Poster: HIPR: Hardware IP Protection through Low-Overhead Fine-Grain Redaction

Aritra Dasgupta, Sudipta Paria, Swarup Bhunia
University of Florida, Gainesville, FL 32611, USA
aritradasgupta@ufl.edu, sudiptaparia@ufl.edu, swarup@ece.ufl.edu

Abstract

Hardware intellectual property (IP) blocks have been subjected to various forms of confidentiality and integrity attacks in recent years due to the globalization of the semiconductor industry. System-on-chip (SoC) designers are now considering a zero-trust model for security, where an IP can be attacked at any stage of the manufacturing process for piracy, cloning, overproduction, or malicious alterations. Hardware redaction has emerged as a promising countermeasure to thwart confidentiality and integrity attacks by untrusted entities in the globally distributed supply chain. However, existing redaction techniques provide this security at high overhead costs, making them unsuitable for real-world implementation. In this paper, we propose **HIPR**, a fine-grain redaction methodology that is robust, scalable, and incurs significantly lower overhead compared to existing redaction techniques. **HIPR** redacts security-critical Boolean and sequential logic from the hardware design, performs interconnect randomization, and employs multiple overhead optimization steps to reduce overhead costs. We evaluate **HIPR** on open-source benchmarks and reduce area overheads by 1 to 2 orders of magnitude compared to state-of-the-art redaction techniques without compromising security. We also demonstrate that the redaction performed by **HIPR** is resilient against conventional functional and structural attacks on hardware IPs. The redacted test IPs used to evaluate **HIPR** are available at: https://github.com/UF-Nelms-IoT-Git-Projects/HIPR.

I. Introduction

DOI: https://doi.org/10.46586/tches.v2025.i3.781-805.

Full reference (IEEE format) to our paper [1] accepted in TCHES Volume 2025 Issue 3: A. Dasgupta, S. Paria, and S. Bhunia, "HIPR: Hardware IP Protection through Low-Overhead Fine-Grain Redaction", TCHES, vol. 2025, no. 3, pp. 781–805, Jun. 2025, doi: 10.46586/tches.v2025.i3.781-805.

GitHub Repository with Artifacts: https://github.com/UF-Nelms-IoT-Git-Projects/HIPR.

Acknowledgment

The authors would like to thank Mr. David Kehlet and Mr. Nij Dorairaj, from Intel Corporation, for their valuable inputs on the **HIPR** approach and its evaluation.

References

[1] A. Dasgupta, S. Paria, and S. Bhunia, "HIPR: Hardware IP Protection through Low-Overhead Fine-Grain Redaction," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2025, no. 3, p. 781–805, Jun. 2025.

HIPR: Hardware IP Protection through Low-Overhead Fine-Grain Redaction

Aritra Dasgupta, Sudipta Paria, and Swarup Bhunia
Department of Electrical and Computer Engineering,
University of Florida, Gainesville, FL 32611

TCHES Article DOI

GitHub Artifacts

NELMS IoT

Background and Motivation

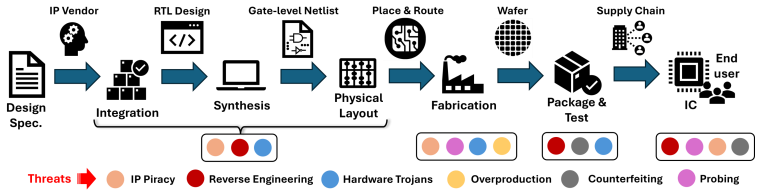
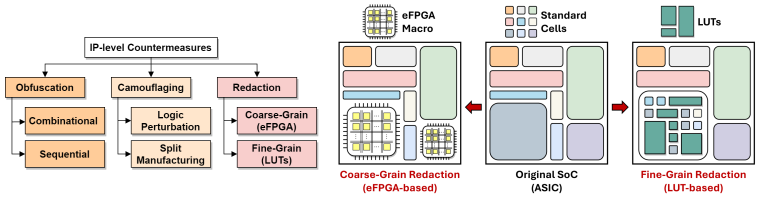


Fig. 1: Various threats to IP confidentiality and integrity encountered in the IC design flow.



