Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3s (2025)

Evaluation of Hardware Trojans in the Adder circuits

Allagadda Seetharamaraju[1], Dr. Arun Raaza[2], Dr. Abhijit Narayanrao Banubakode[3], Dr. M. Meena[4]

[1, 2,4]Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai.

[3]MET Institute of Computer Science, Mumbai Educational Trust, Mumbai, 400050, India.

Article History:

***Received**: 18-09-2024*

***Revised**: 01-11-2024*

***Accepted**: 19-11-2024*

Abstract:
Exporting the design and fabrication of Integrated Circuits (ICs) presents a significant risk to our vital infrastructure since an attacker may exploit them by circumventing security measures by triggering a hardware Trojan. These malicious design changes implemented at an untrusted manufacturing site have the potential to leak nearly any confidential information from a protected system to an attacker. One of the most serious dangers to hardware security has been the hardware Trojan. We present a summary of recent advances in Trojan detection approaches, grouped according to their relevance to various Trojan kinds. Adder has indeed been implemented effectively in integrated circuits like arithmetic circuits as well as arithmetic accelerators. However, recent research indicates that adder circuits contain security flaws as well. Nevertheless, there has been relatively little study of hardware Trojans within adder circuits. The Trojans are based on the attributes of adder circuits. The efficacy of hardware Trojans is often evaluated using adder circuit assessment methodologies. The performance characteristics of adder like power and delay are evaluated with and without hardware Trojans.

Keywords: Hardware Trojan, Adders, arithmetic circuits.

1. Introduction

Hardware Trojans have evolved into a severe hazard to both customers and suppliers as the globalization of IC design and manufacturing has increased. Because Integrated circuits are used in vital applications, the impacts of these Trojans are a highly severe concern. Regrettably, the utilization of untrustworthy foundries as well as design software cannot be avoided because the complexities of integrated circuits and the intricacy of their production have increased dramatically. Most IC manufacturers are unable to establish a reliable foundry for manufacturing. As a consequence, powerful hardware Trojan detection methods are required. A hardware Trojan is a harmful element that is inserted in a silicon chip and causes abnormal behaviour [1, 2].

Hardware Trojans might infect microcontrollers, CPUs, FPGAs, ASICs, and a wide range of other integrated circuits. Figure 1 depicts the classification of hardware Trojan detecting methodologies offered in [3, 4].They are either harmful or non-destructive. Destructive methods are generally employed to produce a Trojan-free chip termed as Golden Chip (GC), which may be exceedingly costly and time demanding [5]. As a result, damaging the testing of chips is frequently impractical. Furthermore, Process Variations (PVs), comparison to GC might induce false positives

in the Trojan-free chips, and evaluating only a fraction of the chips might well be ineffectual since adversaries could implant a Trojan merely a tiny proportion of the chip [6].

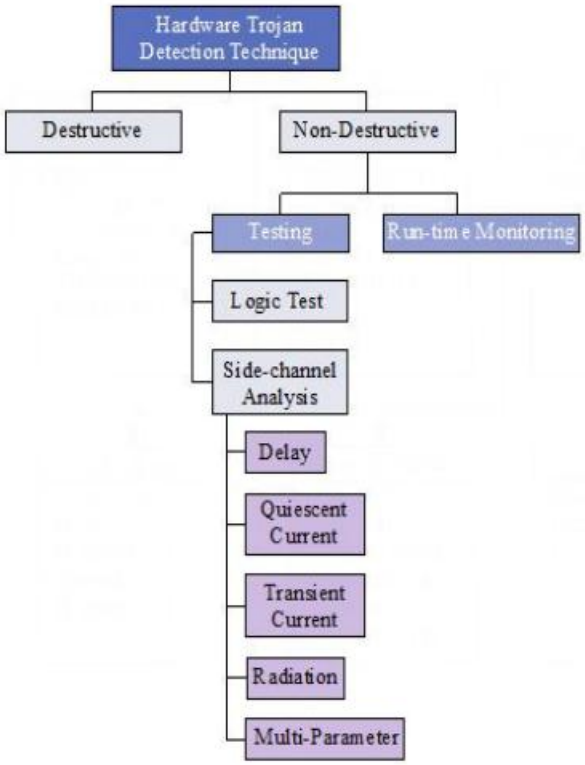

Figure 1: Classification of existing hardware Trojans

Non-destructive approaches are divided into two categories: run-time monitoring or testing. Security circuits, such as scan chains as well as self-test circuits, may be designed to facilitate testing. This increases the efficacy of Trojan detection, however, necessitates that perhaps the testing circuitry not even be affected. The Trojan cannot be activated throughout testing, or it might be programmed to remain dormant until the testing is finished. As a consequence, a Trojan which does not change the chip topology or design may be difficult to detect during testing.Logic testing and side-channel evaluation are two types of testing methodologies. Random test vectors are used in logic testing methodologies to trigger Trojan circuits as well as analyses their impact on chip outcomes. The difficulty of evaluating all inner nodes including logic values is a challenge with this method since chips may have extremely high gate density, making thorough testing intractable[7,8].

When ICs have little complexity and aren't dense, side-channel methods are routinely used and quite successful. Detecting tiny or scattered Trojans on complicated or dense devices, on the other hand, might be difficult. As a result, Trojan circuits are frequently quite tiny in comparison to the IC design. They are very often introduced during the manufacturing process of the chip layout or incorporated by reconfiguring preexisting circuitry [9].

Arithmetic unit, arithmetic circuit-based FFT, arithmetic neural network accelerators[10], and other applications have successfully used digital adder-based computation. Because arithmetic circuits are commonly used, they present additional security concerns [11]. This is mostly due to the

possibility of malevolent attackers exploiting intrinsic faults in the arithmetic circuitry [11]. As a result, the safety of arithmetic circuits must be researched. Several possible vulnerability models, as well as solutions for arithmetic circuits, were examined by Yellu et al.[12]. Regazzoniet al.[13] stated that the arithmetic circuit could leak information, but no precise design was supplied. Arithmetic adder circuitry, as per Dou et al. [14], may be more vulnerable to hardware Trojans . Nonetheless, a full investigation of the hardware Trojan hidden in the arithmetic circuitry is lacking. As a consequence, incorporating arithmetic computation into hardware design not only provides advantages, but also introduces new security vulnerabilities that have not yet been thoroughly examined.

