M-HLS: Malevolent High Level Synthesis for Watermarked Hardware IPs

Published in IEEE Embedded Systems Letters

Anirban Sengupta, Aditya Anshul, Vishal Chourasia and Nitish Kumar, "M-HLS: Malevolent High-Level Synthesis for Watermarked Hardware IPs," in IEEE Embedded Systems Letters, vol. 16, no. 4, pp. 497-500, Dec. 2024

INTRODUCTION

- Reusable hardware intellectual properties (IPs) are an essential component in several electronic and multimedia systems and are commonly generated using HLS frameworks [1].
- HLS-generated watermarked designs may create security vulnerability, which an attacker can exploit to insert Trojan [4].
- A hardware Trojan is a malicious logic inserted into an IP design during its design or manufacturing process, which are designed to remain undetected until triggered by specific conditions..

[1] Y. Jin and Y. Makris, “Hardware trojan detection using path delay fingerprint,” *IEEE International Workshop on HOST*, 2008, pp. 51–57.
[4] A. Sengupta, S. Bhadauria and S.P. Mohanty, "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*,vol.36 (4), pp.655-668, 2017.

MOTIVATION AND THREAT MODEL

- The goal of this approach is to highlight how a malicious HLS framework is capable of inserting hardware Trojans during the Mux-based interconnect stage of watermarked IP design.
- The impact of a malicious HLS tool may be performance degradation or denial of service.
- More explicitly, the target of designing malevolent HLS tool is to create inferior IP components in the market.

TROJAN VULNERABILITY IN HLS-BASED WATERMARKED IPS

- The primary objective of hardware IP watermarking is to provide a detective countermeasure against IP piracy and false IP ownership claim
- Approaches [1], [2], [3] are examples of HLS-based watermarking for IP designs.
- After embedding secret security constraints in the register allocation phase of HLS, the multiplexer-based interconnect design may get altered and yield a free port (input pin of mux) that can be exploited with malicious intent by an attacker to insert Trojan.

[1] Y. Jin and Y. Makris, “Hardware trojan detection using path delay fingerprint,” *IEEE International Workshop on HOST*, 2008, pp. 51–57.
[2] A. Sengupta and D. Roy, "Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 118-124, April 2017.
[3] F. Koushanfar, I. Hong, and M. Potkonjak. 2005. Behavioral synthesis techniques for intellectual property protection, *ACM Trans. Des. Autom. Electron. Syst.*, 10, 523–545.

