

EVAL-HD

Reproducible Hardware Cost Evaluation in Implementation Security

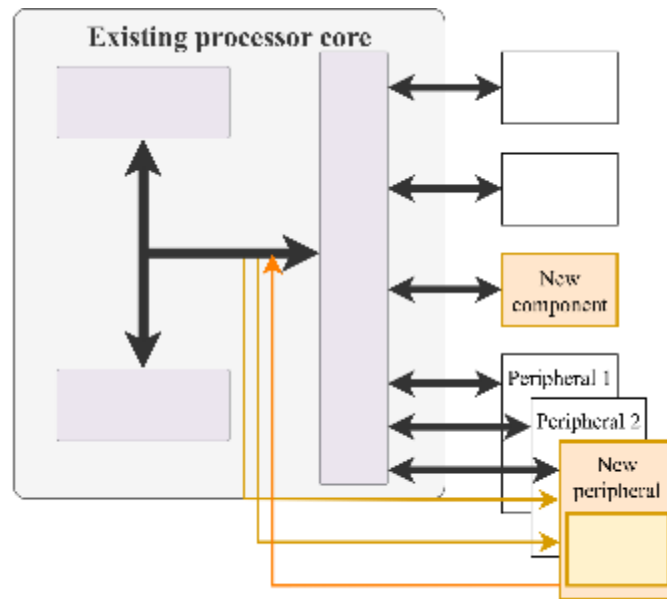
*Jesse De Meulemeester, Quinten Norga, Frank Piessens, Ingrid Verbauwhede,
Marton Bogнар*

OPTIMIST 2026



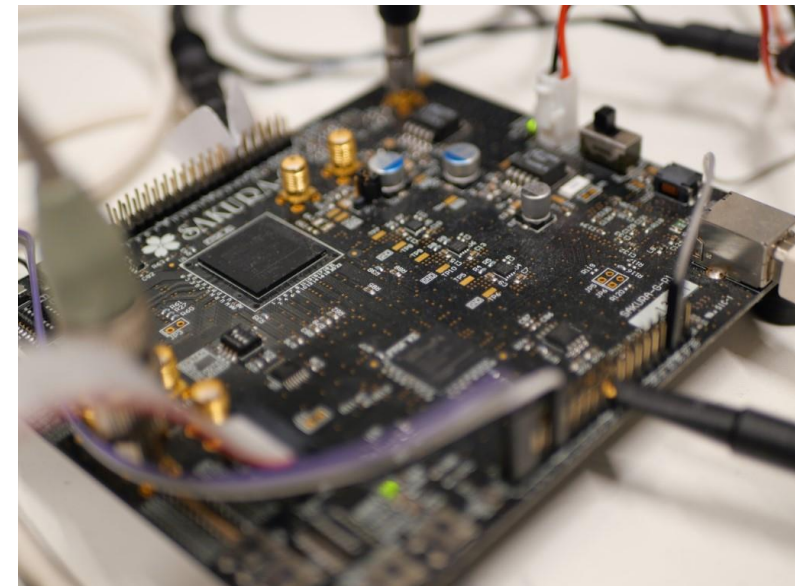
Hardware

Systems Security



Processor extension

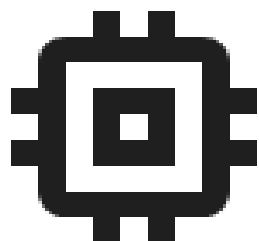
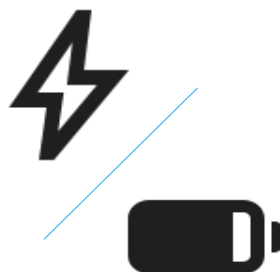
Embedded Security



Crypto accelerator

Hardware cost

- Fair comparison: how to evaluate?



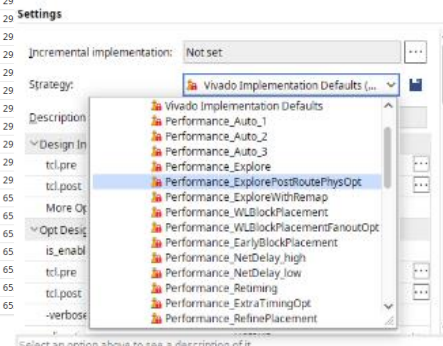
Area cost: LUTs / FFs / DSPs / BRAMs / GEs / mm² / ...

