Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.12, No.2, 2021
www.iiste.org

A Survey on Integrated Circuit Trojans

Halit Türksönmez* Mehmet Hilal Özcanhan
Department of Computer Engineering, Dokuz Eylül University, PO box 35390, İzmir, Turkey

Abstract
Traditionally, computer security has been associated with the software security, or the information-data security. Surprisingly, the hardware on which the software executes or the information stored-processed-transmitted has been assumed to be a trusted base of security. The main building blocks of any electronic device are Integrated circuits (ICs) which form the fabric of a computer system. Lately, the use of ICs has expanded from handheld calculators and personal computers (PCs) to smartphones, servers, and Internet-of-Things (IoT) devices. However, this significant growth in the IC market created intense competition among IC vendors, leading to new trends in IC manufacturing. System-on-chip (SoC) design based on intellectual property (IP), a globally spread supply chain of production and distribution of ICs are the foremost of these trends. The emerging trends have resulted in many security and trust weaknesses and vulnerabilities, in computer systems. This includes Hardware Trojans attacks, side-channel attacks, Reverse-engineering, IP piracy, IC counterfeiting, micro probing, physical tampering, and acquisition of private or valuable assets by debugging and testing. IC security and trust vulnerabilities may cause loss of private information, modified/altered functions, which may cause a great economical hazard and big damage to society. Thus, it is crucial to examine the security and trust threats existing in the IC lifecycle and build defense mechanisms against IC Trojan threats. In this article, we examine the IC supply chain and define the possible IC Trojan threats for the parties involved. Then we survey the latest progress of research in the area of countermeasures against the IC Trojan attacks and discuss the challenges and expectations in this area.
Keywords: IC supply chain, IC security, IP privacy, hardware trojans, IC trojans
DOI: 10.7176/CEIS/12-2-01
Publication date: April 30th 2021

1. Introduction

For a long time, hardware has been assumed as root-of-trust for the entire computer system and used as a virtual layer that runs the code sent from the software layer. Meanwhile, computer system security has been associated with software security or information security. Consequently, the studies on hardware security are mostly associated with the performance improvement of crypto-related algorithms embedded in hardware, such as crypto ICs (Preneel & Takagi 2011; Jin 2015). Hardware copyright protection is also considered in the hardware security domain (Rad *et al.* 2008). For many years, computer systems security researchers assumed that adversaries could not compromise ICs easily, or profit by compromising the ICs. The assumption was so extensive that the security of the IC supply chain was not even considered. The alarm was raised when illegal IC duplicates started to appear in the market.

ICs are the main building blocks of any electronic device that forms the fabric of a computer system. Their usage has been increased over the years, from handheld calculators and desktop computers to servers, smartphones, and Internet-of-Things (IoT) devices. In Figure 1, the income from the global semiconductor market for ICs between 2009 and 2021. In 2021, the income from IC sales is predicted to reach US $383.84 billion by Statista (Alsop 2020).

However, this significant growth in the semiconductor market created intense competition among IC vendors such as Intel, Samsung, Broadcom, and Qualcomm, leading to new trends in IC manufacturing (Salmani 2018). SoC design based on IP, and a globally spread supply chain for production and delivery of ICs are the foremost of these trends.

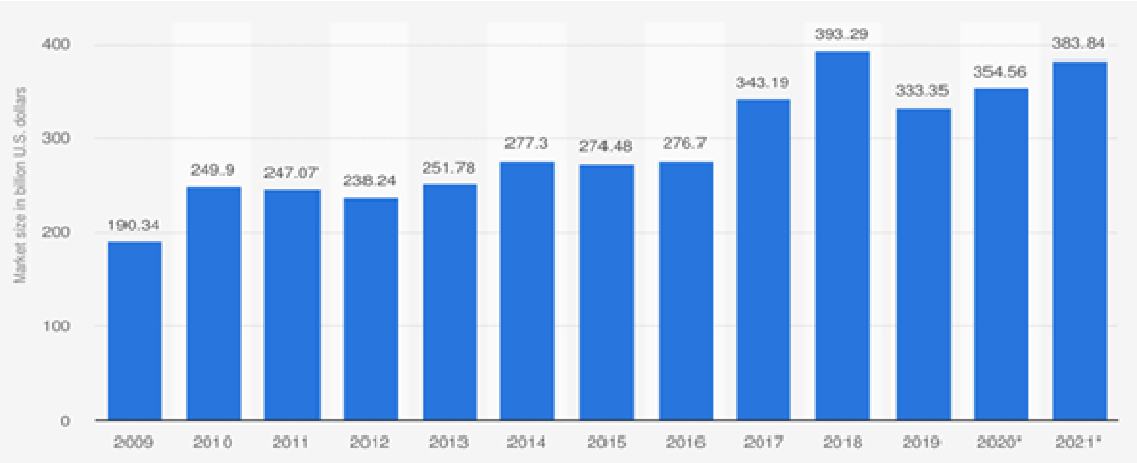

Figure 1. The global income from ICs between 2009 and 2021 (Alsop 2020)

