



# Vulnerability Information Sharing Platform for Securing Hardware Supply Chains

Kento Hasegawa<sup>1</sup><sup>a</sup>, Katsutoshi Hanahara<sup>2</sup>, Hiroshi Sugisaki<sup>1</sup>, Minoru Kozu<sup>1</sup>,  
Kazuhide Fukushima<sup>1</sup><sup>b</sup>, Yosuke Murakami<sup>1</sup> and Shinsaku Kiyomoto<sup>1</sup>

<sup>1</sup>*KDDI Research, Inc., Japan*

<sup>2</sup>*KDDI Foundation, Japan*

**Keywords:** Supply Chain, Design, Hardware Trojan, Detection, Industry.

**Abstract:** The rise of complex global supply chains has increased the risk of malicious actors attempting to insert malicious functions, called hardware Trojans (HTs), into hardware components and devices. Although many HT detection methods have been proposed over a decade, implementing them in industries may take a long time due to concerns about these methods. In this paper, we propose a repository system to manage vulnerability information for securing hardware supply chains and investigate the demand and barriers to introducing hardware Trojan detection schemes in the industry. First, we design a scheme to share the results of HT detection methods. Second, we design questionnaires to investigate the actual situation of the industry's awareness of the threat of HTs and other hardware security issues. We conclude that there is a gap between academics and the industry, whereas many business operators are concerned about the threat of HTs.


## 1 INTRODUCTION


The rise of complex global supply chains has increased the risk of malicious actors attempting to insert malicious functions, called hardware Trojans (HTs), into hardware components and devices (Francq and Frick, 2015; Xiao et al., 2016). HTs may leak internal confidential information, degrade performance, or alter the original functionality of hardware components. Many HT detection methods have been proposed for over a decade to defend hardware products from the insertion of HTs. However, these methods were proposed from the viewpoint of academic research. The feasibility of HTs in the real world and the industry's awareness of the threat posed by HTs have not been sufficiently assessed. Almeida et al. investigated the feasibility of ransomware attacks as HTs (Almeida et al., 2022). This feasibility study demonstrated that there are no barriers for an adversary to devise hardware ransomware in a hardware product. Although this result suggests that HTs can be easily realized, the actual awareness of business operators across various industries has not been investigated.

In this paper, we focus on the actual situation of the industry as it relates to semiconductor supply chains. First, we propose a scheme to share the results of HT detection methods in the hardware design phase. In terms of software management, vulnerability information for software is publicly shared on several platforms, such as the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVEs). Inspired by such platforms, we design a framework to share vulnerability information for hardware. Second, we design questionnaires to investigate the actual situation of the industry's awareness of the threat of HTs. Through the questionnaires, we clarify the demand and concerns with respect to HT detection methods and security assessment schemes in industries.

The contributions of this paper can be summarized as follows:

- We propose a repository operation scheme to share vulnerability information of hardware products. The scenario using the repository is considered a use case for HT detection methods in industries.
- We designed questionnaires to confirm the needs, effectiveness, and concerns regarding the repository operation scheme and conducted a survey tar-

<sup>a</sup> <https://orcid.org/0000-0002-6517-1703>

<sup>b</sup> <https://orcid.org/0000-0003-2571-0116>

getting 15 companies.

- We found that HT detection methods are attractive in industries, and the repository scheme will be enhanced if the scheme covers the whole supply chain, i.e., the whole lifecycle of semiconductor products.

## 2 PRELIMINARIES

### 2.1 Hardware Trojan (HT)

HTs are malicious modifications inserted into integrated circuits (ICs) during the manufacturing process with the intention of causing harmful impacts for manufacturers or IC users. They can be inserted by a malicious adversary with access to the design or fabrication process or by a rogue employee within hardware supply chains. HTs can perform various malicious functions, such as leaking confidential internal information, disabling critical functions, or causing the device to malfunction. A specific trigger, such as a particular input or a specific time, can activate HTs.

HTs are usually composed of small circuits, making them difficult to detect during the design phase. HTs can also be designed to avoid detection by testing methods and to remain dormant until a specific trigger activates them. Adversaries can insert HTs in any phase in hardware supply chains. Particularly, inserting HTs in the design phase is relatively easy and effective because one modification in a design spreads many products.

