

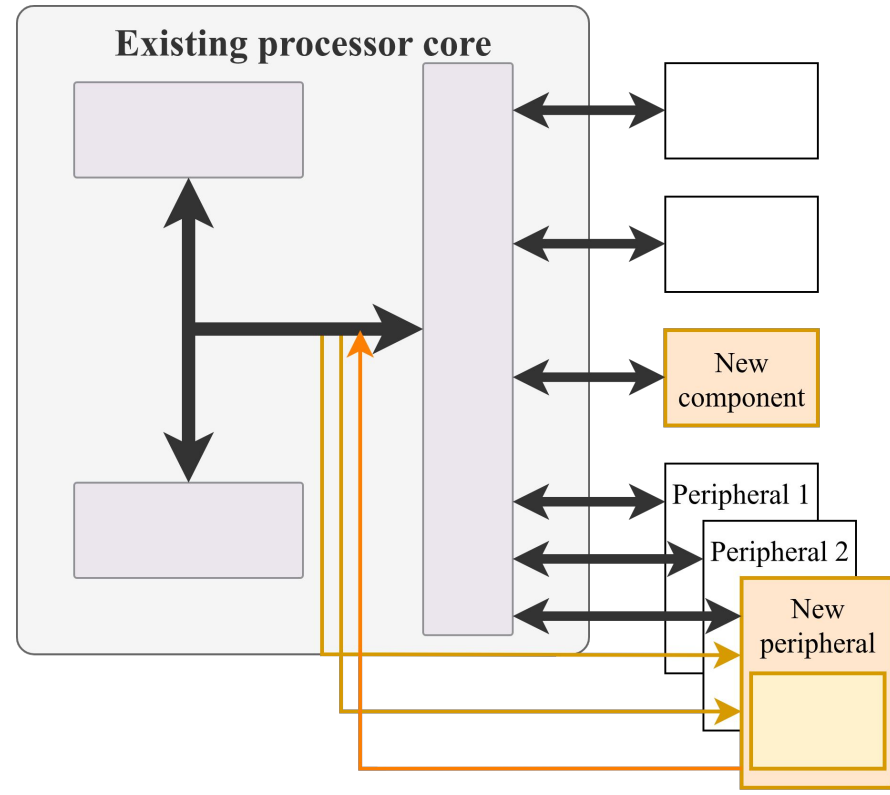
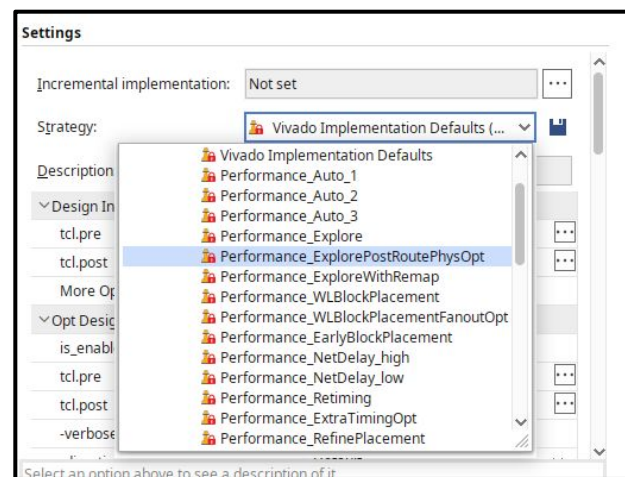
Hardware Cost Evaluation in Microarchitecture Security

Jesse De Meulemeester, Quinten Norga, Frank Piessens, Ingrid Verbauwhede, Marton Bognar
KU Leuven, Belgium

quinten.norga@esat.kuleuven.be

What is hardware cost?

- Scenario: new defense for a microarchitectural attack
 - Prototype: **extend or modify hardware**
- Common evaluation criterion: **how “expensive”?**
- Synthesis-based workflow
 - Field Programmable Gate Array (FPGA)
 - Application-Specific Integrated Circuit (ASIC)
- Many resulting metrics: area (in different components), power, critical path, etc.
- **Vast array** of possible configurations



Test	SCOT Count	Available Data	LCUT Elements	Phases	Block Labels
LCUT1700-2	196	100	1000	16000	10
LCUT1700-1	196	100	1000	16000	10
LCUT1700-100	196	100	1000	16000	10
LCUT1700-1000	196	100	1000	16000	10
LCUT1700-25	225	150	14000	20000	45
LCUT1700-250	225	150	14000	20000	45
LCUT1700-2500	225	150	14000	20000	45
LCUT1700-25000	225	150	14000	20000	45
LCUT1700-250000	225	150	14000	20000	45
LCUT1700-2500000	225	150	14000	20000	45
LCUT1700-25000000	225	150	14000	20000	45
LCUT1700-250000000	225	150	14000	20000	45
LCUT1700-2500000000	225	150	14000	20000	45
LCUT1700-25000000000	225	150	14000	20000	45
LCUT1700-250000000000	225	150	14000	20000	45
LCUT1700-2500000000000	225	150	14000	20000	45
LCUT1700-25000000000000	225	150	14000	20000	45
LCUT1700-250000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-2500000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-25000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	225	150	14000	20000	45
LCUT1700-250000000000000000000000000000000000000000000000000000000000000000					

