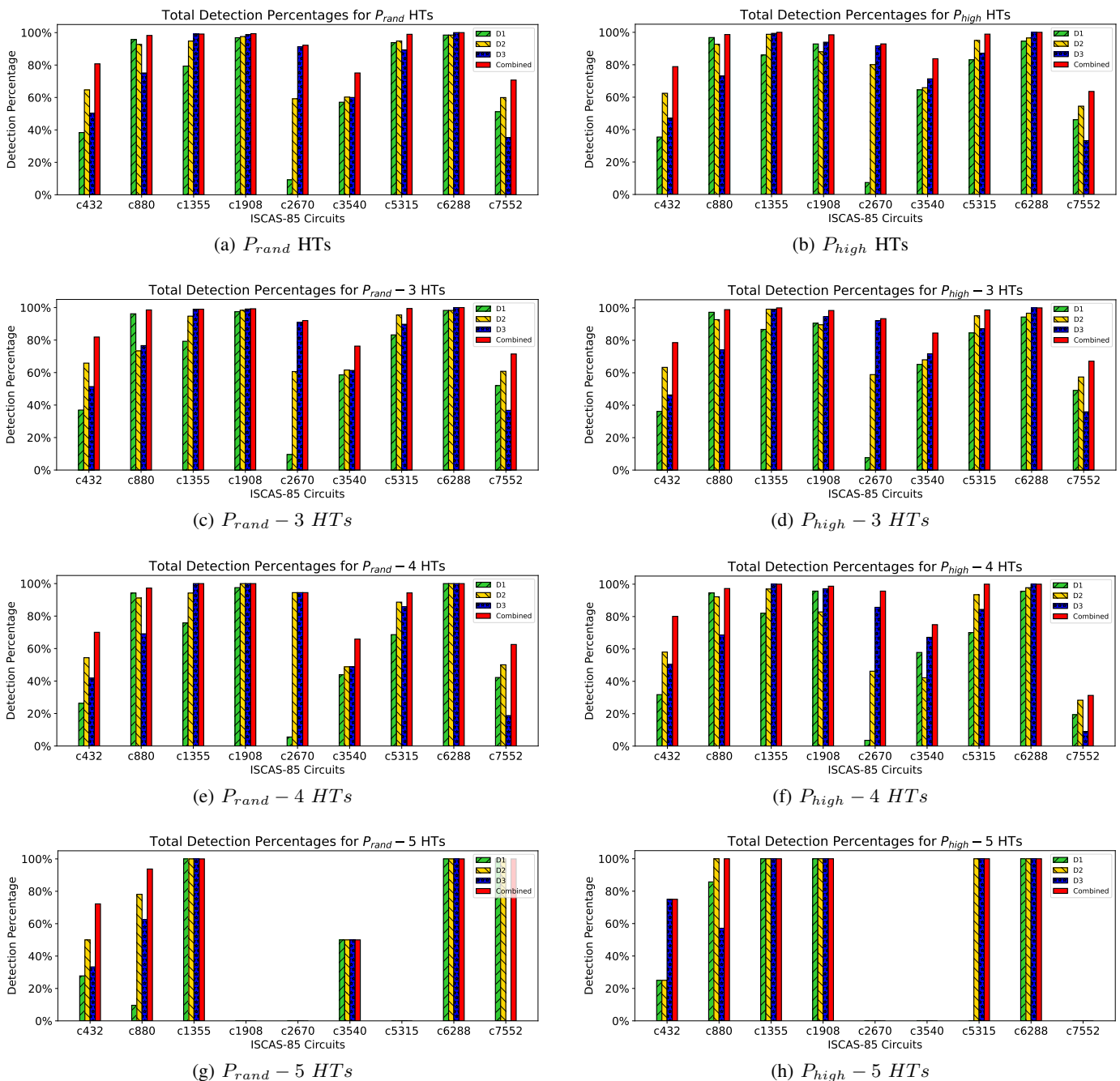


Fig. 10: Detection accuracy of D1, D2, D3, and *Combined* scenarios under P_{high} and P_{high} insertion scenarios in ISCAS-85 benchmark circuits