(a) Taxonomy of countermeasures. (b) Hardware IP Redaction techniques.

Fig. 2: Overview of Anti-RE solution landscape.

Hardware IP Redaction Methodology

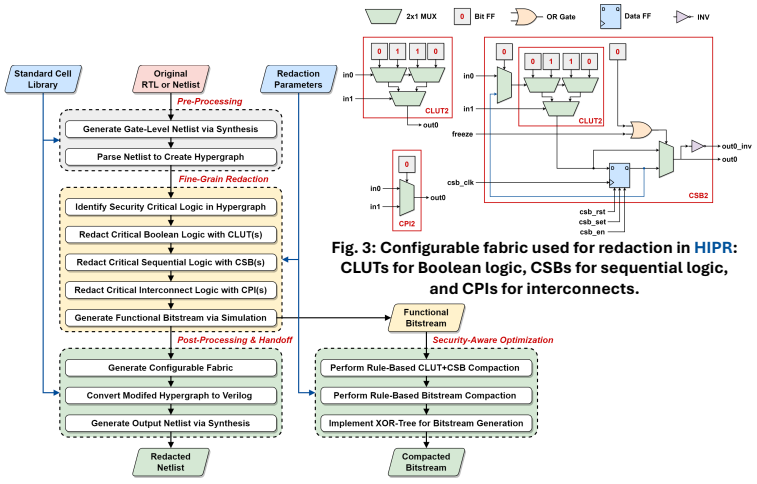


Fig. 3: Configurable fabric used for redaction in HIPR: CLUTs for Boolean logic, CSBs for sequential logic, and CPIs for interconnects.

Fig. 4: Major stages during fine-grain redaction in HIPR [5].

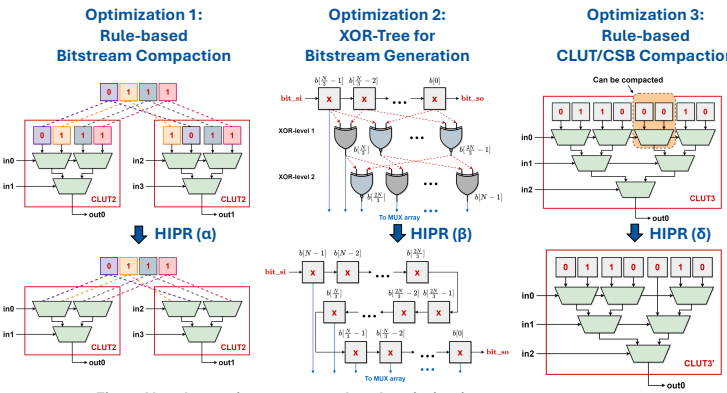


Fig. 5: Novel security-aware overhead optimizations employed in HIPR [5].

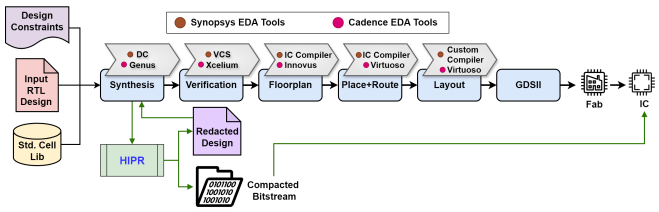


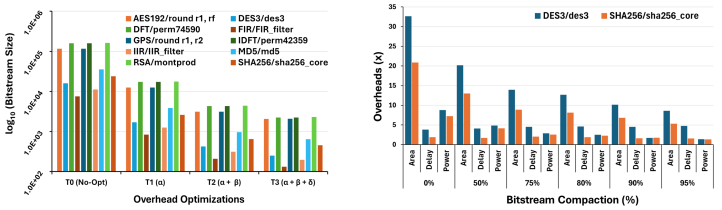
Fig. 6: Integrating HIPR into the commercial EDA tool flow for ASICs.

Overhead Results

Table 1: Overhead results for MIT-CEP benchmarks redacted using HIPR.