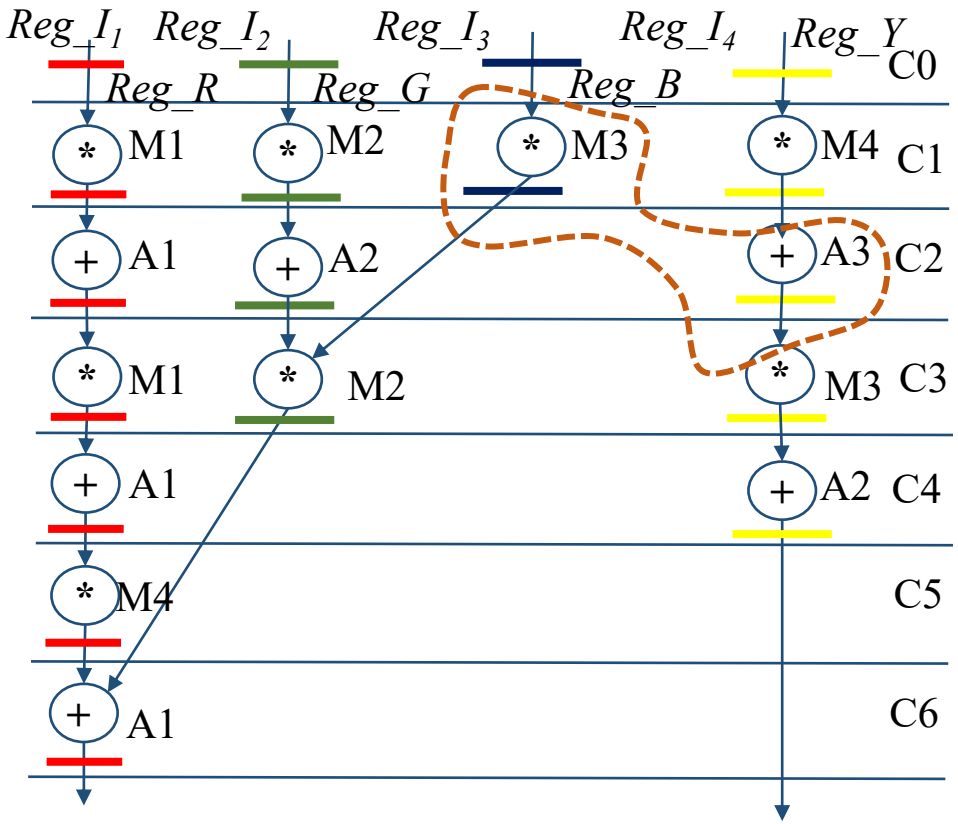

Fig. 1. Scheduled data flow graph of MESA Horner Bezier without watermark

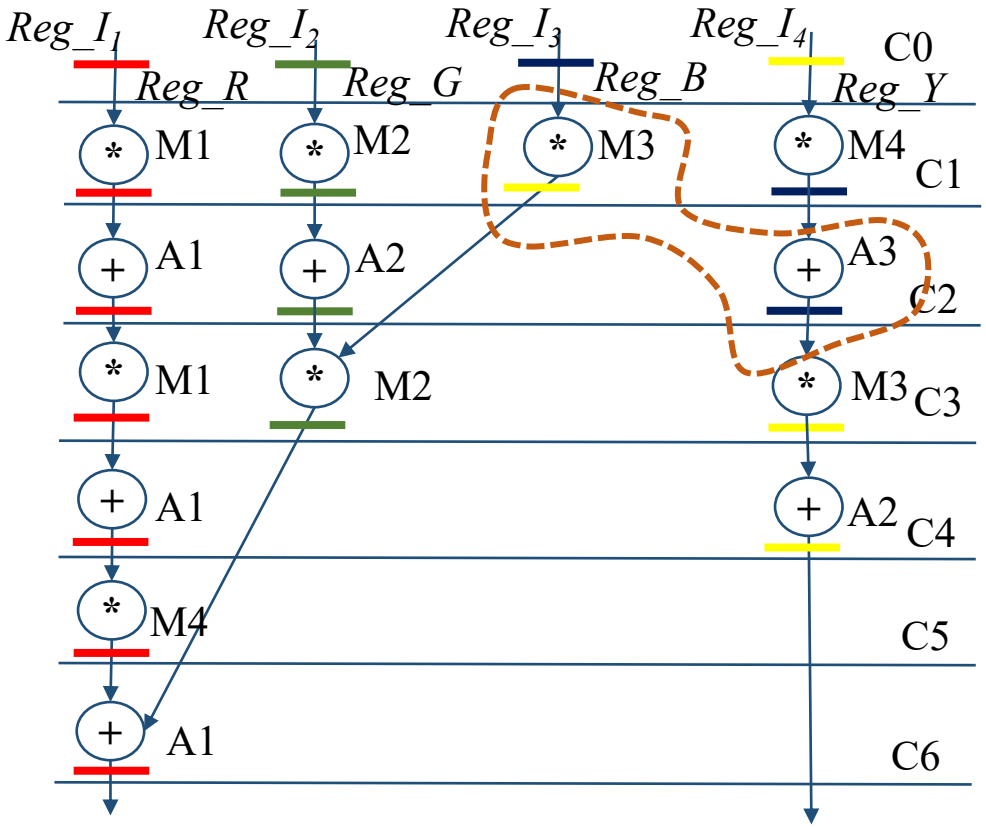

Fig. 2. Scheduled data flow graph of MESA Horner Bezier with embedded watermark

- Fig. 3 and 4 depict the mux-based interconnect design information of datapath without and with watermark in register (Reg_B) corresponding to Figures 1 and 2, respectively.