Hardware Trojan represents one of the most severe threats to hardware security. Trojan attacks on digital circuits are often carried out by switching the circuit's outputs. Nevertheless, since certain erroneous outputs are tolerable by arithmetic circuits, the error tolerances of arithmetic circuits might lead to non-functional for attacks. Further research on the efficacy of hardware Trojans on arithmetic circuits has been required. As a consequence, a detailed study is necessary to determine the sensitivity of the arithmetic circuit for hardware Trojan injection.

In this work, different concepts of hardware Trojan circuits have been presented and introduced into adder circuits: function-destructive Trojan as well as information-leakage Trojan. Depending on adder circuit measurements, this letter examines the security problems of adder circuits to the hardware Trojan insertions. It is intended to provide designers with guidance for understanding security vulnerabilities in adder circuits, while considering extensive detection mechanisms in subsequent circuit designs.Various approaches in adder circuits might bring different defects into the adder circuit. As a result, since adder circuits lack a standardized truth table to represent their functionalities, their computation potential is governed by power usage, speed, as well as area [15].In the section 2, we have discussed how the hardware Trojans are implemented into the circuits. In section 3, the effects of inserting hardware into the arithmetic circuits are discussed. Section 4 demonstrates the simulation results of the

2. Design of Hardware Trojan

Because of the globalization of integrated circuits, attackers now have more options to hack/damage hardware. Any IC manufacturing outsourcing organization may become a possible threat for inserting harmful changes known as hardware Trojans. The examination of IC vulnerabilities is now gaining worldwide interest. It is also necessary to assess the possible hazards if adder circuits are inserted hardware Trojans. As a result, the security of adder circuits is a key component that has been overlooked.

2.1 Hardware Trojan:

A hardware Trojan (HT) is indeed a redundant circuitry containing malicious functionality that an intruder instals into the existing circuitry on intent.HTs are classified into two types based on their payload logic: function-destructive Trojans as well as information-leakage Trojans[16,17].

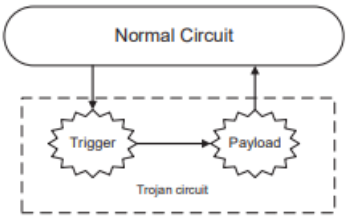

Figure 2: Illustration of the infected Trojan

Function-destructive Trojans seek to degrade circuit performance by destroying function. This is commonly accomplished by adding or removing circuit structures. In an adder, for illustration, the logic functionality may be destroyed by interfering with the adder's outputs, that modifies the original specified truth table. Nevertheless, error metrics dictate an adder circuit's computing capabilities and reliability. Whenever a function-destructive Trojan has been inserted into an arithmetic circuitry, the output might change, whereas a digital circuit consistently produces the same result.To evaluate the efficacy of Function-destructive Trojans on adders, a thorough study is required[18].

Information-leakage HT is intended to attack a part of the original circuit that holds sensitive data, .The chosen circuitry signal was transmitted to the attacker through side - channel information or the circuit's output channels by changing the necessary circuitry logic.An attacker may study such information to get critical details, such as encrypted keys, and so gain access to the secure data in the analogous circuit. Using adder circuit features, many information-leaking Trojans have indeed been constructed. The suggested information-leaking Trojans have been designed to attack logic locking, a frequently used hardware obfuscation mechanism. Following the activation of the Trojans, a straightforward manipulation attack reveal the data. [18] assumes that the attacker could receive the test vector during the testing phase, and that the Trojan's activation vector may subsequently be tailored to escape detection during the test phase. However, ensuring that perhaps the test vectors remain freely accessible is tough. There was no assurance that the key's output would not impact the circuit's planned outcome. Attackers may benefit from adder circuits that can tolerate mistakes.

3. Hardware Trojansin Adder Circuits

The most recent research into digital full adders has concentrated on arithmetic units. Furthermore, amongst some of the arithmetic subunits, adder analyses have received a significant amount of attention[18]. 1) Adders are necessary aspects of many arithmetic subsystems that require adders to accomplish fundamental data computations.2) Adders are indeed fundamental components of digital logic systems, and their performance is influenced by them. As a result, approximation adders have received a lot of attention. In this study, we shall analyse a 13T hybrid adder.