Benchmark	Full Chip Area* (μm^2)	Test IP‡	% Redacted by Area*	Original $\{\mathcal{A},\mathcal{D},\mathcal{P}\}$†	T1 (α) $\{\mathcal{A},\mathcal{D},\mathcal{P}\}$	T2 ($\alpha+\beta$) $\{\mathcal{A},\mathcal{D},\mathcal{P}\}$	T3 ($\alpha+\beta+\delta$) $\{\mathcal{A},\mathcal{D},\mathcal{P}\}$
AES192	68400.6	RD_1 : round r1, rf	10.6%	7270.6, 86.8, 2.0	8.0x, 5.2x, 3.1x	7.0x, 4.8x, 6.8x	4.9x, 3.6x, 4.6x
DES3	821.7	RD_2 : des3	100.0%	821.7, 165.5, 0.6	10.1x, 4.5x, 1.7x	8.8x, 4.6x, 7.5x	6.1x, 4.5x, 5.7x
DFT	82036.3	RD_3 : perm74590	20.9%	17141.6, 369.2, 8.7	5.1x, 1.8x, 1.8x	4.5x, 1.4x, 5.0x	2.9x, 1.6x, 3.4x
FIR	1127.5	RD_4 : FIR_filter	100.0%	1127.5, 396.7, 0.7	4.1x, 1.6x, 1.5x	3.7x, 1.7x, 2.9x	2.9x, 2.3x, 2.6x
GPS	69101.8	RD_5 : round r1, r2	14.1%	9721.9, 86.8, 3.1	6.1x, 4.4x, 2.0x	5.3x, 5.5x, 5.1x	3.8x, 3.5x, 3.6x
IDFT	81763.7	RD_6 : perm42350	21.0%	17141.6, 369.2, 8.7	5.1x, 1.8x, 1.8x	4.5x, 1.4x, 5.0x	2.9x, 1.6x, 3.4x
IIR	1738.6	RD_7 : IIR_filter	100.0%	1738.6, 462.6, 1.1	4.0x, 1.5x, 1.3x	3.5x, 1.8x, 2.8x	2.8x, 1.9x, 2.7x
MD5	2696.5	RD_8 : md5	100.0%	2696.5, 1016.0, 0.7	6.8x, 1.6x, 3.0x	5.9x, 1.7x, 10.4x	4.3x, 1.8x, 8.6x
RSA	130004.2	RD_9 : montprod	13.1%	16985.4, 541.6, 8.7	5.3x, 2.5x, 1.7x	4.6x, 2.4x, 5.0x	3.0x, 1.8x, 2.9x
SHA256	3194.4	RD_{10} : sha256_core	56.8%	1814.6, 341.5, 1.0	6.8x, 1.6x, 1.7x	5.9x, 1.8x, 5.6x	4.6x, 1.9x, 4.8x
Average	44088.5		53.6%	7646.0 383.6, 2.0	6.1x, 2.6x, 2.0x	5.4x, 2.7x, 5.6x	3.8x, 2.4x, 4.2x

$\mathcal{A}/\mathcal{D}/\mathcal{P}$: Area/Delay/Power. †Units: $\mathcal{A}$ (μm^2), $\mathcal{D}$ (ps), $\mathcal{P}$ (mW). ‡RD_i : Redacted Design.
* Reported by Synopsys DC for NanGate 15nm. ⊛Overheads (Ovh) reported as x times original.



(a) Bitstream size variation. (b) Overhead reduction.

Fig. 7: Impact of overhead optimizations on redaction metrics.

Table 2: Overhead comparison between HIPR and state-of-the-art redaction techniques.

Method	Framework	Test IP	Redacted Portion*	Area Overhead* Reported	Area Overhead* Adjusted⊛
$eFPGA_1$ [1]	OpenFPGA	GPS : pcode	0.6% (by area)	1.4x	34.3x
$eFPGA_2$ [2]	OpenFPGA	GPS : cacode	0.1% (by area)	2.1x	271.3x
SheLL [3]	FABulous	AES : _addround_xor	0.1% (by area)	1.4x	180.1x
EvoLUTe [4]	LUT	Multiplier	150 LUTs (13 K bits)	0.9x★	40.1x
HIPR† [5]	LUT	GPS : round r1,r2	14.1% (by area)	1.4x	1.4x

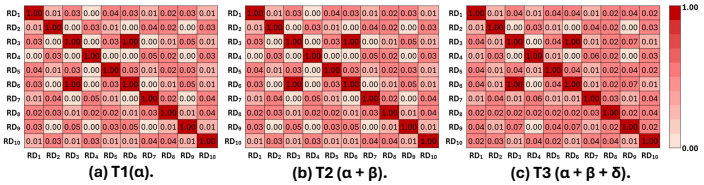
* Compared to the full-chip area. ★Does not include bitstream storage area.
⊛Adjusted to match the amount of logic redacted by HIPR. †This work.