HTs in control paths can lead to stealthier HTs than data paths in circuits. Another interesting finding pertains to the detection rate in *c432*. After administering 100K random test patterns, we discovered that the rarest net in the circuit was triggered 7% of the times, which is in stark contrast to other circuits where a multitude of nets exhibit switching activity of less than 1%. It implies that the inserted HTs in *c432* are probably activated easier with random test patterns. To prove this hypothesis, we generated 20K random test patterns and passed them to the circuit. These test patterns detected 99% of HTs, indicating that attackers should carefully evaluate the activity profile of the nets prior to compromising circuits.

To further evaluate the efficacy of our HT detectors, we compare the *Combined* detector with DETERRENT [9] and HW2VEC [25], two state-of-the-art HT detectors. We use the test vectors generated by DETERRENT [9] and collect detection figures for 4 reported ISCAS-85 benchmark circuits, namely *c2670*, *c5315*, *c6288*, and *c7552*². We also replicate the steps in HW2VEC [25] by gathering the *TJ_RTL* dataset which contains 26 HT-infected (labeled as '1') and 11 HT-Free circuits (labeled as '0'). We train an MLP (multi-layer percep-

²We reached out to the authors of TARMAC and TGRL techniques but we did not receive the test patterns at the time of submission.

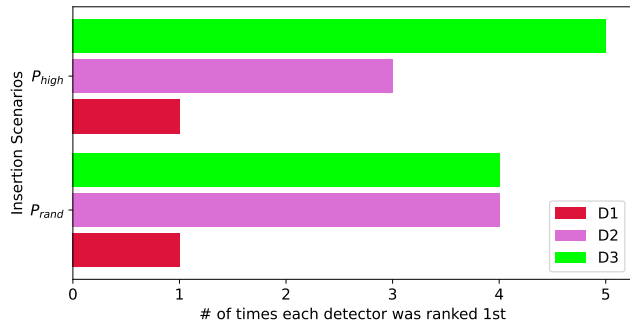
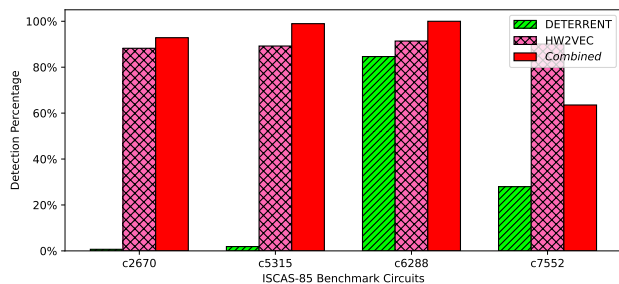
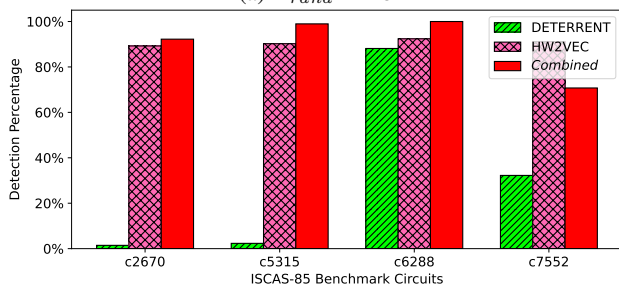


Fig. 11: Comparing the number of times each of $D1$, $D2$ and $D3$ are ranked as the best detector in our two insertion scenarios



(a) P_{rand} HTs



(b) P_{high} HTs

Fig. 12: Comparison of HW2VEC [25], *Combined*, and DETERRENT [9] detection rates under P_{rand} and P_{high} insertion scenarios

tron) binary classifier using a leave-one-out cross validation method to detect the HTs. For the test dataset, we collect the graph embeddings of the HTs generated by the inserting RL agent. Additionally, we add an HT-free version of the original ISCAS-85 ccircuits and another one synthesized with the academic *NanGateOpenCell45nm* library to the test batch to record the number of *TNs* and *FPs*. As was explained and shown in Table II, DETERRENT solely takes signal activity into account while HW2VEC captures structural information of circuits.

