Time-Bomb HLS Trojan for Performance Degradation Payload

***Authors**: Anirban Sengupta and Nabendu Bhui*

IEEE Design & Test, Accepted, 2025

Introduction

- High-level synthesis (HLS) plays a pivotal role in the design of hardware intellectual property (IP) designs, especially from the domain of image/video processing, multimedia etc.
- However, backdoor hardware Trojans (HT) can be inserted in the HLS design flow to compromise the produced register transfer level (RTL) IP design.
- This paper presents a novel time-bomb triggering HLS Trojan with significant performance degradation (PD) payload.

- **Novel Contributions of the Paper**:
  - (i) Presents a novel time-bomb triggered HLS Trojan that has capacity to incur performance degradation payload.
  - (ii) Presents a novel Trojan insertion strategy during the mux-based interconnect design stage of HLS process.
  - (iii) The proposed time-bomb HLS Trojan is capable to achieve significantly stronger performance degradation at lower area overhead, than prior-art [2].

[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.

Related Works

- There has been no prior work on HLS security that presented time-bomb PD-Trojan insertion technique, during HLS flow, by exploiting mux interconnects design stage.
  - In the literature, [1] has presented a functional Trojan secretly injected in the HLS tool library. It has also presented a detection mechanism for such functional Trojan using dual modular redundancy (DMR) based scheduling with distinct IP vendor policy.
  - In the literature, [2] has presented a battery exhaustion hardware Trojan and downgrade attack hardware Trojan that can potentially exhaust the power of the IP design and compromise the security of crypto-cores. Such Trojans were shown to be secretly inserted in the scheduling phase of HLS process.
  - Further, [1] [2] also did not present covert insertion Trojan technique by exploiting the mux-based interconnect design stage of HLS process, unlike the proposed HLS Trojan.
  - Moreover, [3] only presents a Trojan detection technique, but does not deal with Trojan insertion process. Authors in [3] have presented a C-to-RTL equivalence checking technique that is capable of detecting Trojan degradation attack (DA), battery exhaustion (BE) attack, and downgrade attack (DG) respectively.
  - Authors in [5] have proposed a high-level transformation (HLT) driven Trojan detection technique to detect battery exhaustion hardware Trojan. Detection technique [7] focusses on discerning nominal chips from Trojan-inserted chips based on generated path delay fingerprints.
  - Detection techniques such as [3], [5], and [7] are not adequately equipped to detect proposed HLS PD-hardware Trojan.

[1] 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 and Systems, Vol.36 (4), pp.655-668, 2017.
[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.
[3] 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, 2022.
[5] M. Rathor and A. Sengupta, "Revisiting Black-Hat HLS: A Lightweight Countermeasure to HLS-Aided Trojan Attack," IEEE Embedded Systems Letters, Volume: 16 (2), pp. 170-173, 2024.
[7] Y. Jin and Y. Makris “Hardware trojan detection using path delay fingerprint,” IEEE International Workshop on HOST, pp. 51–57, 2008

Proposed Methodology

➢ Threat Model and Motivation

- HLS Trojans exploits the automated characteristics of an HLS framework and poses critical security vulnerabilities. HLS generates RTL hardware architecture directly from its high-level specifications (C/C++/data flow graph), while also exposing potential attack vectors.
- Initially, HLS design processes may lead to hidden vulnerabilities, enabling the insertion of harmful hardware Trojans during IP design, which ultimately compromises the integrity of the produced IP or results in substandard IP components being available in the market.
- Secondly, Trojan inserted HLS frameworks may be included in the national-level attack toolkit/ingredient, where frameworks/tools created in one nation can be utilized in a different nation to design system-on-chips (SoCs). These HLS frameworks are quite unreliable and untrustworthy and could be compromised versions that might include backdoor Trojans without the awareness of the IP designers.
- A rogue HLS tool designer can have access to the mux-based interconnect design stage of the HLS flow, where he/she may insert backdoor Trojan during the HLS tool development process.
- Therefore, an adversary present in the HLS tool vendor house is capable of accessing the important design stages of the HLS process, where he/she can exploit this privilege to covertly insert trojan logic in the mux-based interconnect design stage.
- These vulnerable tools can contain secretly inserted Trojan (that is activated only under specific rare-event condition when attacker wishes) during important stages of HLS design flow.
- The HLS Trojans within the design process can lead to security vulnerabilities such as performance degradation, power exhaustion, data integrity etc. in the generated IP design .