-> Need fair and uniform metrics...

Hardware cost

- Fair comparison: how to measure?

Part	I/O Pin Count	Available IOBs	LUT Elements	FlipFlops	Block RAMs
xc7s15ftgb196-2	196	100	8000	16000	10
xc7s15ftgb196-1	196	100	8000	16000	10
xc7s15ftgb196-1IL	196	100	8000	16000	10
xc7s15ftgb196-1Q	196	100	8000	16000	10
xc7s25csga225-2	225	150	14600	29200	45
xc7s25csga225-1	225	150	14600	29200	45
xc7s25csga225-1IL	225	150	14600	29200	45
xc7s25csga225-1Q	225	150	14600	29200	45
xc7s25csga324-2	324	150	14600	29200	45
xc7s25csga324-1	324	150	14600	29200	45
xc7s25csga324-1IL	324	150	14600	29200	45
xc7s25csga324-1Q	324	150	14600	29200	45
xc7s25ftgb196-2	196	100	14600	29200	45
xc7s25ftgb196-1	196	100	14600	29200	45
xc7s25ftgb196-1IL	196	100	14600	29200	45
xc7s25ftgb196-1Q	196	100	14600	29200	45
xc7s50csga324-2	324	210	32600	65200	90
xc7s50csga324-1	324	210	32600	65200	90
xc7s50csga324-1IL	324	210	32600	65200	90
xc7s50csga324-1Q	324	210	32600	65200	90
xc7s50fpga484-2	484	250	32600	65200	90
xc7s50fpga484-1	484	250	32600	65200	90
xc7s50fpga484-1IL	484	250	32600	65200	90



\$\$\$

Target platform: FPGA or ASIC

-> ... and a reproducible methodology

Hardware cost evaluation in practice

Systems Security

Paper	Implementation Metrics						Metadata				
	FPGA						ASIC				
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform
										Config	Re-synth.
										Open source	Artifact eval.
USENIX Security											
2020											
2020											
2020											
2021											
2021											
2021											
2022											
2022											
2022											
2023											
2023											
2023											
2024											
2024											

Embedded Security

Paper	Implementation Metrics						Metadata				
	FPGA						ASIC				
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform
										Config	Re-synth.
										Open source	Artifact eval.
CHES 2024											

Hardware cost evaluation in practice

Systems Security

Paper	Implementation Metrics									Metadata					
	FPGA						ASIC								
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform	Config	Re-synth.	Open source	Artifact eval.
USENIX Security	2020	●	●	○	○	○	○	○	○	○	○	○	○	○	○
	2020	●	●	○	○	○	○	○	○	○	◐	●	○	○	◐
	2020	◐	○	○	○	○	○	●	○	●	◐	●	○	○	◐
	2021	●	●	○	●	○	○	○	○	○	○	●	-	○	○
	2021	●	●	○	○	○	○	○	○	○	◐	●	○	○	○
	2021	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	2022	●	●	○	○	○	○	○	○	○	◐	●	○	○	○
	2022	●	○	○	○	●	○	○	○	○	●	○	○	○	○
	2022	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	2022	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	2023	●	●	○	○	○	●	○	○	○	◐	●	○	○	○
	2023	●	●	○	○	●	○	○	○	○	◐	●	○	○	○
	2023	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	2024	●	●	○	○	○	○	○	○	○	○	○	○	○	○
	2024	●	●	○	○	○	○	○	○	○	○	○	○	○	○

Embedded Security

Paper	Implementation Metrics						Metadata								
	FPGA						ASIC								
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform	Config	Re-synth.	Open source	Artifact eval.
CHES 2024	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○

Hardware cost evaluation in practice

Systems Security

	Paper	Implementation Metrics						Metadata								
		FPGA					ASIC									
		LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform	Config	Re-synth.	Open source	Artifact eval.
USENIX Security	2020	●	●	○	○	○	○				○	●	○	●	●	●
	2020	●	●	○	○	○	○				●	●	○	○	●	●
	2020	◐	○	○	○	○	○	●	○	●	◐	●	○	●	●	◐
	2021	●	●	○	●	○	○				○	●	○	-	○	○
	2021	●	●	○	○	○	○				◐	◐	○	●	○	○
	2021							●	●	○	●	●	◐	●	●	○
	2022	●	●	○	○	○	○				◐	●	○	○	●	○
	2022	●	○	○	○	●	○				●	●	○	●	●	●
	2022							●	●	●	●	●	○	-	○	●
	2023	●	●	○	○	○	●				◐	●	○	○	●	●
	2023	●	●	○	○	●	○				◐	●	○	●	●	●
	2023							●	●	○	●	●	●	●	○	○
	2024	●	●	○	○	○	○				●	●	○	○	●	○
	2024	●	●	○	○	○	○				●	●	○	●	●	●