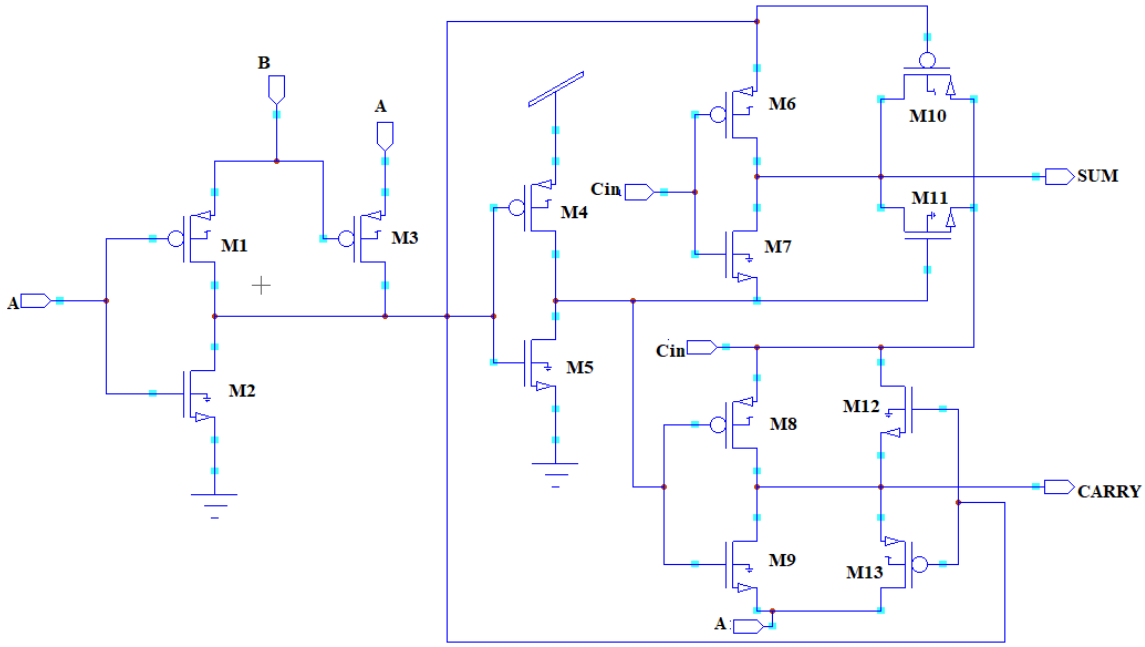

Figure 3: Schematic Representation of 13T Hybrid adder

Figure 3 illustrates the suggested hybrid full adder architecture, which uses just 13 transistors. It is primarily composed of five distinct logic blocks created utilizing the hybrid GDI approach. The XNOR/XOR, two muxes, one transmission gate having swing restoration (M10-M11), and another pass transistor block with swing restoration (M12-M13). The XNOR/XOR component (M1-M2-M3-M4-M5) has been generated using a modified GDI approach. Because the pathway of the inverters employed within the XNOR/XOR sections has little to no voltage loss, these are implemented with ordinary threshold transistors. The GDI MUX-1 (M6-M7) mixes the output of XOR (A $\oplus$ B) along with XNOR (AXNOR B) using the control input (Cin) for generating the sum functionality. The GDI MUX-2(M8,M9) generates the carry signal (Cout) by multiplexing the Cin& B inputs plus the control signal line that comes from the XNOR logical output (A XNOR B). Nevertheless, while prior adders struggled to offer complete swing logic, the suggested topology did so with just 13 transistors. The suggested architecture ensures complete wing by placing a transmission gate along with pass transistor blocks at the total and carry outputs, correspondingly.

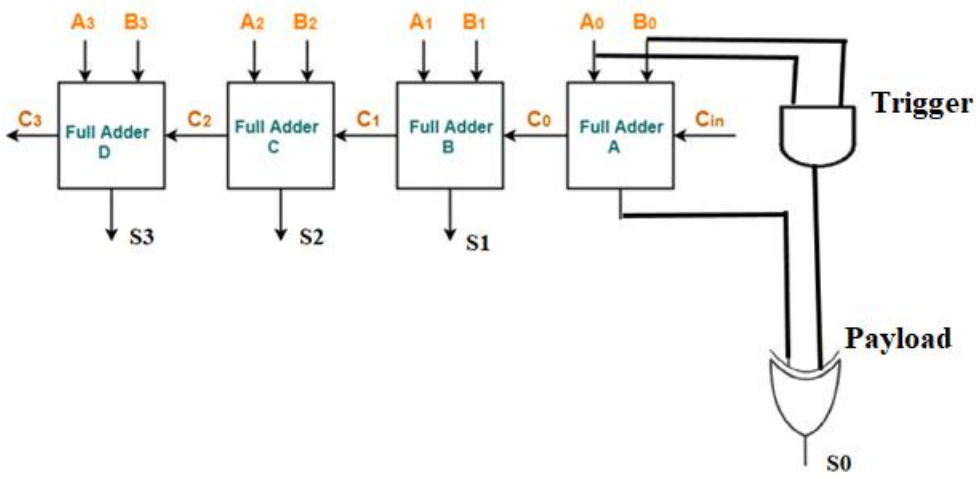

Figure 4: Insertion of the Hardware Trojan into lower full adder of 4-bit RCA.

As an illustration in Figure 4, the the full adder has been introduced with a hardware Trojan, as illustrated in Figure 4. The HT's trigger circuitry is made up of a AND gate, and also the payload circuitry is made up of an XOR gate. This HT's attack approach is as follows:Whenever the adder circuit's inputs are a0=b0=1, the HT would flip the output of the s0 for the adder. To summarize, whenever a Function-destructive Trojan gets placed into a full adder, the outcome of the circuit might well be altered, however the functionality of the full adder is unaffected. Surprisingly, certain HTs might also aid in the improvement of adder circuit efficiency. In conclusion, if the adder circuit is placed in a Function-destructive Trojan, simply switching the output will not harm the adder circuitry.The Figure 5 and 6 represents the full swing GDI logic based AND and XOR gates respectively.