### 2.2 Hardware Trojan Detection

In this paper, we focus on HT detection methods in the design phase to detect HTs earlier in supply chains. A hardware design is described in hardware description languages (HDLs). An adversary may alter the design described in HDL to insert HTs or may provide intellectual property that is infected with HTs.

There are several HT detection approaches in the design phase. A promising method is a structural feature-based approach, in which HT-specific features are identified from a tested hardware design (Yang et al., 2020). In a structural feature-based approach, the structure of a circuit is extracted based on the hardware design. According to (Oya et al., 2015), specific features appear in HT circuits. For example, a trigger circuit in an HT has many fan-ins to implement a rarely triggered condition. The method proposed in (Oya et al., 2015) suggests that feature values that help identify HTs can be extracted from hardware designs.

Based on the findings, HT detection methods using machine learning have been proposed (Hasegawa et al., 2017b; Hasegawa et al., 2017a; Li et al., 2020; Huang et al., 2020). There are two phases for machine learning-based HT detection: the feature extraction phase and the machine learning phase. In the feature extraction phase, a set of possible features that can help identify HTs are extracted from hardware designs (i.e., program codes written in HDL). Then, a model is trained with the extracted feature values in the machine learning phase. The trained model is expected to identify HTs from a given hardware design.

However, there are barriers to implementing HT detection in industries. A major barrier is the cost of HT detection. Performing HT detection will consume some time, thus delaying manufacturing processes. Many vendors may doubt if the benefit of HT detection is greater than the cost.

In this paper, we survey the awareness of HT detection in industries from the perspective of these points. First, to make HT detection beneficial, we propose a repository operation scheme to share the vulnerability information between business operators. Specifically, the list of hardware components and their HT detection results are stored in the repository system. Using this repository system and its operation scheme, we conduct questionnaires to investigate the feasibility and effectiveness.

## 3 METHODOLOGY

In this section, we propose a repository system to share vulnerability information, such as the reports of HT detection. This repository aims to enhance the security of hardware supply chains, particularly in the design phase.

### 3.1 Overview of the Repository Operation Scheme

We propose a scheme to share the results of HT detection as a demonstration. Figure 1 shows an overview of the repository operation scheme that we designed.

Based on the HT detection methods, we design the scheme to share the hardware vulnerability information between business operators. There are three roles for the repository users: administrators, manufacturers, and inspection agencies. Administrators manage the users and contents of the repository. Manufacturers can register their product information in the repository and view the design information registered by other manufacturers. Inspection agencies can register the inspection results of a product that has been

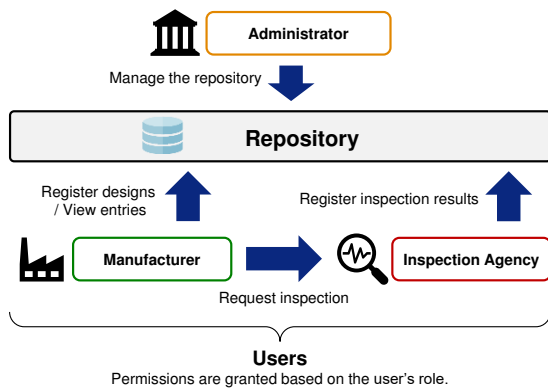


Figure 1: Overview of the repository operation scheme.

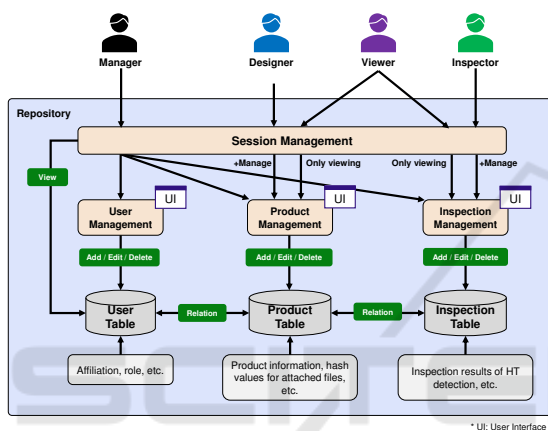


Figure 2: Overview of the repository architecture.

registered in the repository.

