Optimization of Survivability of a Mission Critical System in the Presence of Hardware Trojans

Mohammad Rahman
Department of Computer Science
Tuskegee University
Tuskegee, AL
Email: mrahman@tuskegee.edu

Laurent Njilla
Cyber Assurance Branch
Air Force Research Laboratory
Rome, NY
Email: laurent.njilla@us.af.mil

Swastik Brahma
Department of Computer Science
Tennessee State University
Nashville, TN
Email: sbrahma@tnstate.edu

2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) | 978-1-6654-8303-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CCWC54503.2022.9720756

***Abstract*—The paper presents a novel redundancy-based technique to optimize the survivability of a mission-critical system when its operational components can have hardware Trojans which are activated at run-time. A computationally efficient technique is presented to find the optimal set of redundant components under a given cost budget of the system designer. Numerous numerical results are presented which provide important insights and show the performance advantages of our proposed technique.**

***Keywords*—Mission-Critical Systems, Security, Hardware Trojan, Redundancy, Optimization.**

I. Introduction

A hardware Trojan is a malicious modification of the circuitry of an Integrated Circuit (IC) [1], [2], [8]. The presence of Trojans in ICs can lead to derangement of system operation and even complete system failure. Such attacks pose a serious threat to the semiconductor industry and to modern cyber systems. An approach that has been explored by past work to mitigate Trojan threats is the development of IC design strategies that make it harder for malicious manufacturers to insert Trojans [6], [7]. Since such design strategies, however, can potentially be defeated by a malicious manufacturer, past work has also explored the development of testing strategies that can be used to check for the presence of Trojans in acquired ICs [4], [5], [14]–[16]. For example, in [16], the authors propose a technique, referred to as MERO (Multiple Excitation of Rare Occurence), that maximizes the probability of detecting an inserted Trojan using statistical methods. Since exhaustive testing of all possible Trojan types can be prohibitive, the works in [9]–[11], [17], [18] develop game theoretic [13] testing strategies that can intelligently determine which Trojan types to test against a strategic manufacturer.

It should be noted that past approaches for defending against Trojan threats are fallible and there is always a possibility that installed ICs, even ones in which conducted tests have not found Trojans, have Trojans in them which are activated while operating. *How do we optimize performance of a system when its constituent operational components can have hardware Trojans which are activated at run-time?* Addressing this problem requires exploring techniques that go beyond the mitigation strategies explored by past work and is the topic of interest in this paper.

Specifically, in this paper, we consider a mission-critical system which is meant to serve a certain mission for a defined time duration. Such systems have important applications in various sectors including the military, healthcare, and in automotive industries [12]. In such systems, it is of utmost importance to have the system survive until the desired mission time given that the system components[1] can have hardware Trojans which are activated while operating impeding mission success. To enhance survivability in such a context, in this paper, we

- propose the novel concept of installing *redundant* component ICs in the system that can be kept on standby and used if Trojans are detected in operational components at run-time,
- characterize the optimal set of redundant components to be installed under consideration of the *costs* involved in the redundant acquisition of ICs,
- provide a *computationally efficient* technique to find the optimal set of redundant components, and
- provide numerous *numerical results* to gain important insights.

The rest of the paper is organized as follows. Section II presents our model for the proposed redundancy-based methodology for optimizing survivability of a mission-critical system in the presence of hardware Trojan threats. Section III presents a computationally efficient technique for finding the optimal set of redundant components. Section IV presents numerical results to provide important insights. Finally, Section V concludes the paper.

II. Redundancy-based Survivability Optimization

Consider a mission-critical system consisting of V subsystems, numbered 1 to V. For every subsystem i, suppose that l_i is the number of *operational* components required, m_i^{max} is the *maximum* number of components that can be installed,

This work was supported by the NSF under Award Number HRD 1912414.
Approved for Public Release; Distribution Unlimited. Case Number AFRL -2021-3034. Dated 08 Sep 2021.

[1]We use the terms "IC" and "component" interchangeably.