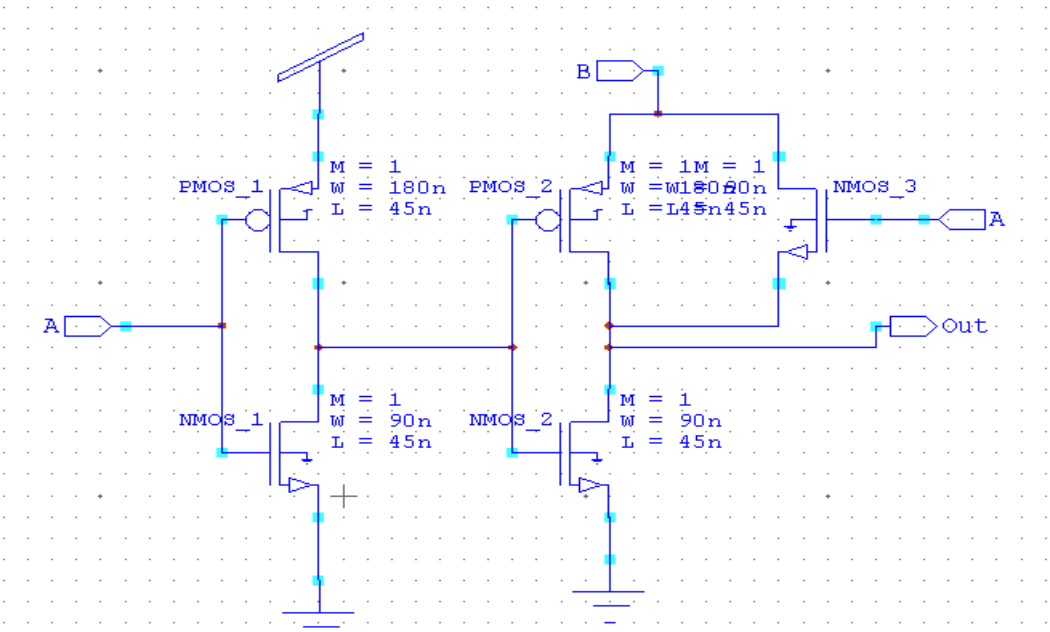

Figure 5: Schematic Representation of full swing AND gate

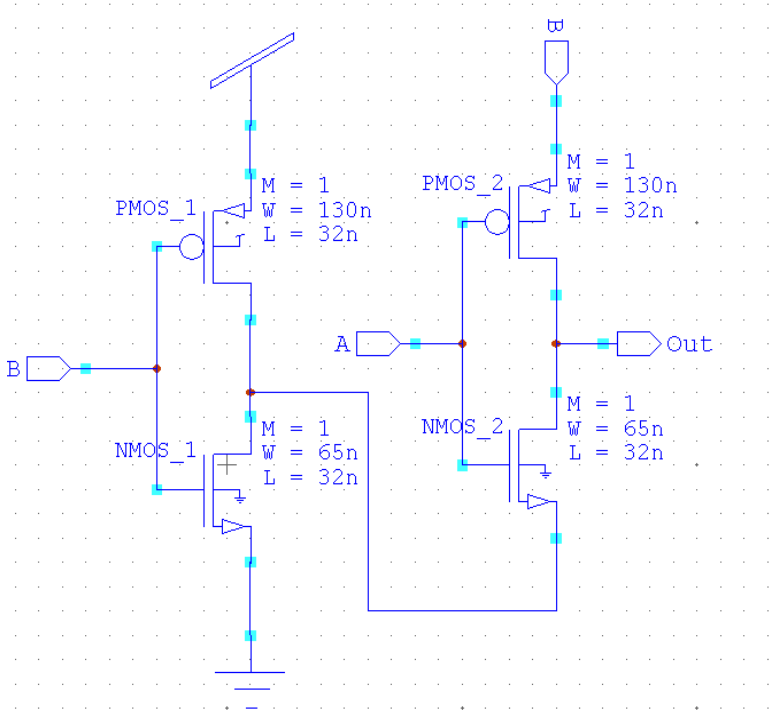

Figure 6: Schematic Representation of XOR gate

4. Simulation Results

The following subsection describes the computational outcomes and viability evaluation of the suggested full adder in conjunction with and without Hardware Trojans. The simulations have been conducted using 45 nm CMOS technology with a supply voltage of 1 V. The simulation results for power and latency are compared to the hardware Trojan-induced adder. To ensure consistency in assessments, the adder circuits given in this study are operating at a rate of 20 KHz and with a temperature of 27°C. None of the entire adder topologies need any additional buffers to obtain accurate outcomes. The simulation results of the AND gate and XOR are demonstrated in the Figures 7 and 8 respectively. Also the transient simulation result of 1-bit adder with and without hardware Trojans are demonstrated in Figure 9 and 10 respectively.

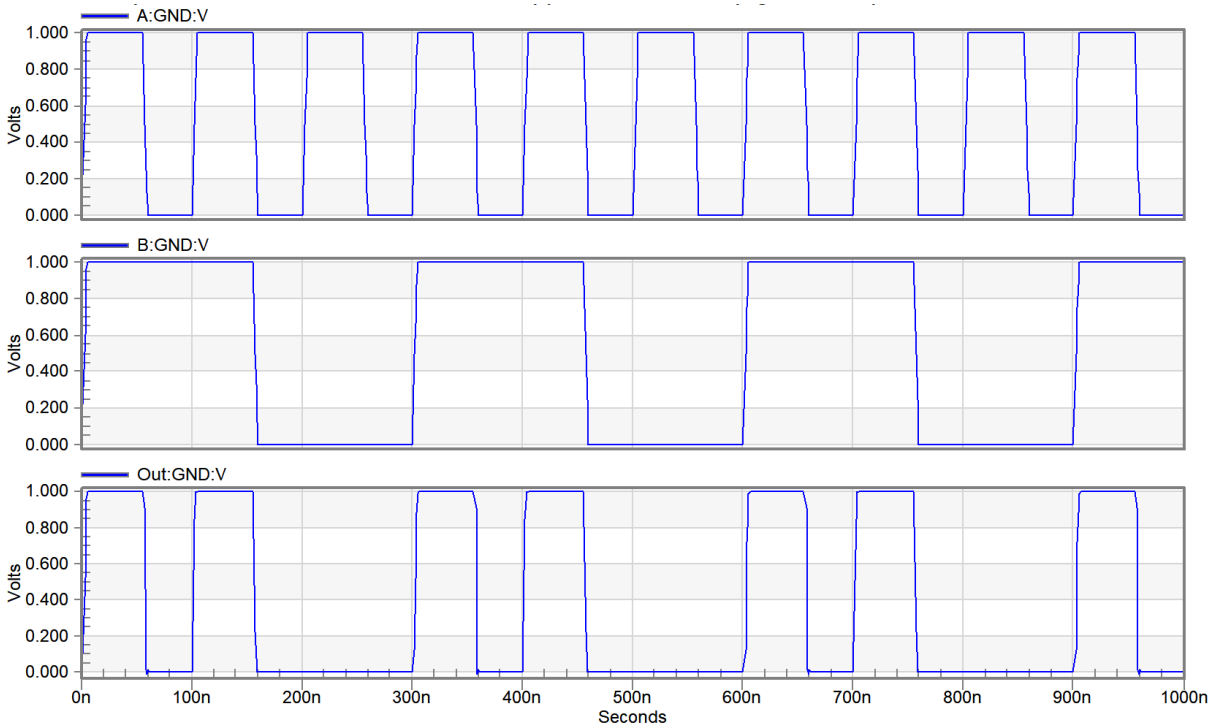

Figure 7: Transient Simulation result of AND gate

The Process variation analysis w.r.t SS,FF and TT for adders with and without hardware Trojans has been carried out at room temperature with supply voltage of 1V. The power consumption and delay of adders with and without hardware Trojans w.r.t process variation have been demonstrated in Figures 11 and 12 respectively. The voltage variation analysis from 0.7V to 1V for adders with and without hardware Trojans has been carried out at room temperature with TT process. The power consumption and delay of adders with and without hardware Trojans w.r.t voltage variation have been demonstrated in Figures 13 and 14 respectively. The temperature variation analysis from -25^{0}C to 75^{0}C for adders with and without hardware Trojans has been carried out at a supply voltage with TT process. The power consumption and delay of adders with and without hardware Trojans w.r.t temperature variation have been demonstrated in Figures 15 and 16 respectively.