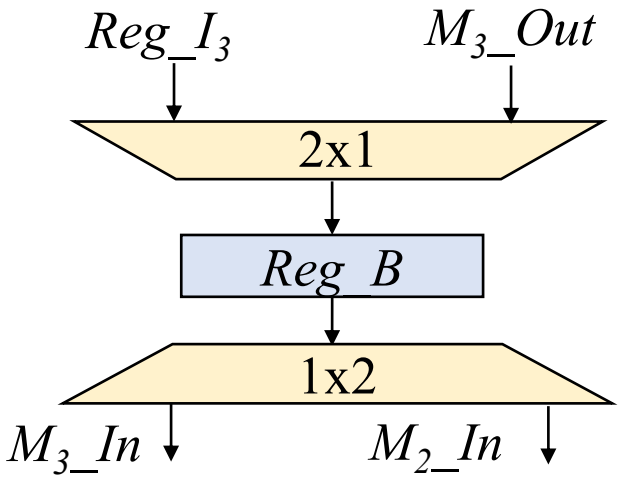

Fig. 3. Mux-based interconnect design of datapath without watermark in register *(Reg_B)* corresponding to Fig. 1

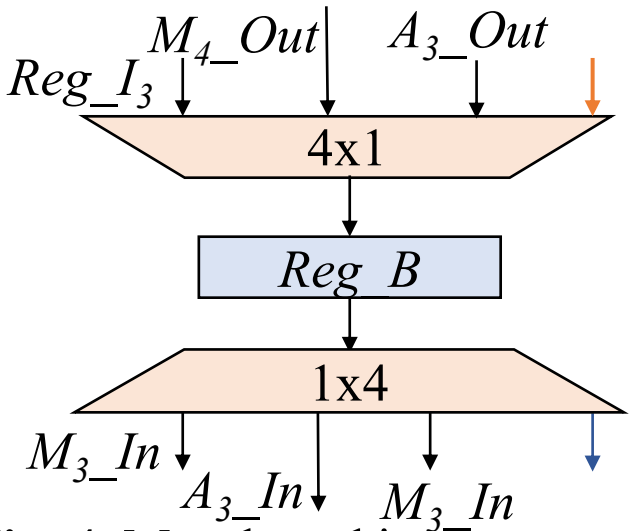

Fig. 4. Mux-based interconnect design of datapath post watermarking in *Reg_B* corresponding to Fig. 2

PROPOSED MALEVOLENT HLS FRAMEWORK

- Fig. 5 highlights the proposed malevolent high-level synthesis framework.