A typical example of globally spread IC production process, spanning multiple countries, is shown in Figure 2 (SIA 2016). These emerging trends are followed by the reduction of IC manufacturers' control over the design and production stages. Consequently, many security and trust weaknesses and vulnerabilities arise (such as IC Trojans attacks, IP piracy and reverse-engineering, IC counterfeiting, etc.) (Salmani 2018; Bhunia & Tehranipoor 2018; Bhunia & Tehranipoor 2019; Farahmandi *et al.* 2020; Behnam 2018; Rostami *et al.* 2013; Rostami *et al.* 2014; Bhunia *et al.* 2014; Belous & Saladukha 2020; Qu & Yuan 2014; Li *et al.* 2016; Karri *et al.* 2010; Özcanhan & Türksönmez 2020).

Figure 2. A typical IC production process example spans multiple countries (SIA 2016)

In the rest of this article, we examine the IC supply chain and describe the potential IC Trojan threats faced by the parties included. Then we explain and compare IC security and IC trust. Finally, we survey the advances in recent studies about the countermeasures against the Trojan attacks and discuss the challenges and expectations in this area.

2. Differences between IC Security and IC Trust

IC security problems emerge from its built-in vulnerability to attacks, such as scan-based attacks, side-channel attacks, and probing attacks. However, IC trust problems emerge from the participation of untrusted parties in the lifecycle of an IC, such as:

- untrusted intellectual property (IP) or electronic design automation (EDA) / computer-aided design (CAD) tool vendors,
- untrusted design,
- untrusted fabrication,
- weak testing,
- insecure distribution facilities.

The parties included in the above IC production activities are liable to violate the trustworthiness of consumers towards an IC. Potentially, they may cause deflections from expected trustworthiness, functionality, reliability, or performance. Trust problems usually escalate to security problems. For instance, an untrusted IP vendor could insert malware entities in a design, which may cause information theft, or denial-of-service (DoS) when the IC goes on to the field. Moreover, trust issues may also cause other problems, such as low energy-

efficiency or performance, or reduced safety, or reliability problems. The horizontal structure of the semiconductor trade model and the growing nature of the globally spread IC supply chain are causing the IC trust problems even more important. Thus, it drives novel research and development studies on IC design for trust assurance and trust verification (Bhunia & Tehranipoor 2019; Farahmandi *et al.* 2020; Behnam 2018).

3. Vulnerable IC Supply Chain

Figure 2 shows a typical IC production process spanning over multiple countries, while Figure 3 shows detailed IC supply chain phases. IC supply chain shown in Figure 3 spreads globally, which causes new IC security and trust issues to emerge from the global trends in IC design, fabrication, and distribution. IC design flow simply shows the stages and assets relevant to this article. System design framed with the dotted lines represents how the forged and poor-quality parts are inserted into the supply chain. Designing an IC covers supplying IP from third-party design houses, joining together IP and in-house designed components, and composing the IC layout. Afterward, the overall design is dispatched to the foundry that produces a mask and fabricates the ICs. Then, the ICs are tested at the fabrication site and test plants. Finally, flawless ICs are packaged up and sent to market. As it can be suspected, there are lots of stages in the IC supply chain, where malicious activities can happen. For instance, a malicious employee, who can reach the design at an untrusted foundry, could insert IC Trojans into any of the photomasks.

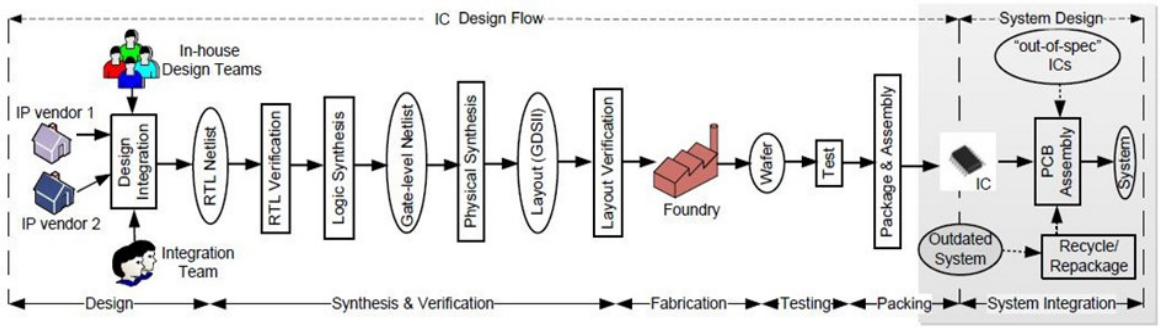

Figure 3. IC supply chain (Rostami *et al.* 2013; Rostami *et al.* 2014)