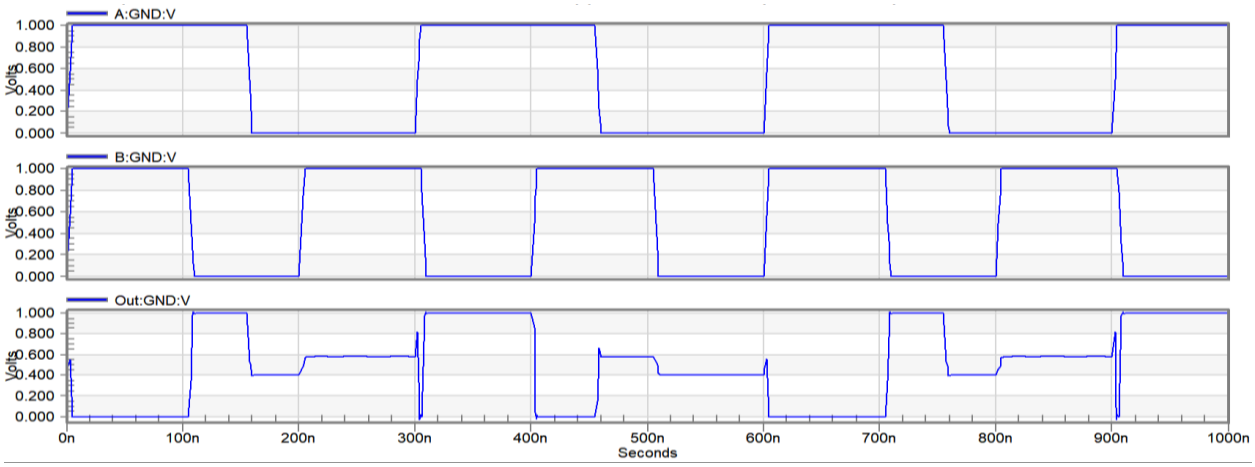

Figure 8: Transient Simulation result of XOR gate

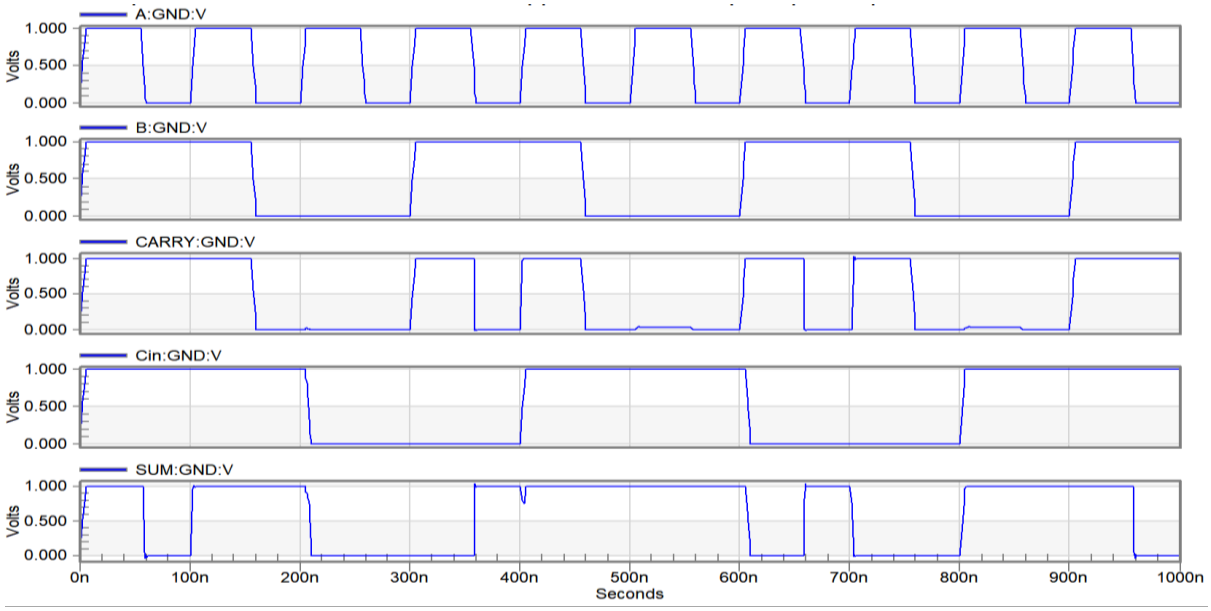

Figure 9: The transient analysis of proposed 1-bit adder

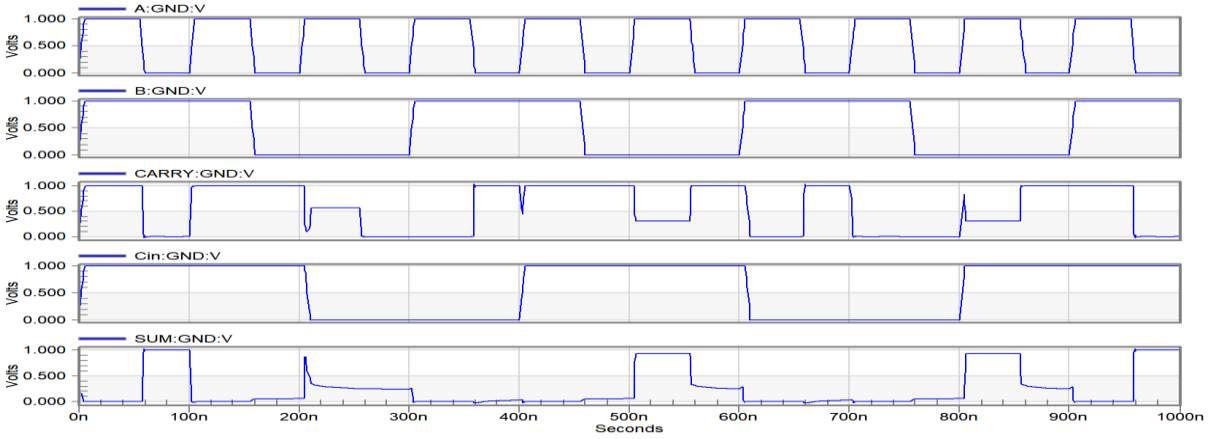

Figure 10: The transient analysis of proposed HT 1-bit adder

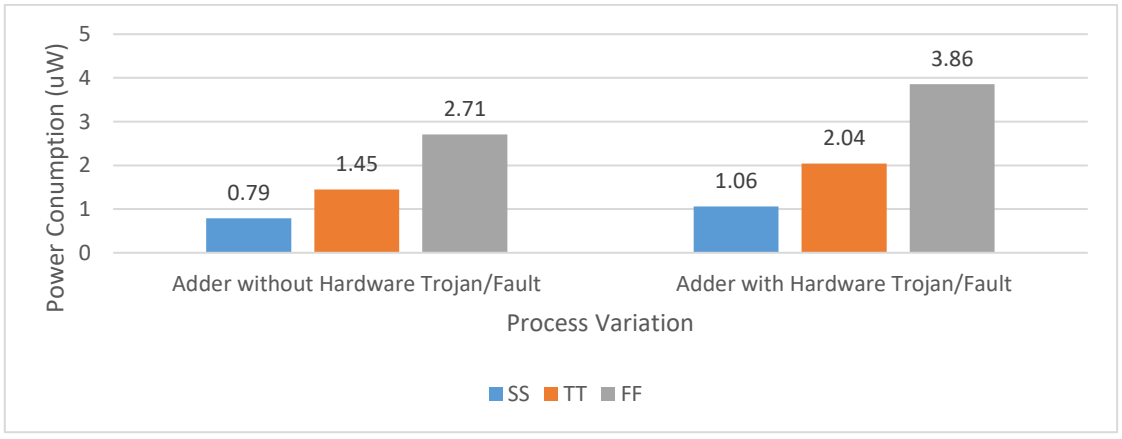