Embedded Security

[illegible]

Hardware cost evaluation in practice

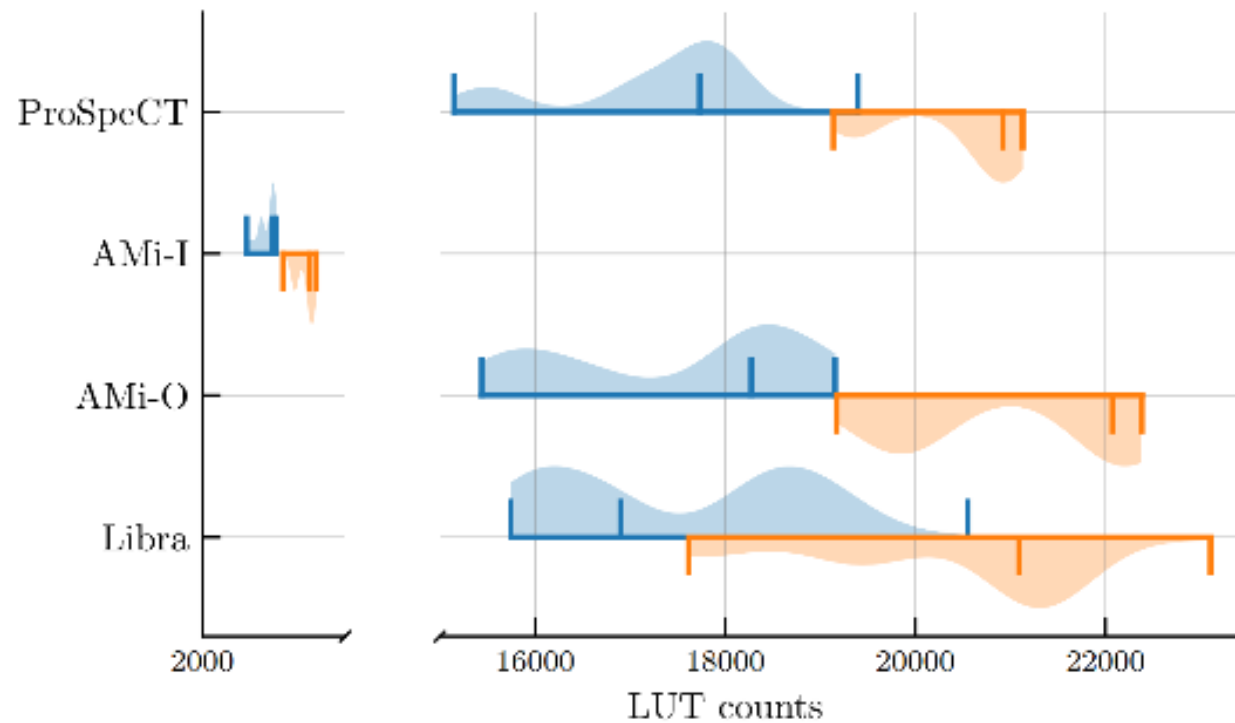
Systems Security

Paper		Implementation Metrics							Metadata							
		FPGA					ASIC		Toolchain Platform Config Re-synth. Open source Artifact eval.							
		LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area							Crit. Path	Other
USENIX Security	2020	●	●	○	○	○	○				○	●	○	●	●	○
	2020	●	●	○	○	○	○				○	●	○	○	●	○
	2020	◐	○	○	○	○	○	●	○	●	○	●	○	○	○	○
	2021	●	●	○	●	○	○				○	●	○	-	○	○
	2021	●	●	○	○	○	○				○	●	○	○	○	○
	2021							●	●	○	○	●	○	○	○	○
	2022	●	●	○	○	○	○				○	●	○	○	○	○
	2022	●	○	○	○	●	○				○	●	○	○	○	○
	2022							●	●	●	○	●	○	-	○	○
	2023	●	●	○	○	○	●				○	●	○	○	○	○
	2023	●	●	○	○	●	○				○	●	○	○	○	○
	2023							●	●	○	○	●	○	○	○	○
	2024	●	●	○	○	○	○				○	●	○	○	○	○
	2024	●	●	○	○	○	○				○	●	○	○	○	○