Figure 12 shows the detection accuracy of each HT detector for each benchmark circuit. The detection accuracy is reported for the total inserted HTs in Table V for both P_{rand} and P_{high} insertion scenarios. The figure shows that the *Combined* detector outperforms DETERRENT and HW2VEC in 3 of our benchmark circuits. The average detection rate among the 4 benchmarks is 87% percent. While the detection gap

between *Combined* and DETERRENT is significant in $c2670$ and $c5315$, it is less evident in $c6288$ and $c7552$. HW2VEC, on the other hand, demonstrates minimal detection variance in all 4 circuits and outperforms *Combined* in $c7552$. Furthermore, HW2VEC illustrates robust performance with HT-Free circuits, where it correctly classifies all of them as *TNs* and a *FP* rate of 0.

In another experiment, we train our MLP with *TJ_RTL* + *EPFL* [36] benchmark suites to obtain a more balanced dataset (26 instances labeled as '1' and 30 instances labeled as '0'). While the *FP* remains 0, similar to the previous experiment, the HT detection accuracy drops to 48%. This sheds light on the shortcomings of the current benchmarks used for training ML HT detectors and it raises the necessity of having more diverse and larger dataset to attain more dependable results. Overall, these two experiments demonstrate the potential of the RL inserting agent and the advantages of a multi-criteria detector compared to a single-criterion (DETERRENT) HT detector.

Table VI shows the individual detection contribution of $D1$, $D2$, and $D3$ towards overall HT detection for each benchmark circuit. The 2nd, 4th and 6th columns display the number of HTs exclusively detected by each detector followed by their contribution in the overall HT detection in the 3rd, 5th and 7th columns for $D1$, $D2$, and $D3$, respectively. As can be inferred, $D3$ has the highest individual contribution, followed by $D2$ and $D1$. This table serves as another piece of evidence of the importance of the multi-criteria HT detector for higher accuracy.

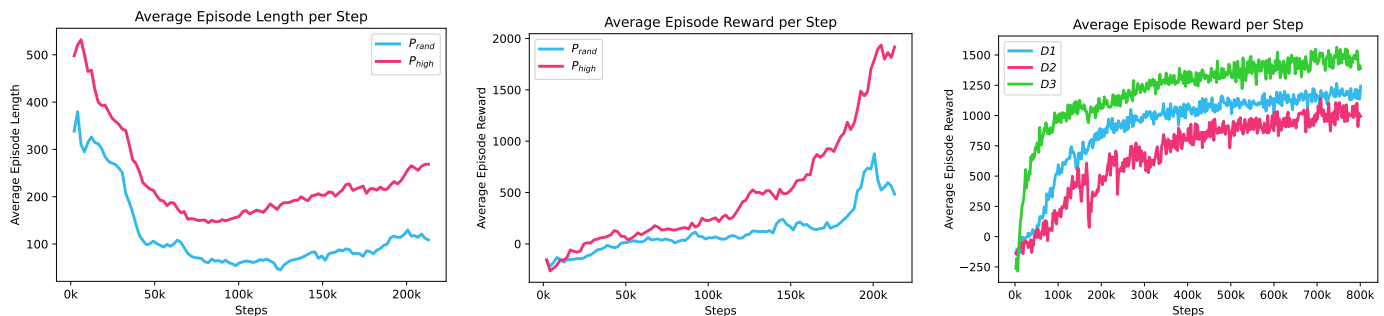
To compute the confidence value of each detector, the overall detection accuracy of each detector is computed in all 9 circuits under both insertion scenarios. Then, each averaged value is plugged in Equation 4. Assuming $\alpha = 10$, the confidence values for each of $D1$, $D2$, $D3$, and *Combined* scenarios are 2.43, 3.36, 3.09, and 5.13, respectively. Thus, the security engineer can put more confidence in the *Combined* detector since it has the highest confidence values. DETERRENT's and HW2VEC's confidence values are 1.24 and 4.34, respectively.