4. Known IC Attack Vectors

Table 1 shows the known security problems arising out of untrusted design, fabrication, and test stages of an IC. Attack vectors are instruments or ways for adversaries to reach ICs for malicious intension. One example is to exploit the IC to get the valuable/confidential data stored. Some attack vectors provide the ability for exploiting implementation problems, by physical tampering and side-channel attacks. Trojan attacks use the lack of control at IC fabrication stage, as an advantage. The Trojan attack vector is shown in yellow in Table 1. Attack surface can be defined as the total exposures of all possible security risks. It can also be described as the total of all known, unknown, and possible vulnerabilities. An adversary can utilize one or more vulnerabilities and start an attack, ending with obtaining confidential data from the system the IC is a part of. The smallest possible attack surface is considered as a primary target for countermeasure developers.

At first glance, IC Trojan attacks may be considered as part of IC trust problems. But the consequences of a Trojan attack on an IC may result in the leakage of secret data in that IC. Therefore, the impact factor of IC Trojan Attacks may be considered greater compared to the other IC attacks. This is the reason why we focused on IC Trojans, in this article.

Table 1. Attack vectors for the stages in an IC's lifespan. (ICS: IC security related attack, ICT: IC trust related attack)

IC Life Cycle / Attack Vectors	CAD/EDA Tool/IP Vendor	IC Design House	Foundry	Test Facility	IC End User /Deployment	Recycling/ Repacking Facility
IC Trojan Attacks (ICT)	✓	✓	✓			
IP Privacy & Overproduction (ICT)		✓	✓			
Reverse Engineering (ICT)		✓	✓	✓	✓	✓
Side-channel Attacks (ICS)					✓	
IC Counterfeiting (ICT)		✓	✓	✓		✓
Scan-based Attacks (ICS)			✓	✓	✓	
Probing Attack (ICS)			✓	✓	✓	
Invasive Fault Injection Attack (ICT)			✓	✓	✓	

5. IC Trojan Attacks

IC Trojans are hostile alterations in the functional behaviors of an IC (Rostami *et al.* 2013; Rostami *et al.* 2014; Bhunia 2018). These alterations are foreign, unknown, and unplanned by the IC designer, which could have harmful impacts on the IC. IC Trojans have three basic features: adversarial purpose, avoidance of detection, and sparseness of activation (Bhunia *et al.* 2014; Belous & Saladukha 2020). An IC Trojan always has the same purpose: application of an unintentional activity to compromise the confidentiality, integrity, or authentication of the underlying IC. Confidentiality, integrity, authentication triplet is referred to as CIA-Triad in the literature (Parker 2010).

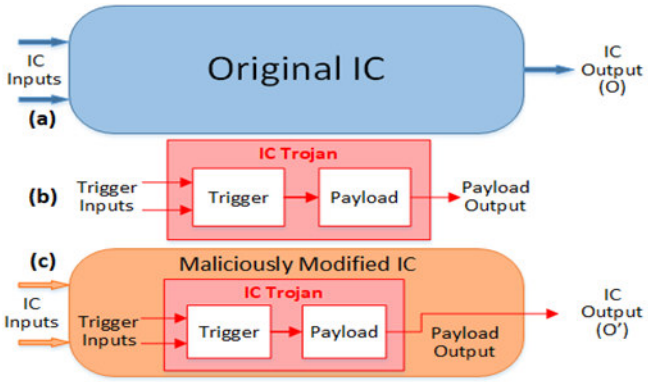

Figure 4. (a) Original IC, (b) IC Trojan, and (c) Trojan implanted IC (Bhunia & Tehranipoor 2018)

In Figure 4(a), an unaltered IC having two inputs and one output is symbolized. In Figure 4(b), an IC Trojan that has a trigger and a payload is symbolized. In Figure 4(c), the Trojan implanted into an IC is shown. In such a scenario, whenever the Trojan becomes active, its payload inverts the output of the IC, such as from O to O'. The size of IC Trojans may be tiny or big relative to the remaining original circuitry, changing from a few transistors to millions of transistors (Bhunia *et al.* 2014). Trojans may be in various shapes. They are mostly activated by a sequential, combinational, or hybrid digital circuit. But, they can also be activated by an analog signal. The Trojan payload can be analog or digital, but each is specially designed to produce malicious results when triggered.