Embedded Security

Paper	Implementation Metrics									Metadata					
	FPGA						ASIC			Toolchain	Platform	Config	Re-synth.	Open source	Artifact eval.
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other						
CHES 2024	●	●	●	●	●	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○
	●	●	○	○	○	○				○	○	○	○	○	○

Why detailed reporting matters



Part	I/O Pin Count	Available IOBs	LUT Elements	Flipflops	Block RAMs
xc7v150jg1w6-2	196	110	8000	14000	10
xc7v150jg1w6-1	196	110	8000	14000	10
xc7v150jg1w6-1L	196	110	8000	14000	10
xc7v150jg1w6-1Q	196	110	8000	14000	10
xc7v250sga225-2	225	150	14000	20000	45
xc7v250sga225-1	225	150	14000	20000	45
xc7v250sga225-1L	225	150	14000	20000	45
xc7v250sga225-1Q	225	150	14000	20000	45
xc7v250sga224-2	324	150	14000	20000	45
xc7v250sga224-1	324	150	14000	20000	45
xc7v250sga224-1L	324	150	14000	20000	45
xc7v250sga224-1Q	324	150	14000	20000	45
xc7v500jg484-2	484	250	32000	40000	100
xc7v500jg484-1	484	250	32000	40000	100
xc7v500jg484-1L	484	250	32000	40000	100

Settings

Incremental implementation: Not set

Strategy: Vivado Implementation Defaults (...)

Description

- Vivado Implementation Defaults
- Performance_Auto_1
- Performance_Auto_2
- Performance_Auto_3
- Performance_Explore
- Performance_ExplorePostRoutePhysOpt
- Performance_ExploreWithRemap
- Performance_WLBlockPlacement
- Performance_WLBlockPlacementFanoutOpt
- Performance_EarlyBlockPlacement
- Performance_NetDelay_high
- Performance_NetDelay_low
- Performance_Retiming
- Performance_ExtraTimingOpt
- Performance_RefinePlacement

Design In

- tcl.pre
- tcl.post

More Op

- Opt Desig
- is_enabl
- tcl.pre
- tcl.post
- verbose

Hardware cost evaluation in practice

- ① Reporting and methodologies
- ↗ Variable evaluation metrics
- ⊖ Fair evaluation and comparison



EVAL-HD: an open-source ASIC toolchain for researchers *(with minimal EDA experience)*

EVAL-HD: How to use

```
./eval-hd.py target_design.v
```

- Single area & timing metric
- Pyosys
- FreePDK nangate-45nm (*or others*)
- Minimal friction

Design	Area (overhead)	f _{max} (change)
ProSpeCT	0.219 mm ² (20.87%)	348 MHz (-9.4%)
AMi-I	0.045 mm ² (6.53%)	500 MHz (-1.1%)
AMi-O	0.199 mm ² (10.30%)	360 MHz (-6.3%)
Libra	0.244 mm ² (6.71%)	381 MHz (-0.0%)

EVAL-HD: RTL to μm^2 and Hz

- **Accessibility** and **transparency**
 - Open-source, script-based and easy-to-use
- **Reproducibility** and **Consistency**
 - No tool- or vendor-specific settings or metrics
- **Fairness** and **Meaningfulness**
 - Uniform and representative metrics for fair comparison

Summary

- Inconsistent evaluation strategy can lead to misleading conclusions
- EVAL-HD aims to be reproducible and meaningful



Paper: <https://mici.hu>

EVAL-HD: <https://github.com/KULeuven-COSIC/eval-hd>

Data set: <https://doi.org/10.48804/WCDDKG>



Future work

- Tapeout-quality results (use OpenRoad-flow-scripts in backend)
 - *Would this make comparison more meaningful?*
- Power metrics
 - *How to keep it accessible?*
- Support more cell libraries
 - *How to ensure fair/direct comparisons?*