C. Average Episode Length and Reward

Figure 13 shows the average episode length and reward of the inserting and detector RL agents for the $c5315$ benchmark circuit. As can be seen from Figure 13.a, initially, the agent leans more towards ending the training episodes to avoid

TABLE VI: Individual contribution of $D1$, $D2$, and $D3$ in detection of unique HTs

Circuit	$D1$ #	$D1$ %	$D2$ #	$D2$ %	$D3$ #	$D3$ %
c432	2	0.1%	275	14.74%	297	15.86%
c880	49	2.52%	16	0.81%	16	0.81%
c1355	0	0%	0	0%	40	4.34%
c1908	1	0.08%	1	0.08%	13	1.04%
c2670	0	0%	1	0.48%	66	32.03%
c3540	7	1.70%	29	7.07%	18	4.39%
c5315	1	0.24%	8	1.93%	9	2.17%
c6288	0	0%	0	0%	8	1.51%
c7552	16	2.08%	29	3.77%	15	1.95%



(a) Average Episode Length per Step in HT insertion for $c5315$ (b) Average Episode Reward per Step in HT insertion for $c5315$ (c) Average Episode Reward per Step in HT Detection for $c5315$

Fig. 13: The average episode length and reward vs. the number of steps in both HT insertion and detection for $c5315$

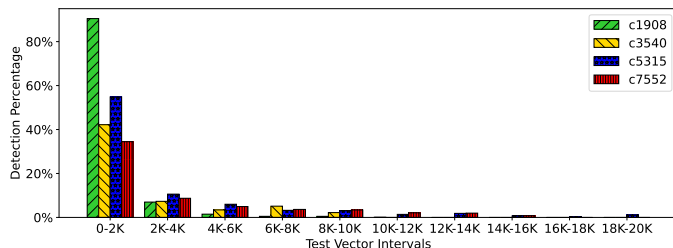


Fig. 14: The number of generated test vectors (x-axis) vs. the HT detection accuracy (y-axis)

further losses. This trend continues until it gradually starts to increase the episode length, resulting in an increase in reward, which can be observed in Figure 13.b. Eventually, the agent collects more and more rewards. Although the agent accumulates higher rewards in P_{high} , the detection rate is not significantly different from P_{rand} . Figure 13.c demonstrates the agent’s ability to augment rewards in our three detection scenarios in an almost steady pace; it learns how to increase rewards along the way. It is worthwhile to point out that the proposed RL framework can save the state of the RL models at arbitrary intervals, which is useful to test the efficacy of the agent at different timesteps. Note that since the detector’s episode length is always 10, this data was not included in the graph. The agent can always be trained for longer steps, but one should consider the trade-off between the amount of time required and the accuracy achieved.

D. Test Vector Size vs. Accuracy

We also investigate the relationship between the number of applied test vectors and the HT detection accuracy. For this experiment, we collect a set of test vectors that have obtained a certain minimum of reward. To identify such vectors, we run the trained RL agent for 20K episodes. We set a cut-off reward of one-tenth of the collected reward in the last training episode. We collect 20K test vectors that surpass this reward threshold. The HT detection distribution of the collected test vectors is shown in Figure 14 for $c1908$, $c3540$, $c5315$, and $c7552$ under the P_{rand} insertion scenario and the $D2$ detection scenario. The x-axis displays the intervals of the applied test vectors and the y-axis shows the detection

percentage of each particular interval. As can be seen, the first 2K vectors have the greatest contribution toward HT detection. This figure is nearly 90% for $c1908$ while it is just below 40% for $c7552$. A similar comparison can be made between different HT detectors to help us find out the relation between the quantity (number of test vectors) and the quality (the detection accuracy). Such analysis leads us to answer this question “Does adding more test vectors to the testing batch improve detection?” If the answer is negative, adopting more intelligent rewarding functions might be considered to offset this diminishing returns effect. That being said, in certain instances, adding more test batches leads to higher detection rates. We tested this scenario for $c3540$ where the *Combined* detection rate with 20K test patterns is around 80% in the P_{rand} scenario. We ran the trained detector agents $D1$, $D2$, and $D3$ for 20K episodes, but this time, we collected all the test patterns that returned positive rewards. Accordingly, we collected 191K, 183K, 121K for $D1$, $D2$, and $D3$ and the detection rates were 89%, 86%, and 97%, respectively.