Proposed Methodology (Contd.)

- Fig. 1(a) shows the insertion stage of the proposed time-bomb triggered Trojan during the HLS design process.
- For explanation and demonstration of the proposed HLS Trojan, we use an HLS generated convolution filter IP design (Fig. 1(b)).

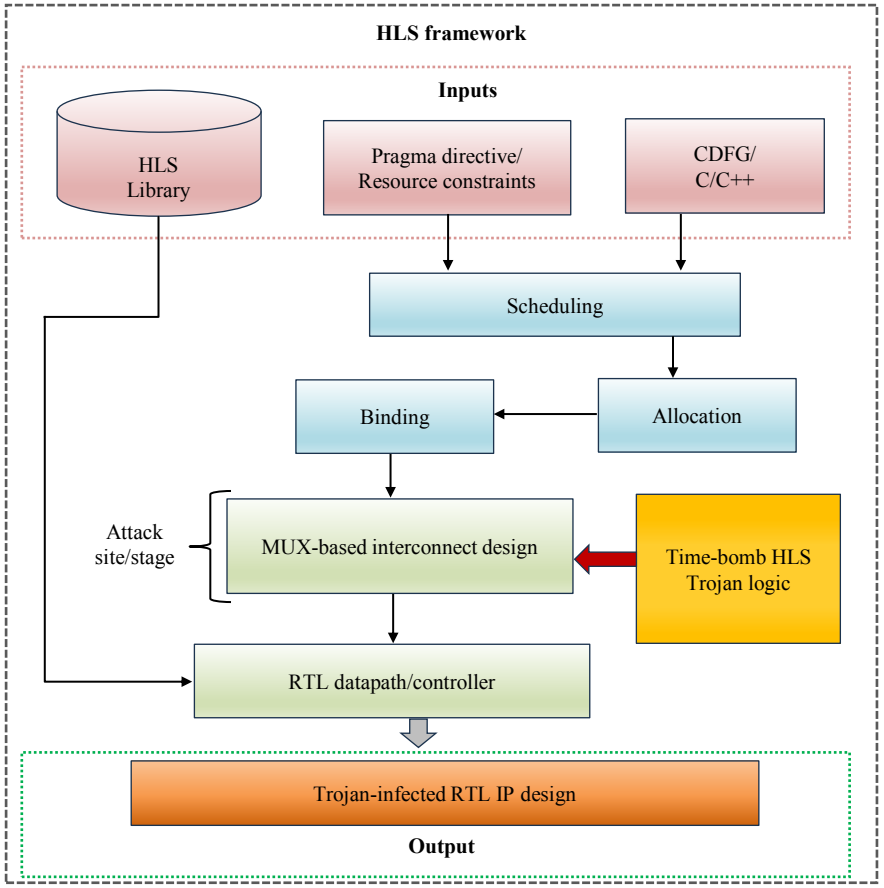

Fig. 1(a). Proposed Trojan insertion in the HLS design flow

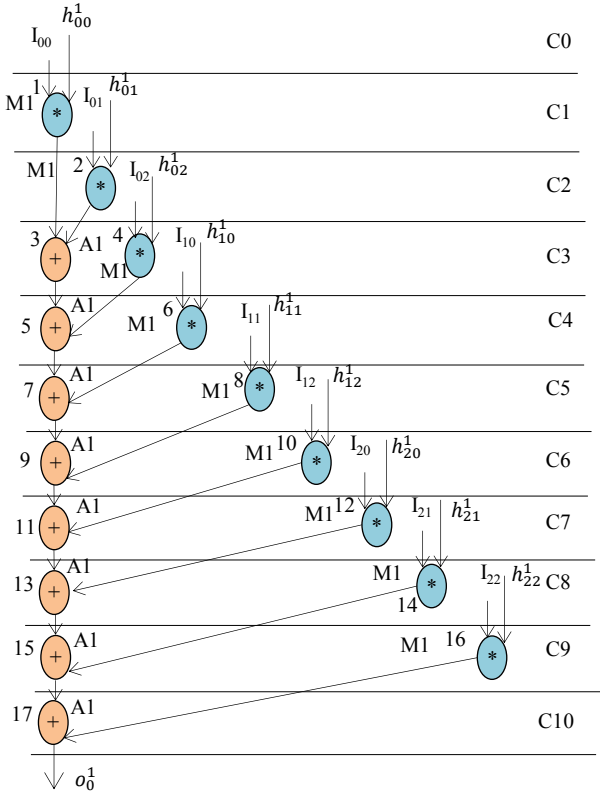

Fig. 1(b). Scheduled DFG of proposed convolutional layer IP core with kernel of size 3x3 based on 1M, 1A resources

Proposed Methodology (Contd.)