### 3.2 Repository Architecture

Figure 2 shows an overview of the repository architecture. In the repository, the database includes mainly three tables: the user, product, and inspection tables. Since the repository targets the management of the hardware design phase, the product here indicates hardware design products.

The user table stores information regarding the repository users, such as their names, affiliations, email addresses, and roles. Administrators assign a role to a user, and users without the administrator role cannot change their role. The details of the user roles are explained later.

The product table includes information regarding hardware design products, such as the designs for processors and interfaces. Users assigned to the manufacturer role can register their product information to the product table, and other users can only see the product information. Users who are authorized can register product information, such as the prod-

uct name, product version, and application category of the product. Documents, including datasheets and hardware design deliverables, can be attached to the product information. The product management function in the repository system provides a user interface that shows detailed product information and the part lists used in the product. Since some attached files cannot be disclosed, the user who registers product information can determine whether the information is disclosed.

The inspection table includes information regarding the vulnerabilities found in hardware designs. Users assigned to the inspection agency role can register their inspection reports to the inspection table. The inspection report includes the results of design testing, such as HT detection and formal verification, and is associated with a product record. The inspection record includes the date of inspection and inspection result.

### 3.3 Scenario of Repository Operation

In this repository scheme, the following scenario is considered.

- **Step 1.** A manufacturer registers their hardware design products to the repository and requests an inspection agency to inspect their products.
- **Step 2.** An inspection agency assesses the vulnerability of the products using HT detection methods and reports the evaluation results.
- **Step 3.** The evaluation results are attached to the product on the repository. These results can be seen by repository users.

When a manufacturer hopes to use an IC chip, they can refer to the repository and check the vulnerability information. If they find a vulnerability or risk information, they can stop using the product. Otherwise, they can feel secure in using the product.

## 4 EVALUATION

### 4.1 Implementation Result

We implemented the repository system as a web application. The tables are stored as a MySQL database, and the backend of the web application is implemented using a Python framework. Using this web application, users, including hardware designers, manufacturers, and inspection agencies, can refer to the information stored in the repository and edit information within their authority.

Design Information	
<a href="#">Upload Design Information</a>	
Design ID	b2ab1f6b2-66a1-42ad-88cc-ad860b8982b9
User	designer
Design Name	0-Soc
Design Version	1.0.0
Designer Organization	1-Designer
Hash	
Digital Signature	
Stored at	
Previous Version	Undecided
Valid Flag	Valid
Registration Date	11/11/2022 14:31:47
Update Date	11/11/2022 14:32:24
Note	

Figure 3: Example of a web form of the repository system.

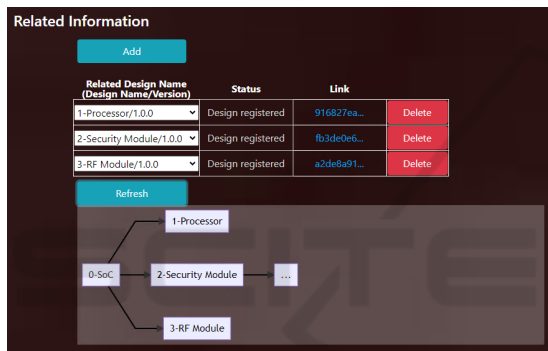


Figure 4: Illustration of the part composition on the repository system.

Figure 3 shows a form of the repository system to register design information. Since the repository is implemented as a web application, users can edit records on a browser.

Figure 4 shows the part composition of a design registered in the repository system. The repository system visualizes the relationship of the parts.

## 4.2 Questionnaire Survey

To investigate the feasibility of the repository operation scheme, we designed questionnaires and conducted a survey based on the designed questionnaires.

There are five categories in the designed questionnaires: (a) basic information, (b) current situations, (c) needs, (d) effectiveness and feasibility, and (e) risk measures in supply chains. The questions are described in Tables 1–6 along with the responses corresponding to the questions.

The questionnaires were conducted through a consulting firm. For a questionnaire survey, we col-

Table 1: Questions and responses to QA – basic information.