6. IC Trojan Threat Patterns

Generally, the design and production procedure of an IC can be separated into three phases: Development of IP core, development of IC, and fabrication of IC. Thus, three types of companies (IP vendors, IC developers, and foundries) have a chance to inject IC Trojans. Trojans can be inserted at any stage of the three phases, by adversaries. The stage of insertion results in various adversarial patterns. Table 2 shows seven potential IC attack patterns for the IC Trojan attacks (Xiao *et al.* 2016).

Table 2. IC Trojan attack patterns (Rostami *et al.* 2013; Rostami *et al.* 2014; Bhunia 2018; Xiao *et al.* 2016)

Pattern	Description	IP Vendor	IC Developer	Foundry
P1	Untrusted IP vendor	Untrusted	Trusted	Trusted
P1	Untrusted foundry	Trusted	Trusted	Untrusted
P3	Untrusted EDA tool or rogue employee	Trusted	Untrusted	Trusted
P4	Commercial off-the-shelf (COTS) component	Untrusted	Untrusted	Untrusted
P5	Untrusted design house	Untrusted	Untrusted	Trusted
P6	Fabless IC design house	Untrusted	Trusted	Untrusted
P7	Untrusted IC developer with trusted IPs	Trusted	Untrusted	Untrusted

*Pattern P1: Untrusted Third-party IP Vendo*r—Driven by the demands of global IC industry (lower expenses, rapid marketing, etc.), most IC designers have to obtain some third-party IP cores for their designs. Adversaries at the untrusted vendor have the chance to implant IC Trojans, concealed from the IC designer, into the third party IP.

Pattern P2: Untrusted Foundry—Fabless design houses outsource the production of ICs to untrusted (mostly overseas) manufacturers. Adversaries employed in these untrusted foundries can reach the layers of the design and insert Trojans into the photolithography masks.

Pattern P3: Untrusted IC Developer—Production of complicated IC designs requires trained IC designers and professional design tools. In this pattern, adversaries are the insiders, who can use untrusted Electronic Design Automation (EDA) and Computer Aided Design CAD tools.

Pattern P4: Untrusted Commercial off-the-shelf (COTS) Components—Several COTS elements are inserted into designs. Mostly, COTS products are cheaper than custom-designed ones. However, no development stage can be trusted for Trojans, in COTS.
Pattern P5: Untrusted Design House—In this pattern, it is assumed that the whole supply chain is untrusted except foundry, i.e. ICs are produced in a trusted foundry, but third-party IP vendors and the design house are not trusted for disinfected designs.
Pattern P6: Untrusted Outsourcer—Pattern P6 is a combination of Pattern P1 and Pattern P2, and it concerns most fabless design houses. The designers utilize third-party IP vendors and untrusted foundries and fabricate these ICs in untrusted third-party foundries.
Pattern P7: Untrusted System Integrator—In this pattern, the customers expect to have a supplier that has both design and fabrication capabilities. But, untrusted system integrators exploit this expectation. The developer can use a diversity of resources to meet customer requests, but the completed hardware design may contain some inherent vulnerabilities (Rostami *et al.* 2013; Rostami *et al.* 2014; Bhunia 2018; Xiao *et al.* 2016).

7. Countermeasures against IC Trojan Attacks

Several methods for IC Trojan detection have been worked out and proposed, for many years. These methods can be grouped under three main categories, Trojan detection, design-for-trust, and split-manufacturing, as shown in Figure 5. These categories can also further be divided into several subcategories (Bhunia & Tehranipoor 2019).