➢ **Overview of the Proposed Trojan Insertion**

- The paper presents novel time-bomb triggering driven performance degradation hardware Trojan (PD-HT) that an attacker can secretly implant by exploiting a free (vacant) input port in the mux-based interconnect design of HLS process.
- During the mux-based interconnect design of HLS, appropriate number and type of multiplexer (mux) units are determined and generated.
- In almost all IP datapath designs, the generated muxes have at least a single free (vacant) port, which can be easily exploited by an attacker to covertly inject Trojan.
- The proposed PD-HT refers to a malicious alteration within the IP design that achieves performance degradation payload under a specific rare-event time-duration based triggering condition.
- The proposed HLS Trojan exploits a time-bomb based trigger which indicates that the Trojan logic only gets activated (by an attacker) when a pre-defined time interval has elapsed.
- The proposed time-bomb Trojan trigger is designed in such a way that the activation only occurs when the modulus up-counter reaches the same state value as pre-defined in the in-built memory (or register).
- Since the proposed HLS Trojan is only activated under a specific rare-event and it only affects the performance, hence it is very challenging to identify this Trojan.

- Fig. 1(a) shows the insertion stage of the proposed time-bomb triggered Trojan during the HLS design process.

Proposed Methodology (Contd.)

➢ Details of the Proposed Trojan Insertion

- Fig. 1(c) shows the proposed performance (delay) degradation hardware Trojan inserted into the convolutional filter IP datapath design, during the mux-based interconnect design stage of HLS process.
- In Fig. 1(c), the red colored components or logic indicates the proposed performance (delay) degradation hardware Trojan logic, while the other components or logic are part of the regular IP datapath design of convolutional filter.
- More is the Tri-State buffer (TSB) chain length, greater is the performance degradation payload achieved by an attacker. The non-red color components are the regular units of convolutional filter IP datapath design.
- The behavioral table of the proposed time-bomb HLS Trojan with its trigger possibilities, triggering conditions and relevant outputs is described in the next slide.