QA1	Business description.
	• Electronics or Vehicle
QA2	Position in the supply chain.
	• Semiconductor manufacturers, fabless vendors, EDA vendors, or vehicle manufacturers
QA3	Revenue.
	• More than 100 M USD: 12
	• Less than 100 M USD: 3
QA4	Number of employees.
	• More than 10000: 13
	• Less than 10000: 2
QA5	Country of headquarters.
	• North America: 5, EU: 4, Asia: 6
QA6	Department of the respondent.
	• Design, Development, Solution or Marketing
QA7	Position of the respondent.
	• Manager or Section head

lected 15 respondents from around the world, including North America, Europe, and Asia. We covered three business types: integrated manufacturer, horizontally specialized manufacturer, and implementation vendor. When asking the questions, the purpose of the survey and the repository scheme proposed in Section 3 were explained to the respondents. The requester of the questionnaires was not disclosed to avoid bias. The survey was conducted from August 2022 to January 2023. In the following section, we provide the questions and responses. Due to page limitations, the representative responses are shown in the response tables.

### 4.2.1 QA: Basic Information

In this part, we asked for basic information about the respondents' affiliation and themselves.

Table 1 shows the summary of the responses to the QA section. The business areas covered semiconductor manufacturers, fabless vendors, EDA vendors, and vehicle manufacturers. The headquarters' countries cover major regions, including North America, Europe, and Asia. To collect feedback from production and development fields, the respondents were mainly stakeholders from the development and solution departments. Since the questionnaires are related to actual design or manufacturing processes, the respondent is chosen from a manager or a section head who understands actual situations.

Table 2: Questions and responses to QB – current situations.

QB1	Does your company investigate the IPs and parts from a security viewpoint before introducing them to the design?
	<ul style="list-style-type: none"> <li>• We do not verify IPs introduced to products. Instead, we verify the final products.</li> <li>• We rigorously inspect products when purchasing. We also certify vendors. However, we use the evaluation metric of quality (i.e., defective rate), not of security.</li> </ul>
QB2	Are there any schemes to share alerts when doubt about some IPs or products occurs?
	<ul style="list-style-type: none"> <li>• A scheme has been established to respond to an issue and to address the issue with internal and external parties.</li> </ul>
QB3	Are there any schemes to share alerts when doubt about your product occurs?
	<ul style="list-style-type: none"> <li>• We have not experienced any problems regarding our products. If this happens, we leverage the scheme to share information about the issues of products.</li> </ul>

#### 4.2.2 QB: Current Situations

In this part, we confirmed the current situation regarding the industry's awareness of HTs. Specifically, we aim to clarify that IPs are investigated from a security viewpoint. In general, hardware design houses aim to provide hardware designs that have sufficient performance and functionality according to specifications. However, the awareness of security incidents, such as being infected with HTs, has not been investigated. We expect the questions in this part to reveal the current attitude toward security perspectives.

Table 2 shows the summary of the responses to the QB section. Few companies investigate IPs when introducing them. Instead, the final products are sufficiently verified in terms of satisfying the specifications and quality. However, such verification aims to confirm the quality of the products, not in terms of security. Remember that HTs are stealthily inserted into products. Thus, it is difficult to detect HTs under current situations.

Most companies have schemes to share issues with their products. When an issue is found, the information is shared with the whole company through the scheme. The scheme can be utilized if a problem in hardware designs, such as an HT, is found.

In summary, currently, there is a scheme to share vulnerability information with the whole company. However, a security-specific investigation has not been sufficiently conducted.

#### 4.2.3 QC: Needs

In this part, we confirmed the need for HT detection methods without considering feasibility. Since hardware supply chains are exposed to geopolitical risks, hardware vendors and manufacturers may pay attention to such security concerns. Security assessment processes, such as HT detection, can be a solution to this concern. In this situation, the cost of introducing

a security assessment process can be a problem. This section clarifies these questions.

Table 3 shows the summary of the responses to the QC section. Most companies were interested in security assessment tools for hardware designs. In particular, identifying counterfeit products is desired. To ensure the neutrality and reliability of the security assessment, many companies expect third-party organizations to perform the security assessment. However, the cost of the security assessment is a major problem. Due to the competition over price, design houses cannot cover the cost. Instead, it would be better for business operators or industry organizations to cover the cost.