Figure 11: Power Consumption of Adder with and without Hardware Trojan/ Fault injection w.r.t process variation

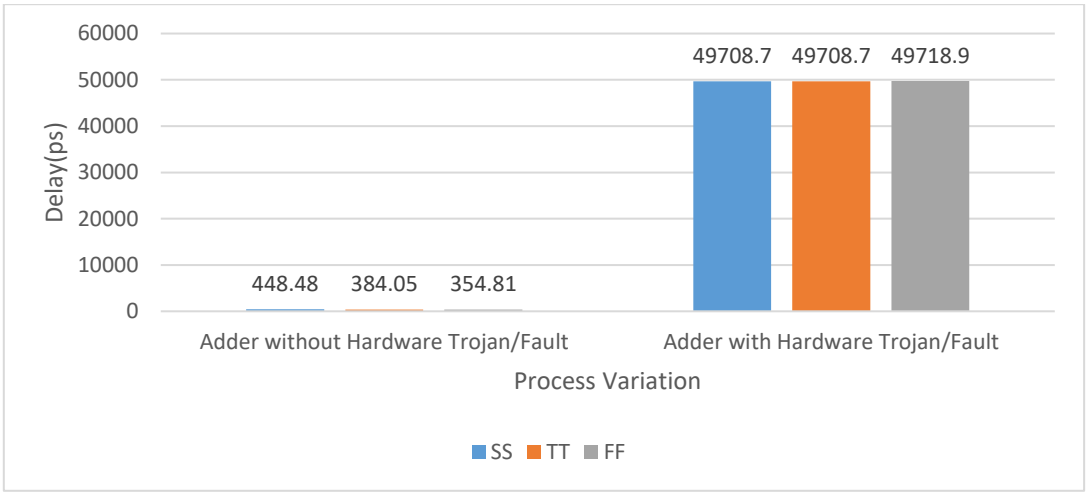

Figure 12: Delay of Adder with and without Hardware Trojan/ Fault injection w.r.t process variation

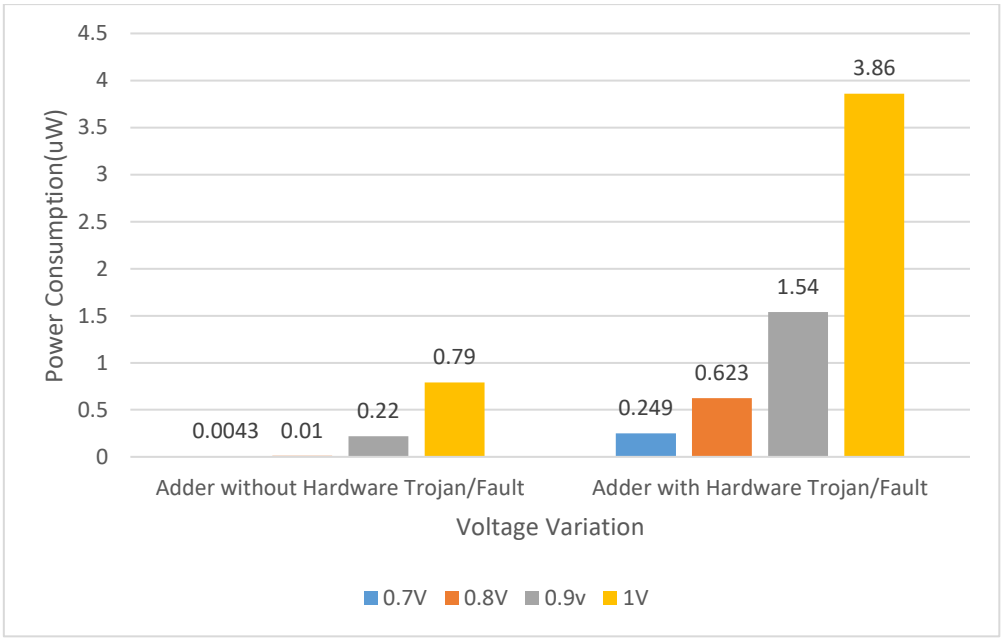

Figure 13: Power Consumption of Adder with and without Hardware Trojan/ Fault injection w.r.t voltage variation