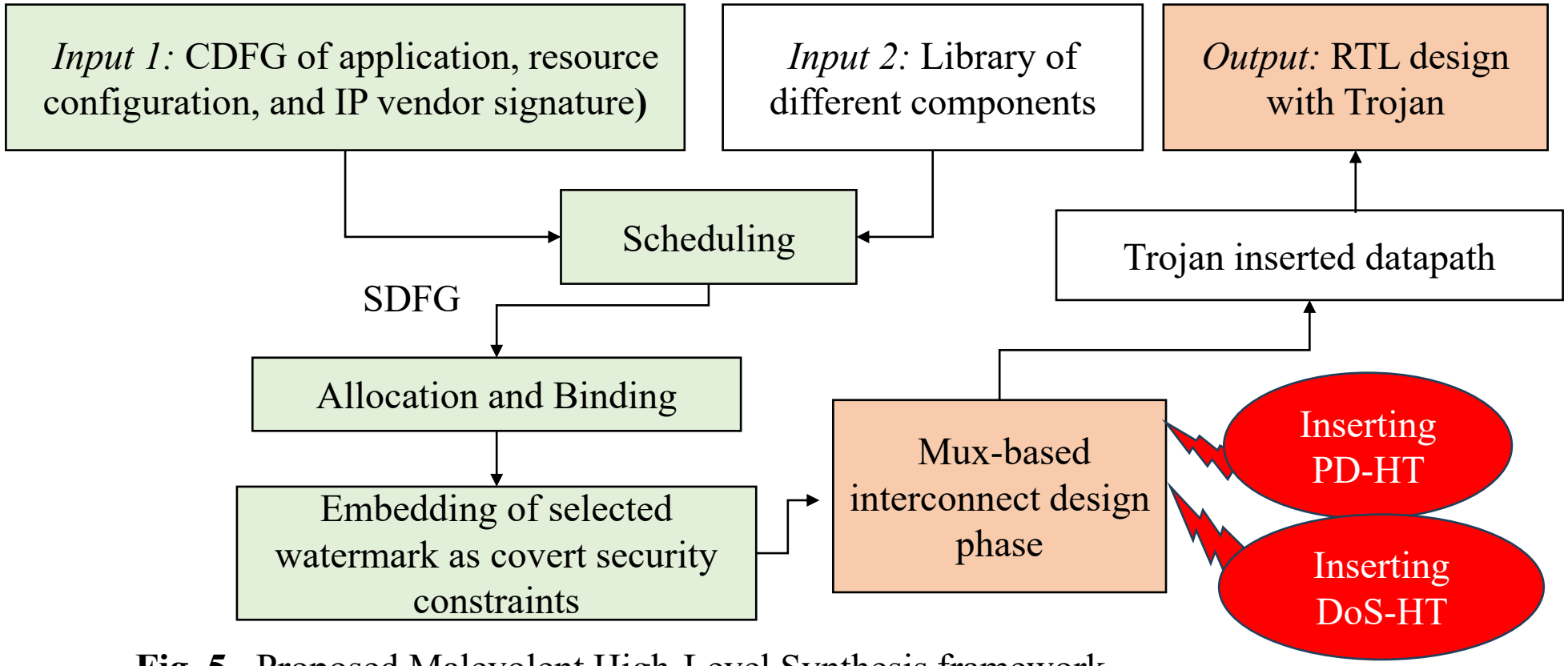

Fig. 5. Proposed Malevolent High-Level Synthesis framework

PROPOSED MALEVOLENT HLS FRAMEWORK

- The first type of proposed Trojan is performance degradation hardware Trojan (PD-HT).
- *Malicious modification and insertion*
- Next, the second type of proposed Trojan consists of denial-of-service (DoS) hardware Trojan (DoS-HT).
- *Open circuit condition/high impendence state/indeterministic state*

PROPOSED TROJAN DESIGNS INSERTED IN MUX-BASED INTERCONNECT DESIGN STAGE USING HLS

The proposed hardware Trojans automatically inserted in mux-based interconnect design information are shown in Figs. 6 and 7.