#### 4.2.4 QD: Effectiveness and Feasibility

In this part, we exhibited several examples of HT detection methods and asked the respondents for an evaluation regarding the efficiency and feasibility of these methods. Although many HT detection methods have been studied in recent years, the feasibility of such methods has not been discussed. In this section, we collected opinions on HT detection from business operators.

In the QD4 question, we asked what level of design information your company can provide for the security assessment process. Although the security assessment process requires the analysis of hardware designs, hardware design information is confidential in most cases. We provided several examples for the question to clarify the possible resources to be disclosed. Table 4 shows the possible resources for the QD4 question. Since hardware designs written in HDL (the QD4-a option) are highly confidential information for most vendors, we provide QD4-b as another option. The QD4-b option shows feature extraction techniques from a hardware design. The extracted features can be used for HT detection, and original designs cannot be restored using the extracted



Table 3: Questions and responses to QC – needs.

QC1	Are you interested in security assessment tools for hardware designs?
	<ul style="list-style-type: none"> <li>• Security assessment tools are interesting.</li> <li>• The market expects to identify counterfeit products everywhere in the supply chain.</li> </ul>
QC2	Does your company investigate the delivered products from the security viewpoint?
	<ul style="list-style-type: none"> <li>• We do not conduct any security-oriented assessment. Instead, we verify and test our products before shipment.</li> <li>• Specialized verification processes are conducted for security-related products.</li> </ul>
QC3	Who should operate the security assessment process?
	<ul style="list-style-type: none"> <li>• Third-party agencies should operate the security assessment process. It is difficult to maintain the reliability of the assessment in the case of in-house assessment.</li> </ul>
QC4	How do you consider the cost of the security assessment process?
	<ul style="list-style-type: none"> <li>• Business operators or industry organizations should cover the cost of the security assessment tools.</li> </ul>

Table 4: Resources for the QD4 question.

#	Item
QD4-a	Hardware designs written in HDL.
QD4-b	Feature values extracted from hardware designs. Specifically, there are three types of feature values: structural feature values (Oya et al., 2015; Dong et al., 2020), SCOAP feature values (Salmani, 2017; Tebyanian et al., 2021), and graph neural network-based embedding (Yu et al., 2021; Hasegawa et al., 2023).
QD4-c	Product information, such as the category of IC.
QD4-d	Application information, such as for communication devices or for industrial devices.
QD4-e	Bill of materials or the component list of the product.
QD4-f	Report of inspection.
QD4-g	Others (free comment).

features.

Table 5 shows the summary of the responses to the QD section. Although the repository scheme covers the design process, most companies expect that the repository scheme should cover all the processes, including the manufacturing process. Since skillful knowledge is required for the security assessment process, many companies hope that an impartial and professional organization should operate the repository scheme. Specifically, government or industry organizations would be appropriate candidates for the operator.

Since the hardware design information is confidential, providing designs, bills of materials, and inspection reports is extremely difficult. However, interestingly, the features extracted from hardware designs (QD4-b explained in Table 4) can be disclosed

for security assessment if necessary. In this case, the extraction process does not affect the existing production process and is sufficiently supported by an extraction tool vendor. Although the design process should be highly confidential, feature extraction is a possible way to adapt security assessment to semiconductor supply chains. Some companies commented that the scope of the disclosure must be restricted when the information is disclosed.

From the results, it can be seen that the demand for identifying counterfeit products is increased. To meet the demand, The repository operation scheme covering the whole supply chain is expected. In the repository operation scheme, the feature extraction process is interesting. Information regarding its cost and benchmarks is useful for considering the process.

In terms of legal regulations, most companies are concerned about geopolitical issues. These issues significantly affect business processes. Business operators in the automotive industry comply with international standards that are more rigorous compared to other industries.

#### 4.2.5 QE: Risk Measures in Supply Chains

In this section, we investigated the concerns and risk measures in semiconductor supply chains in terms of legal regulations.