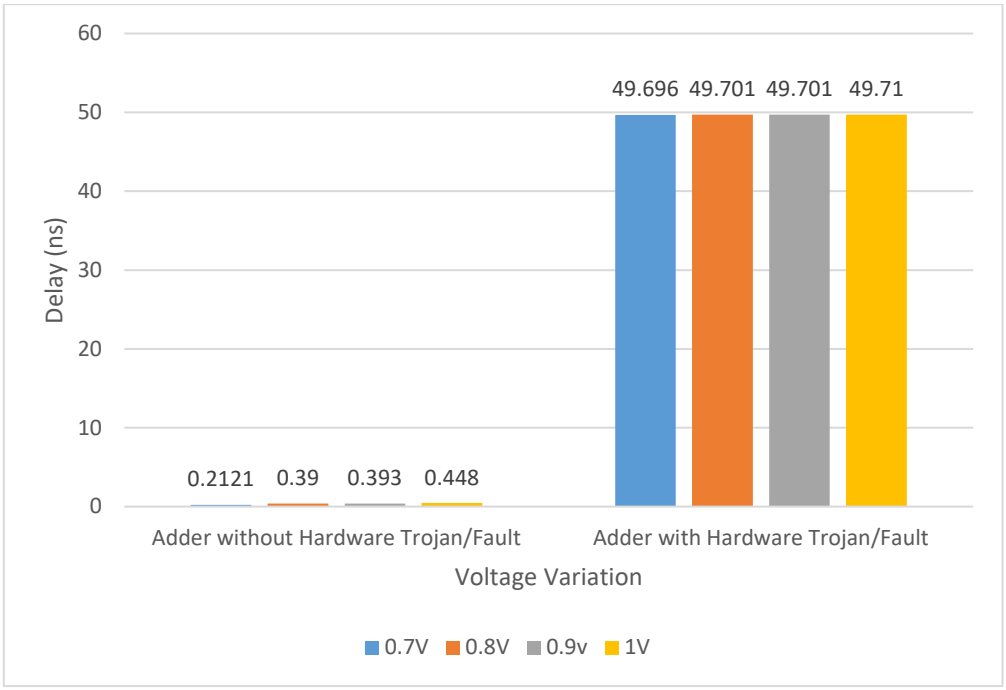

Figure 14: Delay of Adder with and without Hardware Trojan/ Fault injection w.r.t voltage variation

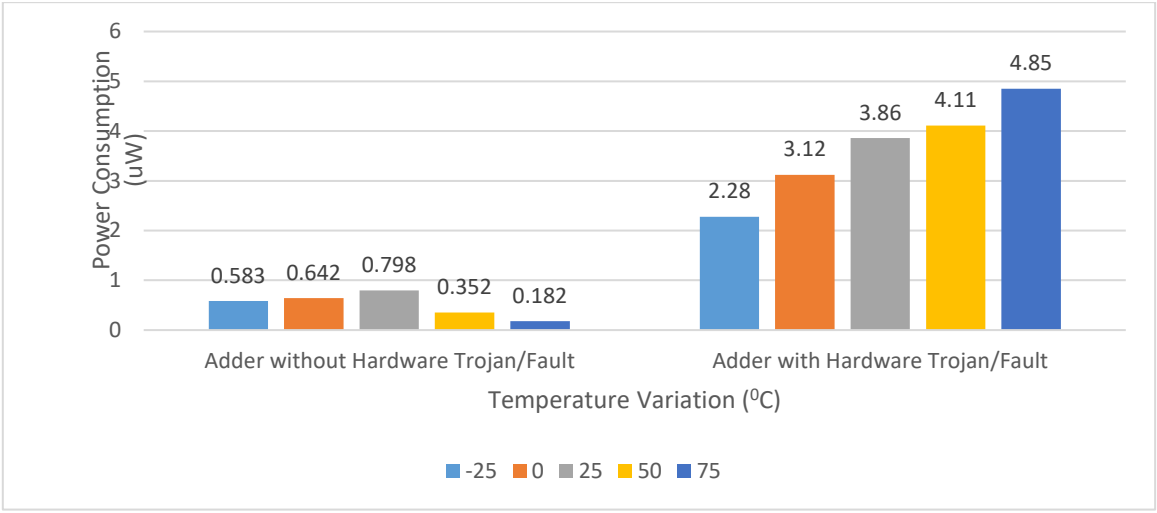

Figure 15: Power Consumption of Adder with and without Hardware Trojan/ Fault injection w.r.t Temperature variation