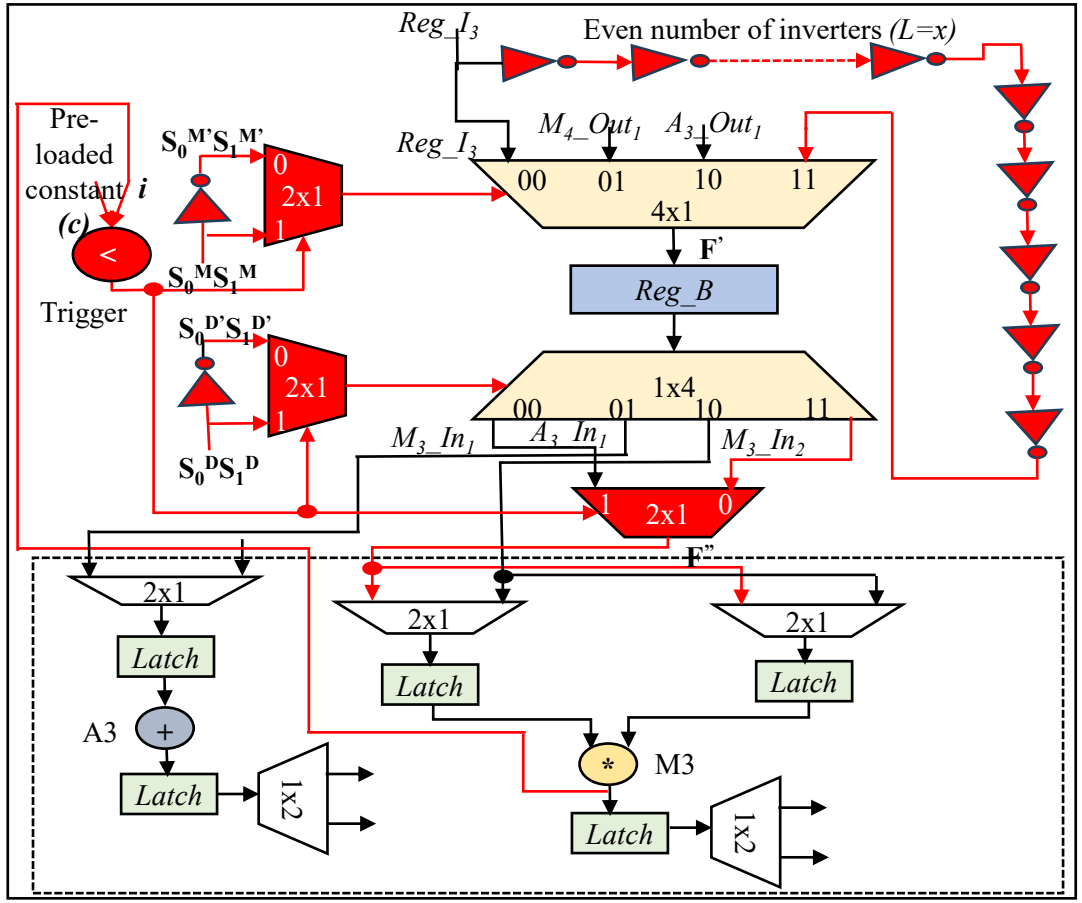

Fig. 6. Partial datapath of a watermarked MESA IP depicting insertion of PD-HT in the multiplexer of register (*Reg_B*)