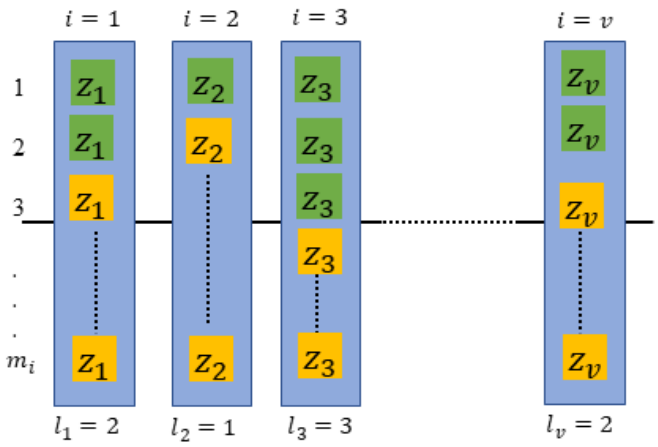

Fig. 1. System with V subsystems.

and that there is a set $\{1, \cdots, n_i\}$ of manufacturers who can supply components (ICs) for the subsystem. Suppose also that for manufacturer $z_i \in \{1, \cdots, n_i\}$ for subsystem i:

- $\alpha_i^{z_i}$ is the probability that z_i is malicious in nature,
- $\rho_i^{z_i}$ is the probability with which a malicious manufacturer z_i inserts a Trojan in a sold component,
- $\lambda_i^{z_i}$ is the activation rate of the Trojan inserted by z_i, and
- $c_i^{z_i}$ is the cost of acquiring a component from z_i.

The system model is shown in Fig. 1, where, in every subsystem, the *green* components depict *operational* ones and the *yellow* components depict *standby* ones which can be used if Trojans are detected in the operational ones. The notations used are summarized in Table I.

In such a scenario, *for every subsystem i, we seek to choose $z_i \in \{1, ..., n_i\}$ (i.e., the manufacturer) and the number of components m_i ($l_i \leq m_i \leq m_i^{max}$) to acquire from the chosen manufacturer such that the system survival probability until a given mission time t is maximized under a cost budget C.*

Next, we formulate the problem of optimally configuring a mission-critical system with redundant components as an optimization problem.

A. Problem Formulation

The survival probability ($S(t)$) of a system having V subsystems, until a given time t, with subsystem i configured with m_i components from manufacturer z_i, and with activations of Trojans in system components modeled as a Poisson process, is

$$S(t) = \prod_{i=1}^{V} \left(1 - \alpha_i^{z_i}\rho_i^{z_i} + \alpha_i^{z_i}\rho_i^{z_i} \sum_{k=0}^{m_i - l_i} \frac{(\lambda_i^{z_i} l_i t)^k}{k!} e^{-\lambda_i^{z_i} l_i t}\right) \tag{1}$$

In such a scenario, our objective is to choose $\mathbf{z} = [z_1, \cdots, z_V]$ (i.e., the manufacturer for each subsystem) and $\mathbf{m} = [m_1, \cdots, m_V]$ (i.e., number of components to acquire from the chosen manufacturers for installation) such that (1) is maximized under a cost budget C. The optimization problem is formulated below:

$$\begin{aligned} \underset{\mathbf{z},\mathbf{m}}{\text{Maximize}} \quad & S(t) \\ \text{subject to} \quad & \sum_{i=1}^{V} m_i c_i^{z_i} \leq C \\ & l_i \leq m_i \leq m_i^{max}, \quad \forall i \in \{1, \cdots, V\} \\ & z_i \in \{1, ..., n_i\}, \quad \forall i \in \{1, \cdots, V\} \end{aligned} \tag{P1}$$

B. Survivability Optimization with $V = 1$

Here, we analyze the case where $V = 1$ to gain some important insights and study the solution for this scenario. For analyzing the problem in this case, in the notations defined earlier, we drop the subscript denoting the subsystem number for simplicity. In such a scenario, (1) becomes

$$S(t, m) = 1 - \alpha^z \rho^z + \alpha^z \rho^z \sum_{k=0}^{m-l} \frac{(\lambda^z l t)^k}{k!} e^{-\lambda^z l t} \tag{2}$$

Clearly, the solution for this case corresponds to choosing manufacturer $z^* = \arg\max_{z \in \{1, \cdots, n\}} S(t, m = \min(\lfloor \frac{C}{c^z} \rfloor, m^{max}))$ and acquiring $\min(\lfloor \frac{C}{c^{z^*}} \rfloor, m^{max})$ components from z^*.