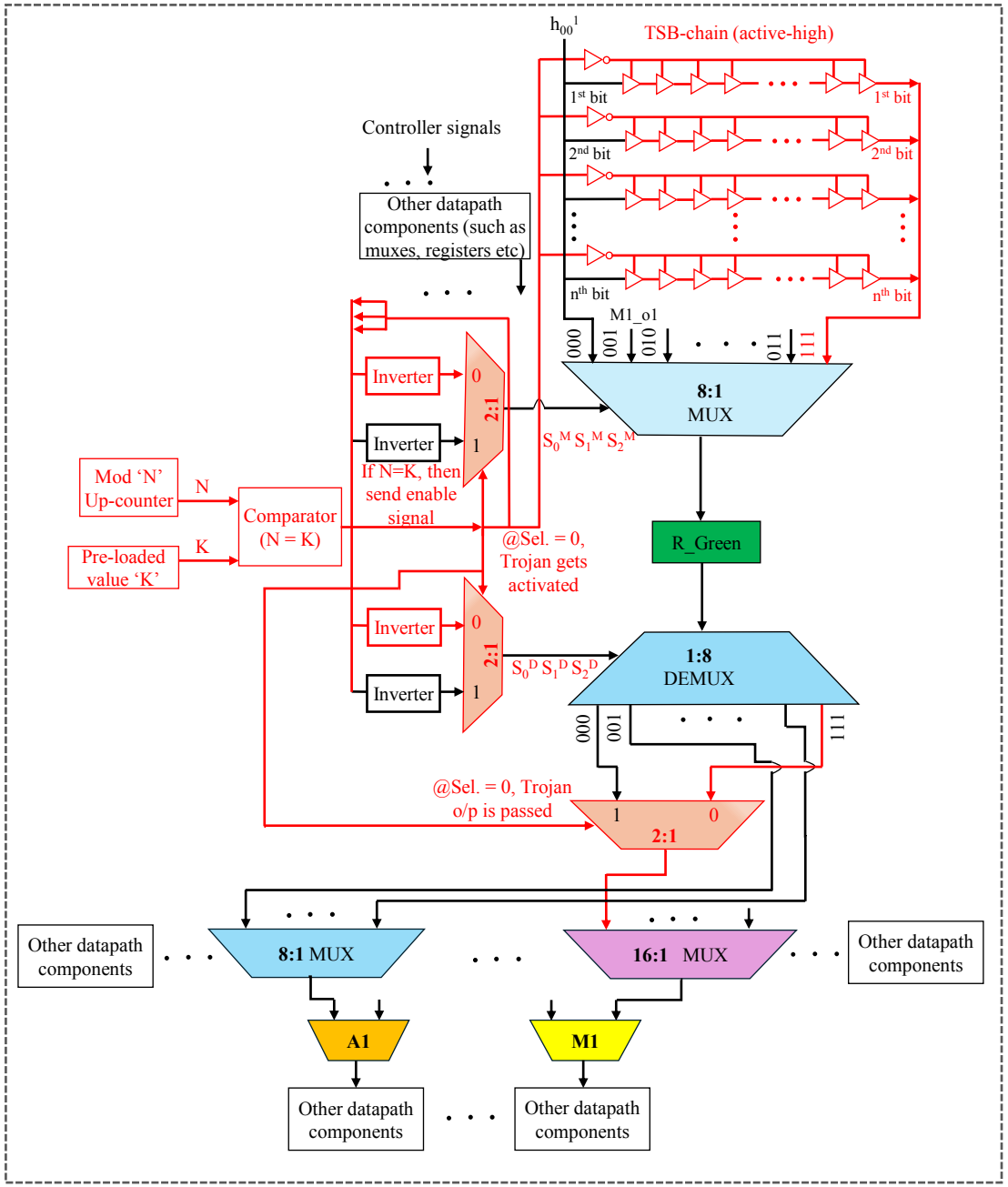

Fig. 1(c). HLS based time-bomb Trojan inserted convolution filter IP datapath design – partial view

Proposed Methodology (Contd.)

Table 1 presents the behavioral description of the proposed time-bomb HLS Trojan with its trigger possibilities, triggering conditions and relevant outputs. The behavioral table indicates the following:

(a) Possibilities

(b) Rare-event trigger condition

(c) Comparator output internal signal

(d) Select lines values $S_0^M S_1^M S_2^M$ of the 8:1 multiplexer

(e) Select lines values $S_0^D S_1^D S_2^D$ of the 1:8 demultiplexer

(f) On specified rare-event triggering, value of '000' is automatically fed into input of 2:1 muxes for ensuring $S_0^M S_1^M S_2^M = S_0^D S_1^D S_2^D = 111$, to generate Trojan o/p (performance degradation payload). Rest of the time, the IP datapath design operates normally (Trojan free) due to no trigger.

(g) Final output

TABLE 1

BEHAVIORAL TABLE CORRESPONDING TO THE PROPOSED TIME-BOMB HLS TROJAN

Possibilities	Trigger condition	Comparator o/p internal signal	$S_0^M S_1^M S_2^M$ select internal signal line for 8:1 MUX	$S_0^D S_1^D S_2^D$ select internal signal line for 1:8 DEMUX	O/P
Trojan active	N = K	0	$S_0^M S_1^M S_2^M = 111$	$S_0^D S_1^D S_2^D = 111$	Delayed of h_{00}^1
Trojan inactive	N ≠ K	1	$S_0^M S_1^M S_2^M \neq 111$	$S_0^D S_1^D S_2^D \neq 111$	Normal

Results and Analysis

The proposed HLS Trojan infected IP designs has been evaluated in terms of the following:

(a) achieved performance degradation from an attacker's perspective, (b) area overhead of the HLS Trojan logic in the context of the target IP designs, (c) area overhead of the HLS Trojan logic in the context of the target IP designs, and (d) comparison of the proposed HLS Trojan with similar prior art [2], in terms of performance degradation achieved and its respective area overhead.