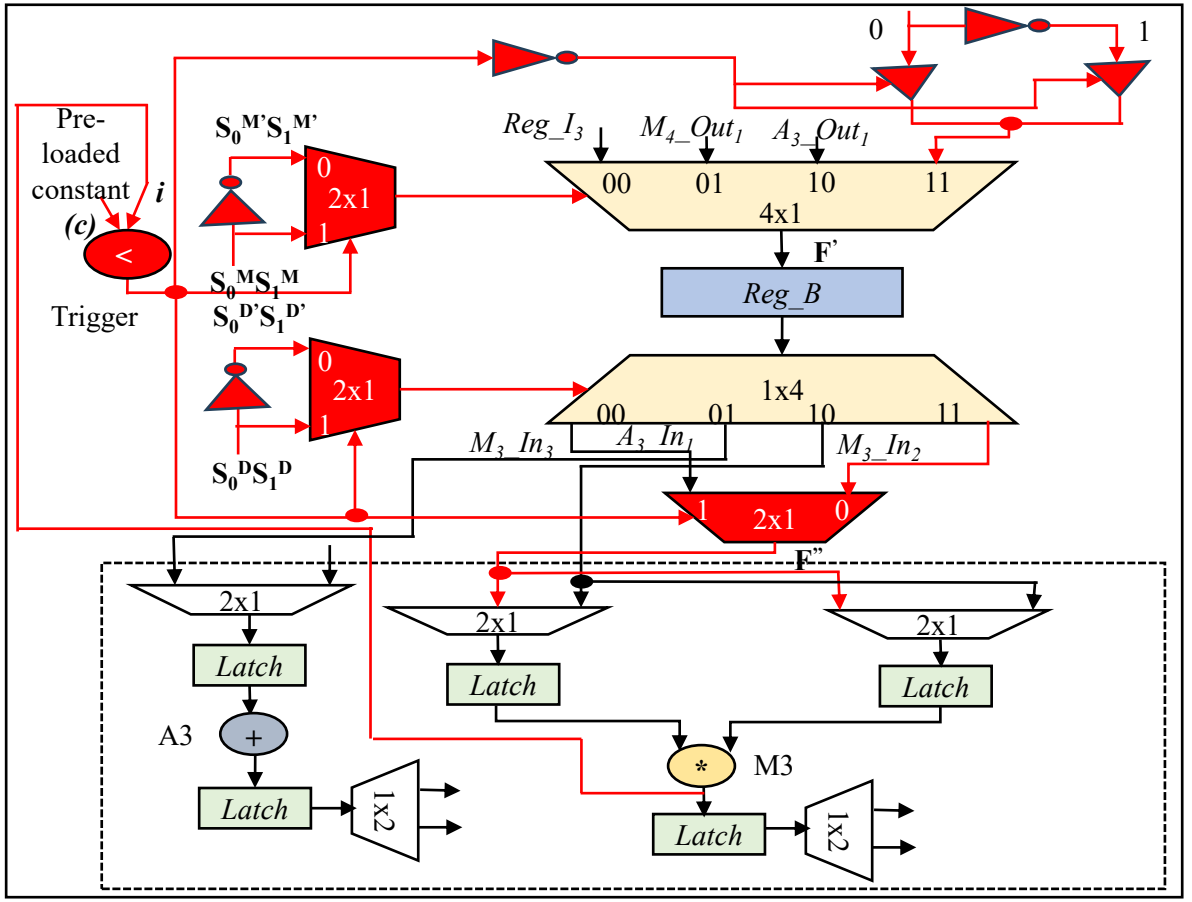

Fig. 7. Partial datapath of a watermarked MESA IP depicting insertion of DoS-HT in multiplexer register (*Reg_B*)

PROPOSED MALEVOLENT HLS FRAMEWORK

Table 1. Behavioral table (output) corresponding to mux of *Reg_b* in fig. 6

Trigger	Comparator o/p (Q)	So	S1	F	O/P
i=c (Trojan active)	0	0	0	Reg_I	Delayed O/P
i≠c (Trojan inactive)	1	0	0	Reg_I	Normal
	1	0	1	M4_Out	
	1	1	0	A3_Out	

Table 2. Behavioral table (output) corresponding to mux of *Reg_b* in fig. 7

Trigger	Comparator o/p (Q)	S0	S1	F	O/P
i=c (Trojan active)	0	0	0	Reg_I	Z(DoS)
i≠c (Trojan inactive)	1	0	0	Reg_I	Normal
	1	0	1	M4_Out	
	1	1	0	A3_Out	

RELATED WORK

Sr. No.	Existing Work	Technique Used	Remarks
1.	C. Pilato et. al., [7] (2019)	Malicious use of HLS tools can alter circuits	However, [7] shows the insertion of Trojans only in non-watermarked HLS-generated IPs.
2.	A. Sengupta et. al., [4] (2017)	functional Trojans in micro 3PIPs of the HLS tool library	However, [4] does not present performance degradation-based Trojan and denial of service-based Trojan.
3.	M. Abderehman et al., [8] (2022)	has assumed the availability of Trojan-infected RTL code (using the Bambu tool) for launching equivalence checking analysis	However, the Bambu tool does not provide Trojan-infected RTL codes for watermarked IP designs. [8] is not capable of detecting DoS-HT attack (like in the proposed approach), as it has shown to work for battery exhaustion and downgrade attacks only.