Next, we provide an example to illustrate our solution for the $V = 1$ case. Consider the availability of three manufacturers, viz. $\{1, 2, 3\}$, for designing a system with a mission time of $t = 5$ hours under a cost budget of $C = 25$ and with $l = 1$. The various parameters of the three manufacturers, as well as the survival probability obtained corresponding to the acquisition of the maximum possible number of components from each manufacturer (without exceeding the cost budget), are shown in Table II. As can be seen from the table, the survival probability of the system is maximized if manufacturer 3 is chosen and 4 components are acquired from the manufacturer, which yields a survival probability of 0.948.

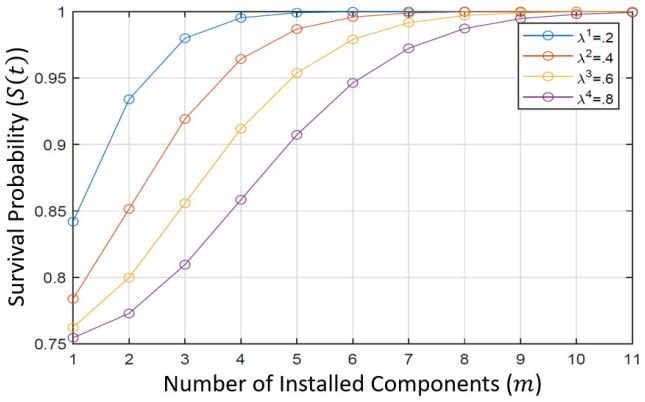

Fig. 2. Survival prob. ($S(t)$) vs. no. of installed components for different Trojan activation rates.

Next, in Fig. 2, we provide numerical results for the $V = 1$ case considering the number of operational components required (l) to be 1, the mission time to be $t = 5$

TABLE I
NOTATIONS USED

Notation	Description
V	Number of subsystems.
z_i	Selected manufacturer for subsystem i from the set $\{1, \cdots, n_i\}$.
m_i	Number of components installed for subsystem i.
l_i	Number of operational components required for subsystem i.
m_i^{max}	Maximum number of components that can be installed for subsystem i.
$\alpha_i^{z_i}$	Probability of manufacturer $z_i \in \{1, \cdots, n_i\}$ being malicious.
$\rho_i^{z_i}$	Probability of malicious manufacturer z_i inserting a Trojan in a sold component.
$\lambda_i^{z_i}$	Activation rate of the Trojan inserted by malicious manufacturer z_i.
$c_i^{z_i}$	Cost of acquiring a component from manufacturer z_i.
C	Cost budget for system design.

TABLE II
AN EXAMPLE

Manufacturer	α	ρ	λ	c	m	$S(t)$
1	0.4	0.5	0.8	7.5	3	0.847
2	0.5	0.7	0.3	7	3	0.933
3	0.6	0.6	0.4	6	4	0.948

hours, the presence of four manufacturers, viz. $\{1, 2, 3, 4\}$, $\alpha^z = \rho^z = 0.5, \forall z \in \{1, 2, 3, 4\}$, and activation rates of the Trojans inserted by the manufacturers to be $\{\lambda^1, \lambda^2, \lambda^3, \lambda^4\} = \{.2, .4, .6, .8\}$. As can be seen from the figure, for every manufacturer, the survival probability of the system (2) increases with the number of components acquired and installed from the manufacturer (i.e, survival probability increases with redundancy). This shows the *advantage of our proposed redundancy-based scheme* and corroborates our solution approach for the $V = 1$ case described earlier.

III. SURVIVABILITY OPTIMIZATION WITH V SUBSYSTEMS

In this section, we provide a computationally efficient technique to solve Problem P1 for finding the optimal set of redundant components for the general case with V subsystems. Our technique is described below:

1) Define Boolean decision variable x_{ijr}, where

$$x_{ijr} = \begin{cases} 1 & \text{if } r \text{ components are acquired from} \\ & \text{manufacturer } j \text{ for subsystem } i \\ 0 & \text{otherwise} \end{cases}$$

2) Calculate the associated cost (β_{ijr}) for acquiring r components from manufacturer j for subsystem i:

$$\beta_{ijr} = c_i^j r$$

3) Take the logarithm of the survival probability of subsystem i corresponding to configuring it with r components acquired from manufacturer j:

$$\gamma_{ijr} = \log\left[1 - \alpha_i^j \rho_i^j + \alpha_i^j \rho_i^j \sum_{k=0}^{r-l_i} \frac{(\lambda_i^j l_i t)^k}{k!} e^{-\lambda_i^j l_i t}\right]$$