Security Analysis

Table 3: Functional (SAT) [6] and Structural (DANA) [7] attack results.

Test IP	SAT-Attack: Runtime (h) † T1(α)	T2($\alpha+\beta$)	T3($\alpha+\beta+\delta$)	DANA-Attack: {|Clusters|, Runtime (s)} Original	T1(α), T2($\alpha+\beta$) ‡	T3($\alpha+\beta+\delta$)
RD_1*	-	-	-	5, 0.22s	63, 2.38s	63, 1.54s
RD_2	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	8, 0.05s	1, 0.22s	1, 0.15s
RD_3	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	26, 2.13s	1767, 40.01s	1503, 25.61s
RD_4	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	45, 0.19s	129, 1.09s	154, 1.42s
RD_5*	-	-	-	6, 0.28s	90, 3.30s	90, 2.56s
RD_6	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	26, 2.12s	1767, 37.50s	1503, 25.40s
RD_7	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	21, 0.47s	165, 2.68s	246, 3.73s
RD_8	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	1, 0.17s	1, 0.86s	1, 0.66s
RD_9	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	31, 2.7s	669, 16.49s	771, 16.83s
RD_{10}	$\mathcal{TO}$	$\mathcal{TO}$	$\mathcal{TO}$	89, 0.60s	335, 2.28s	1, 0.83s
Average				26, 0.89s	499, 10.69s	434, 7.87s

* sld run fails from I/O mismatch (due to dummy CSB FFs). †Timeout ($\mathcal{TO}$) for sld was 24 hours.
‡Redacted logic is unchanged between T1 and T2, only bitstream generation is optimized.



(a) T1(α). (b) T2 (α + β). (c) T3 (α + β + δ).

Fig 8. Heatmaps depicting LATTE [8] attack resilience under different overhead optimizations.

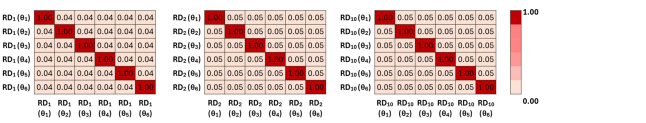


Fig 9. Heatmaps from LATTE [8] attack under varying seed (θ) values.

Conclusion

HIPR is a novel fine-grain hardware redaction methodology for IP protection that:

- utilizes custom programmable fabric to implement the redacted logic and employs security-aware overhead optimizations.
- is robust and scalable, performing hardware redaction at significantly lower overhead costs than the state-of-the-art.
- is resilient against conventional functional [6] and structural attacks [7, 8].

References

[1] P. Mohan *et al.*, "Hardware Redaction via Designer-Directed Fine Grained eFPGA Insertion," *DATE 2021*.
[2] J. Bhandari *et al.*, "Exploring eFPGA-based Redaction for IP Protection," *ICCAD 2021*.
[3] H. M. Kamali *et al.*, "SheLL: Shrinking eFPGA Fabrics for Logic Locking," *DATE 2023*.
[4] R. Guo *et al.*, "EvoLUTe: Evaluation of Look-Up-Table-based Fine Grained IP Redaction," *DATE 2023*.
[5] A. Dasgupta *et al.*, "HIPR: Hardware IP Protection through Low-Overhead Fine-Grain Redaction," *TCHES 2025 Issue 3*.
[6] P. Subramanyan *et al.*, "Evaluating the security of logic encryption algorithms," *HOST 2015*.
[7] N. Albartus *et al.*, "DANA Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering," *TCHES 2020 Issue 4*.
[8] A. Dasgupta *et al.*, "LATTE: Library Attack for Evaluating Hardware IP Protections against Reverse Engineering," *IEEE Design &Test 2025*.