RESULTS AND ANALYSIS

Table 3. Area overhead due to insertion of different types of proposed HLS-aided hardware Trojan in watermarked Mesa IP design

Parameters	Base line IP Design	IP design with PD-HT	IP design with DoS-HT
Area (gate count)	7424	7622	7620
Area Overhead wrt. Baseline (gate count)	--	2.66 %	2.64 %

Table 4. Area overhead and performance degradation achieved for watermarked Mesa IP inserted with HLS-aided PD-HT with variation in attacker's selected number of inverters (x)

Parameters	X = 10	X = 16	X = 20	X = 24
Area Overhead)	2.74 %	2/83 %	2.88 %	2.94 %
Performance degradation	11.41 %	18.25 %	22.81 %	27.37 %

RESULTS AND ANALYSIS

Table 5. Power overhead due to insertion of proposed HLS-aided hardware Trojans in watermarked Mesa IP design

Parameters	Base line IP Design	IP design with PD-HT	IP design with DoS-HT
Power (µw)	64.81	66.85	66.85
Power overhead w.r.t. baseline	--	3.14 %	3.14 %

RESULTS AND ANALYSIS

Table 6. Area overhead comparison of the proposed malevolent hls trojans with [7]

Benchmark	Proposed M-HLS	[7]
FIR IP	Upto 1.89%	Upto 4%
Watermark MESA IP	Upto 2.65%	--

Table 6. Comparison of the proposed malevolent hls trojans with [7] in terms of performance degradation achieved

Benchmark	Proposed M-HLS	[7]
FIR IP	> 15 %	> 15 %
Watermark MESA IP	> 27 %	--

REFERENCE

[1] Y. Jin and Y. Makris, “Hardware trojan detection using path delay fingerprint,” *IEEE International Workshop on HOST*, 2008, pp. 51–57.

[2] A. Sengupta and D. Roy, "Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 118-124, April 2017.

[3] F. Koushanfar, I. Hong, and M. Potkonjak. 2005. Behavioral synthesis techniques for intellectual property protection, *ACM Trans. Des. Autom. Electron. Syst.*, 10, 523–545.

[4] A. Sengupta, S. Bhadauria and S.P. Mohanty, "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*,vol.36 (4), pp.655-668, 2017.

[5] University of California Santa Barbara Express Group, accessed on Feb. 2024. Available: *https://web.ece.ucsb.edu/EXPRESS /benchmark/*.

[6] CAD for Assurance, Crypto-Steganography Tool, accessed on Feb. 2024, IEEE CEDA and IEEE HSTTC, *https://cadforassurance.org/tools/ip-ic-protection/crypto-steganography-tool/*.

[7] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 4, pp. 913-926, April 2019.

REFERENCE

[8] M. Abderehman, R. Gupta, R. R. Theegala and C. Karfa, "BLAST: Belling the Black-Hat High-Level Synthesis Tool," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 41, no. 11, pp. 3661-3672, Nov. 2022.
[9] Huang, Y.W.; Bhunia, S.; Mishra, P. Scalable Test Generation for Trojan Detection Using Side Channel Analysis. *IEEE Trans. Inf. Forensics Secur.* 2018, 13, 2746–2760.
[10] M. Rathor and A. Sengupta, "Revisiting Black-Hat HLS: A Lightweight Countermeasure to HLS-Aided Trojan Attack," *IEEE Embedded Systems Letters*, Volume: 16, Issue: 2, 2024, pp. 170-173.
[11] R. Yasaei, L. Chen, S. -Y. Yu and M. A. A. Faruque, "Hardware Trojan Detection using Graph Neural Networks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2022.
[12] Open Cell NanGate Library, 15 nm open cell library, Available: https://si2.org/open-cell-library/, last accessed on Feb 2024.
[13] Dong, C., Xu, Y., Liu, X., Zhang, F., He, G., Chen, Y., 2020. Hardware Trojans in Chips: A Survey for Detection and Prevention. *Sensors* 20(18), 5165.
[14] A. Sengupta, D. Roy and S. P. Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection During Architecture Synthesis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 4, pp. 742-755, 2018.

Thank You!