TABLE 2A

PERFORMANCE DEGRADATION DUE TO INSERTION OF PROPOSED TIME-BOMB HLS TROJAN IN DIFFERENT IP DESIGNS WITH VARIATION IN ATTACKER'S SELECTED TSB CHAIN LENGTH (L)

IP design	Parameters	Baseline IP design	IP design with PD-HT (L = 6)	IP design with PD-HT (L = 8)	IP design with PD-HT (L = 10)
Convolutional filter [4]	Delay (ps)	2450.98	2866.55	2889.21	2911.87
	Performance degradation w.r.t. baseline (delay)	--	16.9%	17.9%	18.8%
Sharpening filter [9]	Delay (ps)	794.91	1210.48	1233.14	1255.80
	Performance degradation w.r.t. baseline (delay)	--	52.3%	55.1%	57.9%
JPEG-DCT [11]	Delay (ps)	927.40	1342.96	1365.62	1388.28
	Performance degradation w.r.t. baseline (delay)	--	44.81%	47.25%	~50%
Cardiac Pacemaker [12]	Delay (ps)	2517.23	2932.79	2955.45	2978.11
	Performance degradation w.r.t. baseline (delay)	--	~17%	17.41%	18.31%
ECG detector GLRT [12]	Delay (ps)	1656.07	2071.63	2094.29	2116.95
	Performance degradation w.r.t. baseline (delay)	--	25.09%	26.46%	27.83%

[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.
[4] A Sengupta, R. Chaurasia "Secured Convolutional Layer IP Core in Convolutional Neural Network using Facial Biometric", IEEE Transactions on Consumer Electronics, Volume: 68 (3), pp. 291-306, 2022.
[9] A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", Elsevier Microprocessors and Microsystems, Volume 103, 104973, 2023.
[11] A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran, "Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware," IEEE Transactions on Consumer Electronics, vol. 64 (3), pp. 365-374, 2018.
[12] A Sengupta, R Chaurasia "Secure Implantable Cardiac Pacemaker for Medical Consumer Electronics", Nature - npj Biomedical Innovations 2, Article number: 5, Feb 2025.

Results and Analysis (Contd.)

TABLE 2B
AREA OVERHEAD DUE TO INSERTION OF PROPOSED TIME-BOMB HLS TROJAN IN DIFFERENT IP DESIGNS WITH VARIATION IN ATTACKER'S SELECTED TSB CHAIN LENGTH (L)

IP design	Parameters	Baseline IP design	IP design with PD-HT (L = 6)	IP design with PD-HT (L = 8)	IP design with PD-HT (L = 10)
Convolutional filter	Area (gate count)	10448	10678	10710	10742
	Area overhead w.r.t. baseline (gate count)	--	2.2%	2.5%	2.8%
Sharpening filter	Area (gate count)	7264	7494	7526	7558
	Area overhead w.r.t. baseline (gate count)	--	3.2%	3.6%	4.0%
JPEG-DCT	Area (gate count)	8832	9062	9094	9126
	Area overhead w.r.t. baseline (gate count)	--	2.60%	2.97%	3.33%
Cardiac Pacemaker	Area (gate count)	16096	16326	16358	16390
	Area overhead w.r.t. baseline (gate count)	--	1.43%	1.63%	1.83%
ECG detector GLRT	Area (gate count)	11744	11974	12006	12038
	Area overhead w.r.t. baseline (gate count)	--	1.96%	2.23%	2.50%

Results and Analysis (Contd.)

TABLE 2C
POWER OVERHEAD DUE TO INSERTION OF PROPOSED TIME-BOMB HLS TROJAN IN DIFFERENT IP DESIGNS WITH VARIATION IN ATTACKER'S SELECTED TSB CHAIN LENGTH (L)

IP design	Parameters	Baseline IP design	IP design with PD-HT (L = 6)	IP design with PD-HT (L = 8)	IP design with PD-HT (L = 10)
Convolutional filter	Power (µw)	78.72	81.17	81.42	81.67
	Power overhead w.r.t. baseline	--	3.1%	3.4%	3.7%
Sharpening filter	Power (µw)	63.16	65.61	65.86	66.10
	Power overhead w.r.t. baseline	--	3.9%	4.3%	4.7%
JPEG-DCT	Power (µw)	65.70	68.16	68.40	68.65
	Power overhead w.r.t. baseline	--	3.73%	4.11%	4.48%
Cardiac Pacemaker	Power (µw)	130.38	132.83	133.07	133.32
	Power overhead w.r.t. baseline	--	1.88%	2.07%	2.26%
ECG detector GLRT	Power (µw)	87.82	90.27	90.51	90.76
	Power overhead w.r.t. baseline	--	2.79%	3.07%	3.35%

Results and Analysis (Contd.)