Table 6 shows the summary of the responses to the QE section. For any company, the challenge lies in balancing compliance with local laws and regulations and maintaining stable production. Many companies consider decentralizing production bases and multi-sourcing of supply sources to address the risks in semiconductor supply chains.

In case vulnerability assessment in hardware devices is standardized, there is a concern about the burden on business operators in terms of the cost and measures they must take.

Table 5: Questions and responses to QD – effectiveness and feasibility.

QD1	What information is helpful when using the repository scheme?
	<ul style="list-style-type: none"> <li>• Tools or schemes to identify counterfeit products are interesting.</li> <li>• It is useful if the repository can cover the manufactured products to identify counterfeit products.</li> </ul>
QD2	Who should operate the repository scheme?
	<ul style="list-style-type: none"> <li>• Institutions considering introducing a repository operation scheme.</li> <li>• The government or industry organizations should design the system, and an impartial and professional organization should operate it.</li> </ul>
QD3	Is it acceptable if hardware designs are requested for the security assessment process?
	<ul style="list-style-type: none"> <li>• Generally, no companies provide circuit design information.</li> <li>• It is unavailable due to license issues with IP vendors.</li> </ul>
QD4	What level of design information can you provide for the security assessment process? (Possible resources are listed in Table 4)
	<ul style="list-style-type: none"> <li>• If the repository scheme is operational, we can provide the resources QD4-c and QD4-d.</li> <li>• QD4-b can be introduced, but it is necessary to examine issues such as the introduction burden of the feature extraction tool regarding QD4-b.</li> <li>• QD4-a and QD4-b are necessary for the repository operation scheme. However, QD4-a is not available. QD4-b needs to be considered. For others, we think that QD4-c or QD4-d can be provided.</li> </ul>
QD5	What kind of business operators would use the repository scheme?
	<ul style="list-style-type: none"> <li>• The communication infrastructure market is likely to have a high demand for security.</li> </ul>

Table 6: Questions and responses to QE – risk measures in supply chains.

QE1	What are the risks in semiconductor supply chains?
	<ul style="list-style-type: none"> <li>• Counterfeit products.</li> <li>• Geopolitical issues.</li> </ul>
QE2	What measures do you take to avoid supply chain risks?
	<ul style="list-style-type: none"> <li>• Purchasing semiconductor materials from multiple companies and decentralizing production bases.</li> <li>• We are responding to export control measures in each country.</li> <li>• Strengthening public relations, especially by enhancing the relationship with the government.</li> </ul>
QE3	What will affect your business if vulnerability assessment in hardware devices becomes mandatory or is standardized?
	<ul style="list-style-type: none"> <li>• The concern is the burden on semiconductor manufacturers, such as the cost and measures taken.</li> <li>• If the vulnerability assessment is standardized, we respond if it is necessary for our business.</li> </ul>

The major barriers to implementing a security assessment process in semiconductor supply chains are commercialization and showing the benefit of security assurance. Although most companies are concerned about security problems and interested in security assessment tools, they do not clearly find the benefit of security assessment. Considering the price competition of semiconductor products, the cost of security is unacceptable. It would be difficult to change this mindset in the semiconductor market. Therefore, if security assessment is necessary, legal regulation is a solution to solve the problem.

### 4.3 Discussion

To secure hardware supply chains, a method using a blockchain or smart contract platform has been pro-

posed (Chang and Chen, 2020). In supply chain management, traceability, transparency, and stakeholder involvement are major concerns. A platform using blockchain or smart contracts is expected to address the concerns. The major feature of the blockchain technology is decentralization. This technology allows peer-to-peer exchange or transactions, such as digital currency, without trusted authorities. This mechanism also applies to a supply chain context. However, implementing a blockchain-based mechanism faces several issues from the perspective of reliability, throughput, and computational cost.

A supply chain management method using a knowledge graph has been proposed (Zhang et al., 2019). In this method, a knowledge graph is constructed to analyze the risks of a supply chain. Based on the constructed knowledge graph, the connection

between business operators and the bottleneck in the supply chain can be visualized. However, collecting standardized and reliable information from multiple business operators is difficult in the real world.