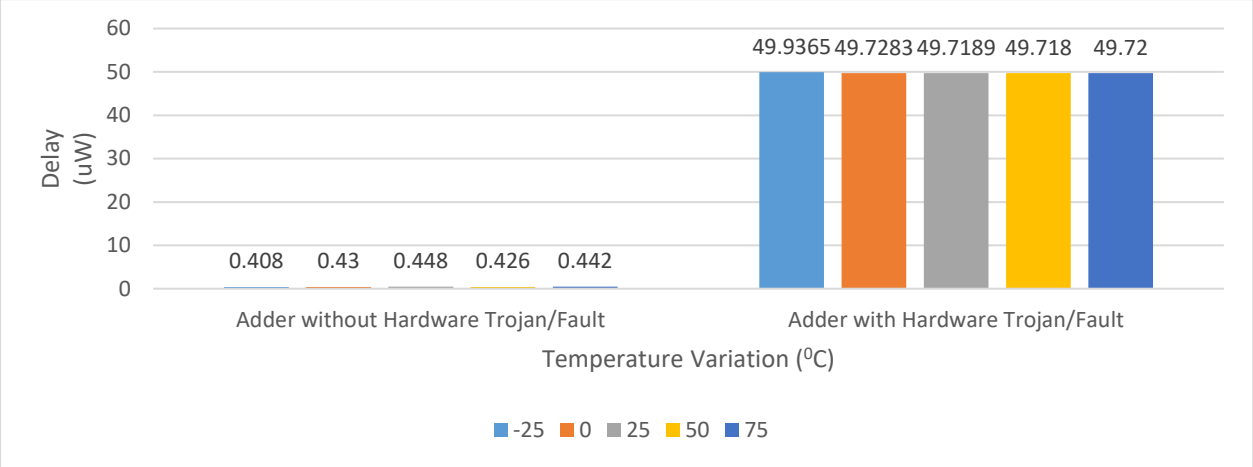

Figure 16: Delay of Adder with and without Hardware Trojan/ Fault injection w.r.t Temperature variation

Here the adder without HT is considered as the golden reference, whenever the HardwareTrojaninserted adder circuit is compared with the golden reference the performance will be worsened. This can be demonstrated from the Figures 11-16. It is evident that the HT circuit performance gets worsened in terms of delay, area and power consumption.

5. Conclusion

In this work,hardware Trojans areinserted into the adder circuits, to assess the security problems of adder circuits for HT insertions. Moreover, research indicates that the Function-based destructive Trojan may not be able to immediately change the result to degrade the performance of the full adder, because the metric influences the effectiveness of the adder circuit.Changing the outputs of the adder circuitry arbitrarily may even enhance its accuracy, which would be opposed to the goal of a Trojan destruction operation. This implies that installing a Function based destructive Trojan in the adder is more challenging than installing one in a circuitry. The performance of the adder circuitry degrades with the insertion of hardware trojans.

Reference:

[1] M. Banga and M. Hsiao, “A region based approach for the identification of hardware trojans,” in Proc.IEEE Int. Workshop on Hardware-Oriented Security and Trust, pp. 40–47, 2008.

[2] Sheikh Ariful Islam. 2019. On the (In)security of Arithmetic Computing Synthesis. arXiv e-prints, Article arXiv:1912.01209 (Dec 2019), arXiv:1912.01209 pages. arXiv:1912.01209 [cs.CR]

[3] V. Camus, M. Cacciotti, J. Schlachter, and C. Enz. 2018. Design of Arithmetic Circuits by Fabrication of False Timing Paths: The Carry Cut-Back Adder. IEEE Journal on Emerging and Selected Topics in Circuits and Systems 8, 4 (Dec 2018), 746–757. https://doi.org/10.1109/JETCAS.2018.2851749.

[4] S. Narasimhan and S. Bhunia, “Hardware trojan detection,” in Introduction to Hardware Security and Trust, M. Tehranipoor and C. Wang (Eds.), Springer, New York, NY, pp. 339– 364, 2012.

[5] C. Bao, D. Forte, and A. Srivastava, “On reverse engineering-based hardware trojan detection,” IEEE Trans. Comput.-Aided Design Integr. Circuits and Sys., vol. 35, no. 1, pp. 49–57, 2015.

[6] Suresh Cheemalavagu, Pinar Korkmaz, Krishna Palem, and Lakshmi Chakrapani. 2020. A Probabilistic CMOS Switch and its Realization by Exploiting Noise. (02 2020)

[7] M. Abramovici and P. Bradley, “Integrated circuit security: New threats and solutions,” in Proc. Workshop on Cyber Security and Inform. Intelligence Res., article no. 55, 2009.

[8] D. McIntyre, F. Wolff, C. Papachristou, and S. Bhunia, “Dynamic evaluation of hardware trust,” in Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust, pp. 108–111, 2009.

[9] Tirmare, Aarti Hemant, et al. "VLSI architecture-based implementation of motion estimation algorithm for Underwater Robot Vision System." Journal of VLSI Circuits and Systems 6.2 (2024): 115-121.

[10] Liu, W., Liao, Q., Qiao, F., Xia, W., Wang, C., Lombardi, F.: Approxi-mate designs for fast fourier transform (FFT) with application to speechrecognition.IEEE Trans. Circuits Syst. I-Regul. Pap.66, 4727–4739(2019)

[11] Liu, W., Gu, C., O’Neill, M.Q.G., Montuschi, P., Lombardi, F.: Se-curity in arithmetic computing and arithmetic computing for se-curity: challenges and opportunities.Proc. IEEE108, 2214–2231(2020)

[12] JS, Prasath. "Design and implementation of modeling and tuning of first order process with dead time using PID controller." International Journal of communication and computer Technologies 7.1 (2019): 1-6.

[13] Regazzoni, F., Alippi, C., Polian, I.: Security: the dark side of arithmetic computing? IEEE ACM International Conference on Computer-Aided Design, Digest of Technical Paper (ICCAD), San Diego, CA,USA, November 5, pp. 1–6 (2018)

[14] Dou, Y., Yu, S., Gu, C., O’Neill, M., Wang, C., Liu, W.: Security analysisof hardware trojans on arithmetic circuits. Proceedings of the ACMGreat Lakes Symposium VLSI (GLSVLSI), Virtual, Online, China,September 9, pp. 315–320 (2020)

[15] Traiola, M., Virazel, A., Girard, P., Barbareschi, M., Bosio, A.: A survey of testing techniques for arithmetic integrated circuits.Proc. IEEE108, 2178–2194 (2020).

[16] Liu, W., Chen, L., Wang, C., O’Neill, M., Lombardi, F.: Design and analysis of inexact floating-point adders.IEEE Trans. Comput.65, 308–314 (2016)

[17] Zhou, Z., Guin, U., Agrawal, V.D.: Modeling and test generation for combinational hardware Trojans. Proceedings of the IEEE VLSI TestSymposium (VTS), pp. 1–6 (2018)

[18] Green, K., and R. Vrba. "Research on Nano Antennas for Telecommunication and Optical Sensing." National Journal of Antennas and Propagation 6.2 (2024): 1-8.