4) Based on the above, reformulate Problem P1 as follows:

$$\begin{aligned} \underset{\mathbf{z},\mathbf{m}}{\text{Maximize}} \quad & \sum_{i=1}^{V} \sum_{j=1}^{n_i} \sum_{r=l_i}^{m_i^{max}} \gamma_{ijr} x_{ijr} \\ \text{subject to:} \quad & \sum_{i=1}^{V} \sum_{j=1}^{n_i} \sum_{r=l_i}^{m_i^{max}} \beta_{ijr} x_{ijr} \leq C \\ & \sum_{j=1}^{n_i} \sum_{r=l_i}^{m_i^{max}} x_{ijr} = 1, \ \forall i \in \{1, \cdots, V\} \end{aligned} \tag{P2}$$

5) Solve Problem P2, which is a 0-1 multiple choice knapsack problem (MCKP), using dynamic programming [3], and extract optimal values of z_i and m_i for each subsystem i by inspecting x_{ijr}, $\forall i \in [1, V]$, $\forall j \in [1, n_i]$, $\forall r \in [l_i, m_i^{max}]$.

Next, we provide an example to illustrate our solution. Consider a system with $V = 4$ (i.e., with four subsystems). For the four subsystems, consider $\{l_1, l_2, l_3, l_4\} = \{2, 1, 3, 1\}$ and $\{m_1^{max}, m_2^{max}, m_3^{max}, m_4^{max}\} = \{5, 4, 6, 3\}$. Consider that there are three different manufacturers for each subsystem. The parameters of the available manufacturers are shown in Table III. The mission time is considered to be $t = 10$ units and the cost budget is considered to be $C = 200$. Table IV shows the optimal solution obtained based on our technique outlined above, which shows that the optimal solution under the aforementioned parameters corresponds to selecting $\{z_1, z_2, z_3, z_4\} = \{3, 2, 3, 1\}$ and $\{m_1, m_2, m_3, m_4\} = \{5, 4, 3, 3\}$ yielding a survival probability of 0.8496.

TABLE III
PARAMETERS OF AVAILABLE MANUFACTURERS

	Manufacturer	α	ρ	λ	c
Subsystem 1	1	0.4	0.3	0.5	8
	2	0.4	0.6	0.8	9
	3	0.3	0.3	0.4	11
Subsystem 2	1	0.1	0.2	0.2	4
	2	0.1	0.3	0.15	3
	3	0.15	0.25	0.1	6
Subsystem 3	1	0.3	0.25	0.22	15
	2	0.35	0.22	0.2	17
	3	0.32	0.2	0.21	18
Subsystem 4	1	0.2	0.20	0.12	23
	2	0.25	0.21	0.18	27
	3	0.22	0.26	0.15	28

TABLE IV
OPTIMAL SYSTEM CONFIGURATION

	z	**m**	$S(t)$
Subsystem 1	3	5	0.8496
Subsystem 2	2	4	
Subsystem 3	3	3	
Subsystem 4	1	3	

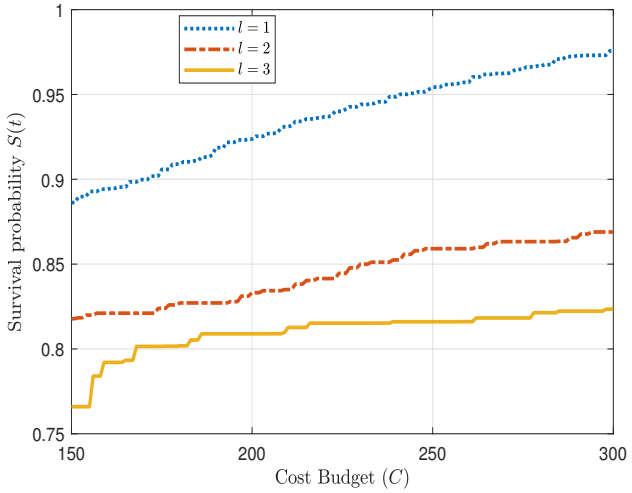

Fig. 3. Impact of cost budget (C) on survival probability ($S(t)$) with 4 subsystems.