TABLE 3A
PERFORMANCE DEGRADATION COMPARISON OF THE PROPOSED TIME-BOMB HLS TROJAN WITH [2]

IP design	Proposed time-bomb HLS	[2]
Convolutional filter	up to 19%	up to 17%
Sharpening filter	up to 58%	
JPEG-DCT	up to 50%	
Cardiac Pacemaker	up to 18%	
ECG detector GLRT	up to 28%	

TABLE 3B
AREA OVERHEAD COMPARISON OF THE PROPOSED TIME-BOMB HLS TROJAN WITH [2]

IP design	Proposed time-bomb HLS	[2]
Convolutional filter	upto 2.8 %	upto 4%
Sharpening filter	upto 4.0 %	
JPEG-DCT	up to 3.3%	
Cardiac Pacemaker	up to 1.8%	
ECG detector GLRT	up to 2.5%	

[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.

Results and Analysis (Contd.)

TABLE 4A

DEMONSTRATION OF TROJAN EVASION FOR KNOWN DETECTION TECHNIQUES

*(**Note**: HLT - High-Level Transformations from [5], DMR – Dual Modular Redundancy from [1], TMR – Triple Modular Redundancy from [9])*

Detection approach	Proposed Trojan status	Remarks
HLT based detection [5]	Not detected	HLT based detection technique is only able to handle fake operations as trojans (therefore is able to detect only HLS based battery exhaustion trojan attacks)
TL-HLS [1]	Not detected	TL-HLS detection technique with DMR design is only able to handle HLS functional trojan (unable to detect trojan with performance degradation payload)
Trojan resistance [9]	Not detected	Trojan resistance technique with TMR design is only able to handle HLS functional trojan (unable to detect trojan with performance degradation payload)
GNN [10]	Not detected	GNN based detection technique uses Pyverilog that is incapable to handle VHDL codes/ RTL circuits as well as generates weaker learning behaviour for complex IP designs
C to RTL Equivalence checking [3]	Not detected	As this equivalence checking relies on creation of finite state machine with datapath (RTL) for comparing with C code, hence it is only capable to detect battery exhaustion-based HLS trojan and downgrade attack HLS trojan
Detection using path delay fingerprint [7]	Not detected	Path delay fingerprint-based detection technique is incapable to detect trojans in complex HLS generated IP designs

[1] 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 and Systems, Vol.36 (4), pp.655-668, 2017
[3] 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, 2022.
[5] M. Rathor and A. Sengupta, "Revisiting Black-Hat HLS: A Lightweight Countermeasure to HLS-Aided Trojan Attack," IEEE Embedded Systems Letters, Volume: 16 (2), pp. 170-173, 2024.
[7] Y. Jin and Y. Makris "Hardware trojan detection using path delay fingerprint," IEEE International Workshop on HOST, pp. 51–57, 2008
[9] A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", Elsevier Microprocessors and Microsystems, Volume 103, 104973, 2023.
[10] R. Yasaei, L. Chen, S. -Y. Yu and M. Abdullah Al Faruque, "Hardware Trojan Detection Using Graph Neural Networks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 44 (1), pp. 25-38, 2024.

Results and Analysis (Contd.)

TABLE 4B

DEMONSTRATION OF PROPOSED TROJAN EVASION FOR KNOWN DETECTION TECHNIQUES

*(**Note**: U^{OG}, U^{DP} and U^{TP} indicate original, duplicate, and triplicate units from [1] and [9]; HLT: High-Level Transformations from [5])*