VII. CONCLUSIONS

This paper presented the first framework for joint HT insertion and detection. Both the inserting and detection RL agents have tunable rewarding functions that enable researchers to experiment with different approaches to the problem. This framework will accelerate HT research by helping the research community to evaluate their insertion/detection ideas with less effort. Our inserting tool provides a robust dataset that can be used for developing finer HT detectors, and our detector tool emphasizes the need for a multi-criteria detector that can cater to different HT insertion mindsets. We also presented a methodology to help the community compare HT detection methods, regardless of their implementation details. We apply this methodology to our HT detection and discovered that our tool offers the highest confidence in HT detection when using a combined detection scenario. As a future work, we would like to explore more benchmarks and create a more diverse HT dataset for the community.

REFERENCES

- [1] “Securing defense-critical supply chains: An action plan developed in response to president biden’s executive order 14017.” [Online]. Available: <https://tinyurl.com/3wmdx5d>

- [2] Z. Pan and P. Mishra, "Automated test generation for hardware trojan detection using reinforcement learning," in *Proceedings of the 26th Asia and South Pacific Design Automation Conference*, 2021, pp. 408–413.
- [3] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of hardware trojans and maliciously affected circuits," *Journal of Hardware and Systems Security*, vol. 1, no. 1, pp. 85–102, 2017.
- [4] A. Sarihi, A. Patooghy, A. Khalid, M. Hasanzadeh, M. Said, and A.-H. A. Badawy, "A survey on the security of wired, wireless, and 3d network-on-chips," *IEEE Access*, 2021.
- [5] H. Salmani, M. Tehranipoor, and R. Karri, "On design vulnerability analysis and trust benchmarks development," in *2013 IEEE 31st international conference on computer design (ICCD)*. IEEE, 2013, pp. 471–474.
- [6] H. Salmani, "Cotd: Reference-free hardware trojan detection and recovery based on controllability and observability in gate-level netlist," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 338–350, 2016.
- [7] K. Hasegawa, M. Yanagisawa, and N. Togawa, "Trojan-feature extraction at gate-level netlists and its application to hardware-trojan detection using random forest classifier," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017, pp. 1–4.
- [8] S. M. Sebt, A. Patooghy, H. Beitollahi, and M. Kinsy, "Circuit enclaves susceptible to hardware trojans insertion at gate-level designs," *IET Computers & Digital Techniques*, vol. 12, no. 6, pp. 251–257, 2018.
- [9] V. Gohil, S. Patnaik, H. Guo, D. Kalathil, and J. Rajendran, "Deterrent: detecting trojans using reinforcement learning," in *Proceedings of the 59th ACM/IEEE Design Automation Conference*, 2022, pp. 697–702.
- [10] J. Cruz, Y. Huang, P. Mishra, and S. Bhunia, "An automated configurable trojan insertion framework for dynamic trust benchmarks," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 1598–1603.
- [11] Y. Lyu and P. Mishra, "Scalable activation of rare triggers in hardware trojans by repeated maximal clique sampling," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 7, pp. 1287–1300, 2020.
- [12] M. Fyrbiak, S. Wallat, P. Swierczynski, M. Hoffmann, S. Hoppach, M. Wilhelm, T. Weidlich, R. Tessier, and C. Paar, "HAL- the missing piece of the puzzle for hardware reverse engineering, trojan detection and insertion," *IEEE Transactions on Dependable and Secure Computing*, 2018.
- [13] S. Yu, W. Liu, and M. O'Neill, "An improved automatic hardware trojan generation platform," in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2019, pp. 302–307.