## 5 CONCLUSION

In this paper, we focus on the demand and awareness of security assessment for hardware designs in industries. First, we propose a repository operation scheme to share security assessment results with inter-companies. Next, we design questionnaires to confirm the needs, effectiveness, and concerns based on the repository operation scheme and summarize the results of the questionnaires.

From the survey, we found that HT detection methods are attractive for protecting semiconductor supply chains. However, the barriers to implementing HT detection in industries lie in commercialization and in cultivating awareness of security in the industry. Specifically, identifying counterfeit products and covering the whole supply chain are expected. For expectations, future work should cover the whole supply chain and clarify the benefits of the scheme in industries.

## ACKNOWLEDGMENTS

The questionnaire survey was conducted by Omdia, a part of Informa Tech as a consulting project for KDDI Research, Inc. in 2022. The copyright of the original questionnaire survey belongs to Omdia. The results reported in this paper were obtained from “The Contract of Research for Detection Techniques of Hardware Vulnerabilities” (Ministry of Internal Affairs and Communication, Japan in FY2022).

## REFERENCES

- Almeida, F., Imran, M., Raik, J., and Pagliarini, S. (2022). Ransomware attack as hardware trojan: A feasibility and demonstration study. *IEEE Access*, 10:44827–44839.
- Chang, S. E. and Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access*, 8:62478–62494.
- Dong, C., Liu, Y., Chen, J., Liu, X., Guo, W., and Chen, Y. (2020). An unsupervised detection approach for hardware trojans. *IEEE Access*, 8:158169–158183.
- Franco, J. and Frick, F. (2015). Introduction to hardware trojan detection methods. In *2015 Design, Automation & Test in Europe Conference Exhibition (DATE)*, pages 770–775.
- Hasegawa, K., Yamashita, K., Hidano, S., Fukushima, K., Hashimoto, K., and Togawa, N. (2023). Node-wise hardware trojan detection based on graph learning. *IEEE Transactions on Computers*, pages 1–13.
- Hasegawa, K., Yanagisawa, M., and Togawa, N. (2017a). Hardware trojans classification for gate-level netlists using multi-layer neural networks. In *Proc. IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 227–232.
- Hasegawa, K., Yanagisawa, M., and Togawa, N. (2017b). Trojan-feature extraction at gate-level netlists and its application to hardware-trojan detection using random forest classifier. In *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–4.
- Huang, Z., Wang, Q., Chen, Y., and Jiang, X. (2020). A survey on machine learning against hardware trojan attacks: Recent advances and challenges. *IEEE Access*, 8:10796–10826.
- Li, S., Zhang, Y., Chen, X., Ge, M., Mao, Z., and Yao, J. (2020). A xgboost based hybrid detection scheme for gate-level hardware trojan. In *Proc. IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, volume 9, pages 41–47.
- Oya, M., Shi, Y., Yanagisawa, M., and Togawa, N. (2015). A score-based classification method for identifying hardware-trojans at gate-level netlists. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 465–470.
- Salmani, H. (2017). Cotd: Reference-free hardware trojan detection and recovery based on controllability and observability in gate-level netlist. *IEEE Transactions on Information Forensics and Security*, 12:338–350.
- Tebyanian, M., Mokhtarpour, A., and Shafieinejad, A. (2021). Sc-cotd: hardware trojan detection based on sequential/combinational testability features using ensemble classifier. *J. Electron. Test.*, 37(4):473–487.
- Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., and Tehranipoor, M. (2016). Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems*, 22.
- Yang, Y., Ye, J., Cao, Y., Zhang, J., Li, X., Li, H., and Hu, Y. (2020). Survey: Hardware trojan detection for netlist. In *2020 IEEE 29th Asian Test Symposium (ATS)*, pages 1–6.
- Yu, S.-Y., Yasaei, R., Zhou, Q., Nguyen, T., and Faruque, M. A. A. (2021). Hw2vec: a graph learning tool for automating hardware security. In *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE.
- Zhang, W., Liu, Y., Jiang, L., Shah, N., Fei, X., and Cai, H. (2019). The construction of a domain knowledge graph and its application in supply chain risk analysis. In *IEEE International Conference on E-Business Engineering*, pages 464–478.