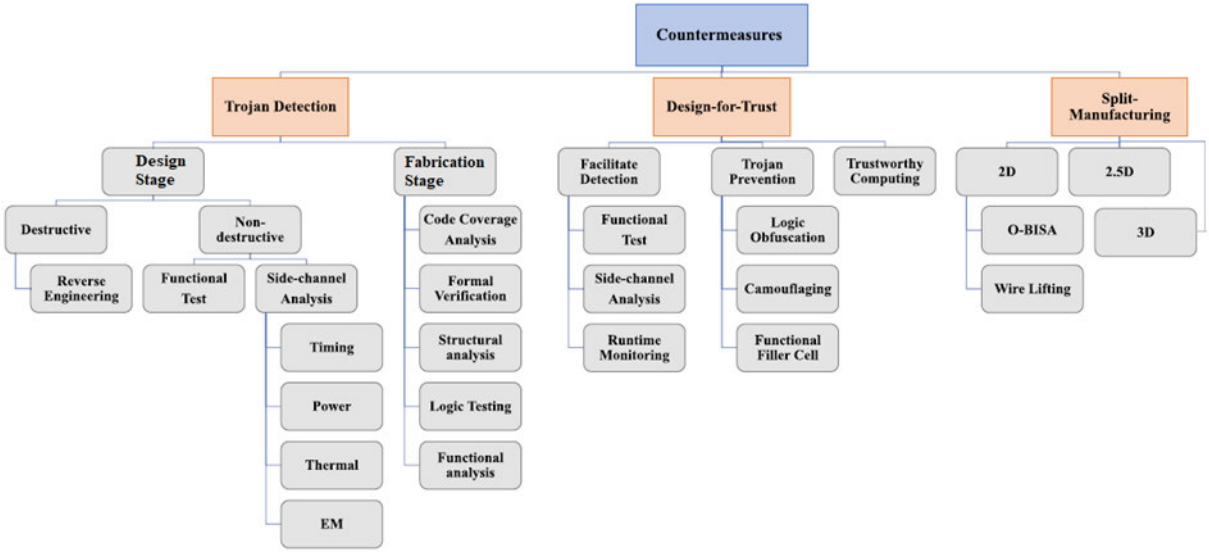

Figure 5. Taxonomy of IC Trojan countermeasures (Bhunia & Tehranipoor 2019).

Trojan detection is the fundamental and most utilized method to fight the IC Trojans. Its purpose is the verification of newly fabricated ICs with the present IC designs. These methods are used at the design phase to confirm IC designs or after the fabrication phase to validate fabricated ICs. They can be grouped under two subcategories, destructive and nondestructive methods (See Figure 5). Reverse-engineering is utilized by destructive methods to open an IC case and get images of layers to rebuild the design-for-trust (DFT) confirmation. Non-destructive methods can be grouped under two subcategories, functional test and side-channel analysis. Functional test technics apply test vectors to activate Trojans and check against the responses with the correct results (Bhunia *et al.* 2014; Banga & Hsiao 2009; Chakraborty & Bhunia 2009). IC Trojans are detected by side-channel signal analysis methods using circuit parameters, such as power dissipation (Agrawal *et al.* 2007; Aarestad *et al.* 2010), temperature (Forte *et al.* 2013), delay (Jin & Makris 2008; Xiao *et al.* 2013), and radiation (Stellari *et al.* 2014; Zhou *et al.* 2015). The side effects from Trojan activation alter power and/or heat dissipation, propagation or contamination delays, or radiation patterns due to additional circuit activity. Design stage Trojan detection methods are utilized to support IC developers and designers for validation of IP cores and the final designs. Present design stage detection techniques can be classified into formal verification (Jin *et al.* 2013; Guo *et al.* 2015; Rajendran *et al.* 2015; Rajendran *et al.* 2016), code coverage analysis (Hicks *et al.* 2010; Sturton *et al.* 2011), logic testing, functional analysis (Waksman *et al.* 2013), and structural analysis (Salmani & Tehranipoor 2013; Salmani *et al.* 2013; Tehranipoor *et al.* 2013).

DFT methodologies can be grouped under three subcategories with respect to their goals: Trojan prevention, facilitate detection, and trustworthy computing (See Figure 5). Trojan prevention methods are formed by techniques that aim to prevent IC Trojan implantation by adversaries. The adversaries need to know the function of the design first, in order to able to implant Trojans. Usually, reverse engineering is used by adversaries, who

are not employed in the design house, to determine circuit functionality (Bhunia & Tehranipoor 2019). These techniques can be sub classified into camouflaging (Rajendran *et al.* 2013; Cocchi *et al.* 2014), logic obfuscation (Roy *et al.* 2010; Baumgarten *et al.* 2010; Wendt *et al.* 2014), and functional filler cell (Xiao & Tehranipoor 2013). Facilitate detection can be sub classified into runtime monitoring (Forte *et al.* 2013; Narasimhan *et al.* 2012), side-channel analysis (Salmani & Tehranipoor 2012; Rajendran *et al.* 2011; Ramdas *et al.* 2014) and functional test; which targets triggering a Trojan from inputs and observing the Trojan impact from outputs (Salmani *et al.* 2012; Zhou *et al.* 2014). Trustworthy computing is the last class of DFT on untrusted elements (McIntyre *et al.* 2010; Liu *et al.* 2014).

Recently, split-manufacturing has been offered as an approach to IC foundries to be able to reduce the risks of Trojan insertion in IC design (Bhunia & Tehranipoor 2019). Current split manufacturing methods trust either 2D integration (Vaidyanathan *et al.* 2014; Jagasivamani *et al.* 2014; Hill *et al.* 2013), 2.5D integration (Xie *et al.* 2015), or 3D integration (Valamehr *et al.* 2013).

8. Future Work

The competition among IC vendors in the semiconductor market forced a trade-off, between IC security and the market cost-performance requirements on ICs. This development is expected to result in novel IC trust issues in the global IC supply chain. ULSI (Ultra Large Scale Integration), the successor of VLSI (Very Large Scale Integration) has become the main propulsion of the global IC market. With the advances in ULSI technology, IC Trojans will be more accurate, smaller, more concealed, and more difficult to be detected. Therefore, the adversaries are expected to launch new, more sophisticated, and unexpected, attacks which are even more difficult to be handled by existing countermeasures. Thus, countermeasure techniques against emerging IC Trojan attacks will need continuous further development.