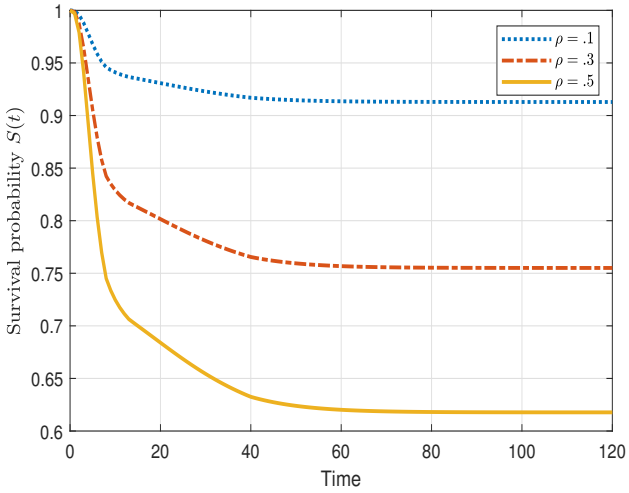

Fig. 4. Impact of mission time (t) on survival probability ($S(t)$) with 4 subsystems.

IV. NUMERICAL RESULTS

In this section, we provide numerical results to gain insights and show the performance advantages of our proposed technique. For obtaining the numerical results, the optimal set of redundant components were obtained by solving Problem P2 under different scenarios. In Fig. 3, we study how the cost budget (C) impacts the optimal survival probability of a mission-critical system. For the figure, we consider $V = 4$ (i.e., a system with four subsystems), with $m_1^{max} = m_2^{max} = m_3^{max} = m_4^{max} = 10$, and a mission time of $t = 15$ units. Three different manufacturers are considered to be available for each subsystem (Table III shows the parameters of the available manufacturers). The number of operational components required for the subsystems is considered to be $l_1 = l_2 = l_3 = l_4 = l$. As can be seen from the figure, for a given number of operational components (l) for the subsystems, the optimal survival probability of the system shows a non-decreasing trend with cost budget. This is because, increase of the cost budget enables the acquisition of components from manufacturers who are less likely to insert Trojans as well as in the acquisition of components having lower Trojan activation rates, even if the cost of acquiring such components is higher, while enabling the sustenance of a higher degree of redundancy.

Further, as can also be seen from Fig. 3, for a given cost budget (C), the optimal survival probability of the system

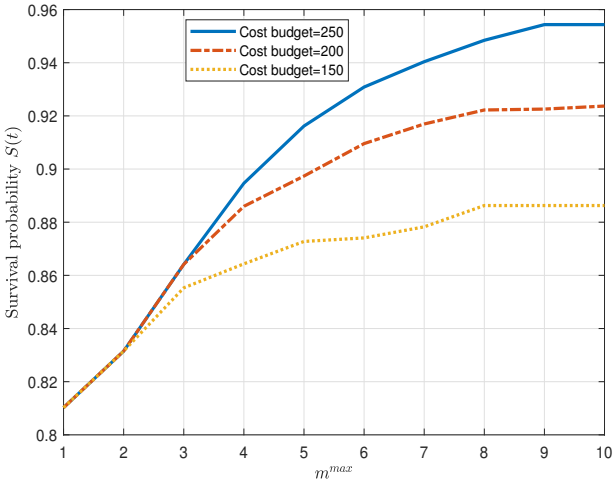

Fig. 5. Impact of the maximum number of components that can be installed per subsystem (m^{max}) on survival probability ($S(t)$) with 4 subsystems.

increases as the number of operational components required for the subsystems decreases. This is because, under a given cost budget (and a given maximum number of components that can be installed in the subsystems), decrease in the number of operational components needed for the subsystems enables the sustenance of a higher degree of component redundancy for the subsystems.

In Fig. 4, we study how the mission time (t) impacts the optimal survival probability of a mission-critical system. For the figure, we again consider $V = 4$ (i.e., a system with four subsystems), with $m_1^{max} = m_2^{max} = m_3^{max} = m_4^{max} = 10$, and a mission time of $t = 15$ units. Three different manufacturers are considered to be available for each subsystem, with every malicious manufacturer considered to insert a Trojan in its sold component with a probability ρ (whose values are shown in the figure). Aside from ρ, the other parameters of the manufacturers follow Table III. As can be seen from the figure, and as is intuitive, survival probability shows a non-increasing trend with the length of the mission time. Further, the figure also shows that, as expected, a higher ρ yields a lower survival probability.