Detection approach	Features in proposed IP (baseline) - Design A	Features in proposed IP (with Trojan) – Design B	Features in proposed IP (baseline) – Design C	Justification of evasion	Trojan Status
TL-HLS [1]	# of distinct 3PIP vendor: 1 (U^{OG}: 20 opn. allocations for sharpening filter) (U^{OG}: 17 opn. allocations for convolution filter)	# of distinct 3PIP vendor: 1 (U^{DP}: 20 opn. allocations for sharpening filter) (U^{DP}: 17 opn. allocations for convolution filter)	Not applicable	Difference in functional o/p between designs A & B using comparator: Nil	Not detected
HLS based detection [5]	Opn. count (sharpening filter): 20 (convolution filter): 17 HLT: 0	Opn. count (sharpening filter): 20 (convolution filter): 17 HLT: 0	Not applicable	Difference in opn. count between designs A & B: Nil	Not detected
GNN based detection [10]	> 1000 lines of VHDL code for convolution filter processor (datapath & controller) IP	> 1000 lines of VHDL for convolution filter processor (datapath & controller) IP	Not applicable	Incapable of handling VHDL using *Pyverilog* | weaker learning	Not detected
TMR based resistance technique [9]	U^{OG}: allocated to 3PIP vendor 1 U^{OG} o/p = 9	U^{DP}: allocated to 3PIP vendor 2 U^{DP} o/p = 9	U^{TP}: allocated to 3PIP vendor 3 U^{TP} o/p = 9	Difference in functional o/p between designs A,B & C using comparator: Nil	Not detected
	Sample test vectors for U^{OG}, U^{DP} and U^{TP} : {I1,…I18} = (1,…,1)				
Functional RTL simulation/validation for Trojan detection [8]	Baseline design output = 9 (Note: a sample value is reported based on a specific test pattern provided. Large exhaustive set of test patterns were tested)	Trojan infected design output = 9 (Note: a sample value is reported based on a specific test pattern provided. Large exhaustive set of test patterns were tested)	Not applicable	Difference in functional o/p between designs A & B: Nil	Not detected

[1] 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 and Systems, Vol.36 (4), pp.655-668, 2017.
[5] M. Rathor and A. Sengupta, "Revisiting Black-Hat HLS: A Lightweight Countermeasure to HLS-Aided Trojan Attack," IEEE Embedded Systems Letters, Volume: 16 (2), pp. 170-173, 2024.
[8] Intel Quartus Tool, https://www.intel.com/content/www/us/en/software-kit/666221/intel-quartus-ii-web-edition-design-software-version-13-1-for-windows.html, last accessed on April 2025.
[9] A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", Elsevier Microprocessors and Microsystems, Volume 103, 104973, 2023.
[10] R. Yasaei, L. Chen, S. -Y. Yu and M. Abdullah Al Faruque, "Hardware Trojan Detection Using Graph Neural Networks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 44 (1), pp. 25-38, 2024.

Conclusion

- This paper presented a novel time-bomb triggered HLS Trojan attack technique that can use significant higher performance degradation for IP designs, at lesser design area overhead, than prior work [2].

- The proposed attack technique is stealthy and cannot be detected through state-of-the-art detection techniques.

- The proposed Trojan attack has capacity to be covertly injected in the mux-based interconnect design stage of HLS process.

[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, “Black-Hat High-Level Synthesis: Myth or Reality?,” IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.

References

[1] 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 and Systems, Vol.36 (4), pp.655-668, 2017

[2] C. Pilato, K. Basu, F. Regazzoni and R. Karri, "Black-Hat High-Level Synthesis: Myth or Reality?," IEEE Transactions on VLSI Systems, vol. 27 (4), pp. 913-926, 2019.

[3] 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, 2022.

[4] A Sengupta, R. Chaurasia "Secured Convolutional Layer IP Core in Convolutional Neural Network using Facial Biometric", IEEE Transactions on Consumer Electronics, Volume: 68 (3), pp. 291-306, 2022.

[5] M. Rathor and A. Sengupta, "Revisiting Black-Hat HLS: A Lightweight Countermeasure to HLS-Aided Trojan Attack," IEEE Embedded Systems Letters, Volume: 16 (2), pp. 170-173, 2024.

[6] A. Sengupta, A. Anshul, V. Chourasia and N. Kumar, "M-HLS: Malevolent High-Level Synthesis for Watermarked Hardware IPs," IEEE Embedded Systems Letters, vol. 16 (4), pp. 497-500, Dec. 2024.

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

[8] Intel Quartus Tool, https://www.intel.com/content/www/us/en/software-kit/666221/intel-quartus-ii-web-edition-design-software-version-13-1-for-windows.html, last accessed on April 2025.

[9] A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", Elsevier Microprocessors and Microsystems, Volume 103, 104973, 2023.

[10] R. Yasaei, L. Chen, S. -Y. Yu and M. Abdullah Al Faruque, "Hardware Trojan Detection Using Graph Neural Networks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 44 (1), pp. 25-38, 2024.

[11] A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran, "Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware," IEEE Transactions on Consumer Electronics, vol. 64 (3), pp. 365-374, 2018.

[12] A Sengupta, R Chaurasia "Secure Implantable Cardiac Pacemaker for Medical Consumer Electronics", Nature - npj Biomedical Innovations 2, Article number: 5, Feb 2025.

Thank You !!!