9. Conclusion

The purpose of this article is to demonstrate the latest advances in the IC Trojan attack vectors and the countermeasures against the attacks. At the same time, it is intended to provide a general understanding and guidance to those who want to engage in IC Trojan research. Fighting against the IC Trojan threat will require everlasting and hard endeavor. With proper, progressive, scientific approaches, the difficulty and cost of IC Trojan attack elimination can be achieved.

References

Aarestad, J., Acharyya, D., Rad, R. & Plusquellic, J. (2010), "Detecting Trojans through leakage current analysis using multiple supply pads", IEEE Trans. Inf. Forensics Security, 893–904. doi: 10.1109/TIFS.2010.2061228

Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P. & Sunar, B. (2007), "Trojan detection using IC fingerprinting", Security and Privacy, SP'07, IEEE Symposium on IEEE, 296–310. doi: 10.1109/SP.2007.36

Alsop, T. (2020), "Semiconductor integrated circuits' global revenue 2009-2021", Statistica.

Banga, M. & Hsiao, M. S. (2009), "A novel sustained vector technique for the detection of hardware Trojans, in: VLSI Design", 22nd International Conference on, IEEE, 327–332. doi: 10.1109/VLSI.Design.2009.22

Baumgarten, A., Tyagi, A. & Zambreno, J. (2010), "Preventing IC piracy using reconfigurable logic barriers", IEEE Design & Test of Computers 27(1), 66-75. doi: 10.1109/MDT.2010.24

Behnam, P. (2018), "Validation of Hardware Security and Trust: A Survey," arXiv:1801.00649.

Belous, A. & Saladukha, V. (2020), "Viruses, Hardware and Software Trojans: Attacks and Countermeasures", Springer.

Bhunia, S. & Tehranipoor, M. (2019), "Hardware Security: A Hands-on Learning Approach", Elsevier.

Bhunia, S. & Tehranipoor, M. (2018), "The Hardware Trojan War: Attacks, Myths, and Defenses", Springer.

Bhunia, S., Hsiao, M. S., Banga, M. & Narasimhan, S. (2014), "Hardware Trojan attacks: threat analysis and countermeasures", Proceedings of the IEEE 102, 1229–1247. doi: 10.1109/JPROC.2014. 2334493

Chakraborty, R. S. & Bhunia, S. (2009), "Security against hardware Trojan through a novel application of design obfuscation", Proc. Int. Conf. Comput.-Aided Design, ACM, 113–116. doi: 10.1145/1687399.1687424

Cocchi, R. P., Baukus, J. P., Chow, L. W. & Wang, B. J. (2014), "Circuit camouflage integration for hardware IP protection", Proceedings of the 51st Annual Design Automation Conference, ACM, 1–5. doi: 10.1145/2593069.2602554

Farahmandi, F., Huang, Y. & Mishra, P. (2020), "System-on-Chip Security Validation and Verification", Springer.

Forte, D., Bao, C. & Srivastava, A. (2013), "Temperature tracking: an innovative run-time approach for hardware Trojan detection", Comput.-Aided Design (ICCAD), IEEE/ACM Int. Conf. IEEE, 532–539. doi: 10.1109/ICCAD.2013.6691167

Guo, X., Dutta, R. G., Jin, Y., Farahmandi, F. & Mishra, P. (2015), "Pre-silicon security verification and validation: a formal perspective", 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 1-6. doi: 10.1145/2744769.2747939

Hicks, M., Finnicum, M., King, S. T., Martin, M. M. & Smith, J. M. (2010), "Overcoming an untrusted computing base: Detecting and removing malicious hardware automatically", IEEE Symposium on Security and Privacy, 159–172. doi: 10.1109/SP.2010.18

Hill, B., Karmazin, R., Otero, C. T. O., Tse, J. & Manohar, R. (2013), "A split-foundry asynchronous FPGA", Custom Integrated Circuits Conference (CICC), IEEE, 1–4. doi: 10.1109/CICC.2013.6658536

Jagasivamani, M., Gadfort, P., Sika, M., Bajura, M. & Fritze, M. (2014), "Split-fabrication obfuscation: metrics and techniques", HOST, IEEE Int. Symp., 7–12. doi: 10.1109/HST.2014.6855560

Jin, Y. (2015), "Introduction to Hardware Security", Electronics 4, 763-784. doi:10.3390/electronics4040763