- [14] A. Sarihi, A. Patooghy, P. Jamieson, and A.-H. A. Badawy, "Hardware trojan insertion using reinforcement learning," in *Proceedings of the Great Lakes Symposium on VLSI 2022*, 2022, pp. 139–142.
- [15] A. Sarihi, P. Jamieson, A. Patooghy, and A.-H. A. Badawy, "Multi-criteria hardware trojan detection: A reinforcement learning approach," *arXiv preprint arXiv:2304.13232*, 2023.
- [16] "Trust-Hub," <https://trust-hub.org/#/home>, accessed: 2022-12-19.
- [17] V. Jyothi, P. Krishnamurthy, F. Khorrami, and R. Karri, "Taint: Tool for automated insertion of trojans," in *2017 IEEE International Conference on Computer Design (ICCD)*. IEEE, 2017, pp. 545–548.
- [18] S. Wallat, M. Fyrbiak, M. Schlögel, and C. Paar, "A look at the dark side of hardware reverse engineering-a case study," in *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*. IEEE, 2017, pp. 95–100.
- [19] J. Cruz, P. Gaikwad, A. Nair, P. Chakraborty, and S. Bhunia, "Automatic hardware trojan insertion using machine learning," *arXiv preprint arXiv:2204.08580*, 2022.
- [20] K. Nozawa, K. Hasegawa, S. Hidano, S. Kiyomoto, K. Hashimoto, and N. Togawa, "Generating adversarial examples for hardware-trojan detection at gate-level netlists," *Journal of Information Processing*, vol. 29, pp. 236–246, 2021.
- [21] L. H. Goldstein and E. L. Thigpen, "Scoop: Sandia controllability/observability analysis program," in *Proceedings of the 17th Design Automation Conference*, 1980, pp. 190–196.
- [22] V. Gohil, H. Guo, S. Patnaik, and J. Rajendran, "Attrition: Attacking static hardware trojan detection techniques using reinforcement learning," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 1275–1289.
- [23] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "Mero: A statistical approach for hardware trojan detection," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 396–410.
- [24] L. Goldstein and E. Thigpen, "Scoop: Sandia controllability/observability analysis program," in *17th Design Automation Conference*, 1980, pp. 190–196.
- [25] S.-Y. Yu, R. Yasaei, Q. Zhou, T. Nguyen, and M. A. Al Faruque, "Hw2vec: A graph learning tool for automating hardware security," in *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2021, pp. 13–23.
- [26] C. Wolf, J. Glaser, and J. Kepler, "Yosys-a free verilog synthesis suite," in *Proceedings of the 21st Austrian Workshop on Microelectronics (Austrochip)*, 2013.
- [27] L. Bassett, *Introduction to JavaScript Object Notation: A To-the-Point Guide to JSON*. O'Reilly Media, 2015. [Online]. Available: <https://books.google.com/books?id=Qv9PCgAAQBAJ>
- [28] G. Brockman, V. Cheung, L. Pettersson, J. Schneider, J. Schulman, J. Tang, and W. Zaremba, "Openai gym," *CoRR*, vol. abs/1606.01540, 2016. [Online]. Available: <http://arxiv.org/abs/1606.01540>
- [29] M. L. Bushnell, "Essentials of electronic testing for digital," *Memory & Mixed-Signal VLSI Circuits*, 2000.
- [30] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," *arXiv preprint arXiv:1707.06347*, 2017.
- [31] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Transactions on Neural Networks and Learning Systems*, 2019.
- [32] A. Raffin, A. Hill, M. Ernestus, A. Gleave, A. Kanervisto, and N. Dormann, "Stable baselines3," 2019.
- [33] D. Bryan, "The iscas85 benchmark circuits and netlist format," *North Carolina State University*, vol. 25, p. 39, 1985.
- [34] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using networkx," in *Proceedings of the 7th Python in Science Conference*, G. Varoquaux, T. Vaught, and J. Millman, Eds., Pasadena, CA USA, 2008, pp. 11 – 15.
- [35] "benchmark," <https://web.eecs.umich.edu/~jhayes/iscas.restore/benchmark.html>, accessed: 2023-02-07.
- [36] L. Amarú, P.-E. Gaillardon, and G. De Micheli, "The eplf combinational benchmark suite," in *Proceedings of the 24th International Workshop on Logic & Synthesis (IWLS)*, no. CONF, 2015.