In Fig. 5, we analyze how the maximum number of components that can be installed in each subsystem, m^{max}, impacts the optimal survival probability of a mission-critical system. For the figure, we again consider $V = 4$ (i.e., a system with four subsystems), with $m_1^{max} = m_2^{max} = m_3^{max} = m_4^{max} = m^{max}$ (which is varied on the X-axis), and a mission time of $t = 15$ units. Three different manufacturers are considered to be available for each subsystem, with the parameters of the available manufacturers following Table III. As can be seen from the figure, system survival probability shows a non-decreasing trend with m^{max} as increase of m^{max} enables the sustenance of a higher degree of redundancy. Also, as can be seen from the figure, for a given m^{max}, as expected, system survival probability shows a non-decreasing trend with the available cost budget.

V. Conclusion

The paper presented a novel redundancy-based technique to optimize the survivability of a mission-critical system whose operational components can have hardware Trojans which are activated at run-time. A computationally efficient technique was presented to find the optimal set of redundant components under a cost budget of the system designer. Numerous numerical results were presented which provided important insights and showed the performance advantages of our proposed technique.

References

[1] S. Bhunia, M. S. Hsiao, M. Banga and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," in Proceedings of the IEEE, 2014, vol. 102, no. 8, pp. 1229-1247.

[2] R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," IEEE International High Level Design Validation and Test Workshop, San Francisco, CA, 2009, pp. 166-171.

[3] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, "Introduction to Algorithms", 3rd Edition. MIT Press 2009.

[4] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, 2008, pp. 40-47.

[5] H. Salmani, M. Tehranipoor and J. Plusquellic, "New design strategy for improving hardware Trojan detection and reducing Trojan activation time," IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, 2009, pp. 66-73.

[6] T. Linscott, P. Ehrett, V. Bertacco and T. Austin, "SWAN: Mitigating Hardware Trojans with Design Ambiguity," IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2018, pp. 1-7.

[7] T. Trippel, K. Shin, K. Bush, M. Hicks, "T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing," CoRR, abs/1906.08842, 2019.

[8] J. Rajendran, E. Gavas, J. Jimenez, V. Padman and R. Karri, "Towards a comprehensive and systematic classification of hardware Trojans," IEEE International Symposium on Circuits and Systems, Paris, 2010, pp. 1871-1874.

[9] C. A. Kamhoua, H. Zhao, M. Rodriguez and K. A. Kwiat, "A Game-Theoretic Approach for Testing for Hardware Trojans," in IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 3, pp. 199-210, 2016.

[10] J. Graf, W. Batchelor, S.Harper, R. Marlow, E. Carlisle IV and P. Athanas, "A practical application of game theory to optimize selection of hardware Trojan detection strategies," in J Hardw Syst Secur vol. 4, 2020.

[11] J. Graf, "Trust games: How game theory can guide the development of hardware Trojan detection methods," 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 91-96, 2016.

[12] M. Hinchey and L. Coyle, "Evolving Critical Systems: a Research Agenda for Computer-Based Systems," 17th IEEE International Conference and Workshops on Engineering of Computer-Based Systems, pp. 430-435, 2010.

[13] D. Fudenberg and J. Tirole, "Game Theory", MIT press, Cambridge, MA, 1991.

[14] S. Bhasin and F. Regazzoni, "A survey on hardware trojan detection techniques," 2015 IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, 2015, pp. 2021-2024.

[15] D. Agarwal, S. Baktir, D. Karakoy, P. Rohatgi and B. Sunar, "Trojan Detection using IC Fingerprinting," IBM Research Report, 2006.

[16] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou and S. Bhunia, "MERO: A statistical approach for hardware Trojan detection," in Proc. Workshop Cryptograph. Hardware Embedded Syst., 2009, pp. 396-410.

[17] S. Brahma, S. Nan and L. Njilla, "Strategic Hardware Trojan Testing with Hierarchical Trojan Types," 2021 55th Annual Conference on Information Sciences and Systems (CISS), 2021, pp. 1-6.

[18] S. Brahma, L. Njilla, and S. Nan, "Game theoretic hardware trojan testing under cost considerations," International Conference on Decision and Game Theory for Security, Springer, 2021, pp. 251–270.