Jin, Y. & Makris, Y. (2008), "Hardware Trojan detection using path delay fingerprint", Hardware-Oriented Security and Trust, IEEE International Workshop , 51–57. doi: 10.1109/HST.2008. 4559049

Jin, Y., Yang, B. & Makris, Y. (2013), "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing", IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, TX, 99-106. doi: 10.1109/HST.2013.6581573

Karri, R., Rajendran, J., Rosenfeld, K. & Tehranipoor, M. (2010), "Trustworthy hardware: Identifying and classifying hardware trojans", IEEE Computer 43, 39–46. doi: 10.1109/MC.2010.299

Li, H., Liu, Q. & Zhang, J. (2016), "A Survey of Hardware Trojan Threat and Defense", ScienceDirect 55, 426-437.

Liu, C., Rajendran, J., Yang, C. & Karri, R. (2014), "Shielding heterogeneous MPSoCs from untrustworthy 3PIPs through security driven task scheduling", IEEE Transactions on Emerging Topics in Computing 2(4), 461-472. doi: 10.1109/TETC.2014.2348182

McIntyre, D., Wolff, F., Papachristou, C. & Bhunia, S. (2010), "Trustworthy computing in a multi-core system using distributed scheduling", IEEE 16th Int. On-Line Testing Symp., 211-213. doi: 10.1109/IOLTS.2010.5560200

Narasimhan, S., Yueh, W., Wang, X., Mukhopadhyay, S. & Bhunia, S. (2012), "Improving IC security against Trojan attacks through integration of security monitors", IEEE Design & Test of Computers 29(5), 37-46. doi: 10.1109/MDT.2012.2210183

Özcanhan, M. H. & Türksönmez, H. (2020), "A Strong Mutual Authentication Protocol for SHIELD", Advances in Electrical and Computer Engineering 20(4), 81-90. doi: 10.4316/AECE.2020.04010

Parker, D. (2010), "Our Excessively Simplistic Information Security Model and How to Fix It", ISSA Journal, 12-21.

Preneel, B. & Takagi, T. (2011), "Cryptographic Hardware and Embedded Systems—CHES 2011", Proc. 13th Internat. Workshop, Nara, Japan.

Qu, G. & Yuan, L. (2014), "Design things for the internet of things-an EDA perspective", Comput.-Aided Design (ICCAD), 2014 IEEE/ACM Int. Conf., 411–416. doi: 10.1109/ICCAD. 2014.7001384

Rad, R. M., Wang, X., Tehranipoor, M. & Plusquellic, J. (2008), "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans", Proc. IEEE/ACM Int. Conf. on Computer-Aided Design, San Jose, CA, USA, 632–639. doi:10.1109/ICCAD.2008.4681643

Rajendran, J., Dhandayuthapany, A. M., Vedula, V. & Karri, R. (2016), "Formal security verification of third party intellectual property cores for information leakage", 29th Int. Conf. VLSI Design and 15th Int. Conf. Embedded Systems (VLSID), Kolkata, 547-552. doi: 10.1109/VLSID.2016.143

Rajendran, J., Jyothi, V., Sinanoglu, O. & Karri, R. (2011), "Design and analysis of ring oscillator based design-for-trust technique", 29th VLSI Test Symposium, Dana Point, CA, 105-110. doi: 10.1109/VTS.2011.5783766

Rajendran, J., Sam, M., Sinanoglu, O. & Karri, R. (2013), "Security analysis of integrated circuit camouflaging," Proc. ACM SIGSAC Conf. Comput. & Comm. Security, ACM, 709–720. doi:.10.1145/2508859.2516656

Rajendran, J., Vedula, V. & Karri, R. (2015), "Detecting malicious modifications of data in third-party intellectual property cores", 52nd ACM/EDAC/IEEE Design Autom. Conf., CA, 1-6. doi: 10.1145/2744769.2744823

Ramdas, A., Saeed, S. M. and Sinanoglu, O. (2014), "Slack removal for enhanced reliability and trust", 9th IEEE Int. Conf. Design & Technol. Integrated Systems in Nanoscale Era (DTIS), 1-4. doi: 10.1109/DTIS.2014.6850660

Rostami, M., Koushanfar, F., Rajendran, J. & Karri, R. (2013), "Hardware Security: Threat Models and Metrics", 2013 IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD). doi: 10.1109/ICCAD. 2013.6691207

Rostami, M.; Koushanfar, F. & Karri, R. (2014), "A Primer on Hardware Security: Models, Methods, and Metrics", Proc. IEEE 102, 1283-1295. doi: 10.1109/JPROC.2014.2335155

Roy, J. A., Koushanfar, F. & Markov, I. L. (2010), "Ending piracy of integrated circuits", Computer 43, 30–38.

doi: 10.1109/MC.2010.284

Salmani, H. & Tehranipoor, M. (2012), "Layout-aware switching activity localization to enhance hardware Trojan detection", IEEE Trans. Inf. Forensics Security 7(1), 76-87. doi: 10.1109/TIFS.2011.2164908

Salmani, H. & Tehranipoor, M. (2013), "Analyzing circuit vulnerability to hardware Trojan insertion at the behavioral level", IEEE Int. Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), New York City, NY, 190-195. doi: 10.1109/DFT.2013.6653605

Salmani, H. (2018), "Trusted Digital Circuits: Hardware Trojan Vulnerabilities, Prevention and Detection", Springer, Cham.

Salmani, H., Tehranipoor, M. & Karri, R. (2013), "On design vulnerability analysis and trust benchmarks development", IEEE 31st Int. Conf. Comput. Design (ICCD), Asheville, NC, 471-474. doi: 10.1109/ICCD.2013.6657085

Salmani, H., Tehranipoor, M. & Plusquellic, J. (2012), "A novel technique for improving hardware Trojan detection and reducing Trojan activation time", IEEE Trans. Very Large Scale Integration (VLSI) Systems, 112–125. doi: 10.1109/TVLSI.2010.2093547

SIA, Semiconductor Industry Association (2016), "Beyond Borders: How an Interconnected Industry Promotes Innovation and Growth", SIA, Washington, DC, USA.

Stellari, F., Song, P., Weger, A. J., Culp, J., Herbert, A. & Pfeiffer, D. (2014), "Verification of untrusted chips using trusted layout and emission measurements", Hardware-Oriented Security and Trust (HOST), IEEE International Symposium on IEEE, 19–24. doi: 10.1109/HST.2014.6855562

Sturton, C., Hicks, M., Wagner, D. & King, S. T. (2011), "Defeating uci: Building stealthy and malicious hardware", IEEE Symposium on Security and Privacy, 64–77. doi: 10.1109/SP.2011.32

Tehranipoor, M. & Koushanfar, F. (2010), "A survey of hardware Trojan taxonomy and detection", IEEE Design & Test of Computers 27, 10–25. doi: 10.1109/MDT.2010.7

Tehranipoor, M., Salmani, H. & Zhang, X. (2013), "Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection", Springer Science & Business Media.

Vaidyanathan, K., Das, B. P. & Pileggi, L. (2014), "Detecting reliability attacks during split fabrication using test-only BEOL stack", Proc. 51st Annual Design Automation Conf., ACM, 1–6. doi: 10.1145/2593069.2593123

Valamehr, J., Sherwood, T., Kastner, R., Marangoni-Simonsen, D., Huffmire, T., Irvine, C. and Levin, T. (2013), "A 3-D split manufacturing approach to trustworthy system development", IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 32, 611–615. doi: 10.1109/TCAD.2012.2227257

Waksman, A., Suozzo, M. & Sethumadhavan, S. (2013), "FANCI: identification of stealthy malicious logic using boolean functional analysis", Proc. 2013 ACM SIGSAC Conf. Computer & Communications Security, ACM, 697–708. doi: 10.1145/2508859.2516654

Wendt, J. B. & Potkonjak, M. (2014), "Hardware obfuscation using PUF-based logic", IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, 270-271. doi: 10.1109/ICCAD.2014.7001362

Xiao, K. & Tehranipoor, M. (2013), "BISA: Built-in self-authentication for preventing hardware Trojan insertion," IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST), 45-50. doi: 10.1109/HST.2013.6581564

Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S. & Tehranipoor, M. (2016), "Hardware Trojans: lessons learned after one decade of research", ACM Trans. Des. Autom. Electron. Syst. 22(1), 6:1–6:23. doi: 10.1145/2906147

Xiao, K., Zhang, X. & Tehranipoor, M. (2013), "A clock sweeping technique for detecting hardware Trojans impacting circuits delay", IEEE Design & Test, 26–34. doi: 10.1109/MDAT.2013.2249555

Xie, Y., Bao, C. & Srivastava, A. (2015), "Security-aware design flow for 2.5D IC technology", Proc. 5th Int. Workshop on Trustworthy Embedded Devices, ACM, 31–38. doi: 10.1145/2808414.2808420

Zhou, B., Adato, R., Zangeneh, M., Yang, T., Uyar, A., Goldberg, B., Unlu, S. and Joshi, A. (2015), "Detecting hardware Trojans using backside optical imaging of embedded watermarks," 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 1-6. doi: 10.1145/2744769.2744822

Zhou, B., Zhang, W., Thambipillai, S. & Teo, J. (2014), "A low cost acceleration method for hardware Trojan detection based on fan-out cone analysis", International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), New Delhi, 1-10. doi: 10.1145/2656075.2656077