Literature survey

- **Hardware cost** evaluation in practice
- Manual survey of published hardware designs
 - Systems security conference (USENIX Security 2020-2024), 8/14 of which analyze *microarchitecture* security
 - Cryptographic hardware conference (CHES 2024)

[illegible]

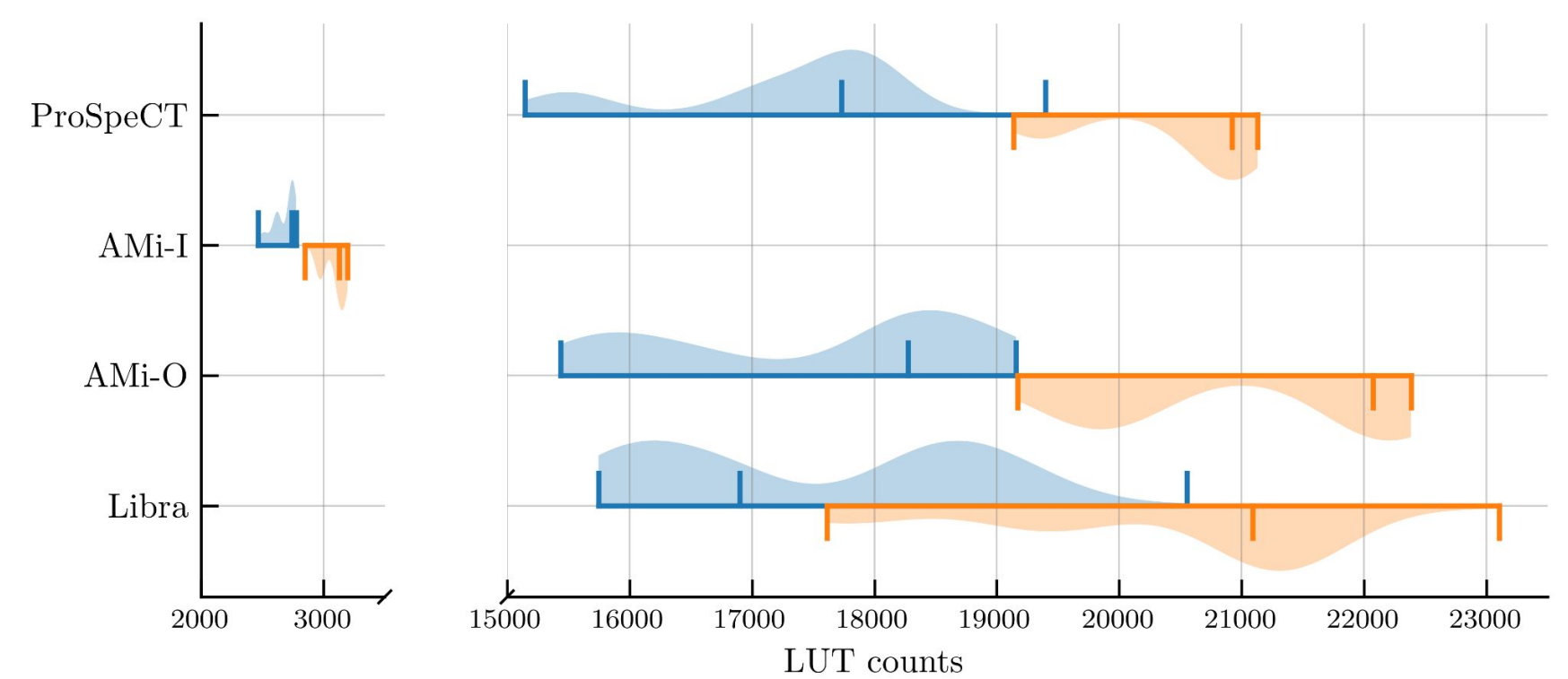
- **Common reproducibility issues:**
 - Unspecified toolchain (57% vs. 29%)
 - Missing configuration (93% vs. 57%)
 - Unfair comparisons (25% vs. 56%)
 - Closed source (29% vs. 38%)

- **Main takeaways:**
 - ASIC more common at CHES
 - More evaluation metrics reported
 - Better config reporting
 - Artifacts more often available/evaluated at USENIX
 - Sometimes comparing to related work without re-synthesizing

Case study: exposing the problem

- What happens if **configuration** is **not sufficiently** reported?
- **Comparison** with related work based on reported numbers
- Detailed configuration required for comparing related work
- Case study in microarchitecture security: variability of results for **Proteus processor** (RISC-V) extensions
 - Synthesis to the same FPGA
 - Different optimization options
 - Large differences in look-up table (LUT) count and clock frequency

Design	LUTs (overhead)			f _{max} [MHz] (change)		
	min	avg	max	min	avg	max
ProSpeCT	19137 (12.7%)	20524 (16.2%)	21131 (19.7%)	32.287 (-4.17%)	32.492 (-0.95%)	33.113 (+1.70%)
AMi-I	2847 (14.2%)	3093 (17.4%)	3197 (20.2%)	58.483 (-3.27%)	58.888 (-0.68%)	60.017 (+2.26%)
AMi-O	19172 (16.0%)	21110 (21.5%)	22383 (26.5%)	32.279 (-3.51%)	32.598 (-0.48%)	33.428 (+2.76%)
Libra	17613 (8.78%)	20359 (13.1%)	23104 (16.5%)	26.752 (-3.81%)	27.067 (-0.07%)	27.880 (+2.52%)



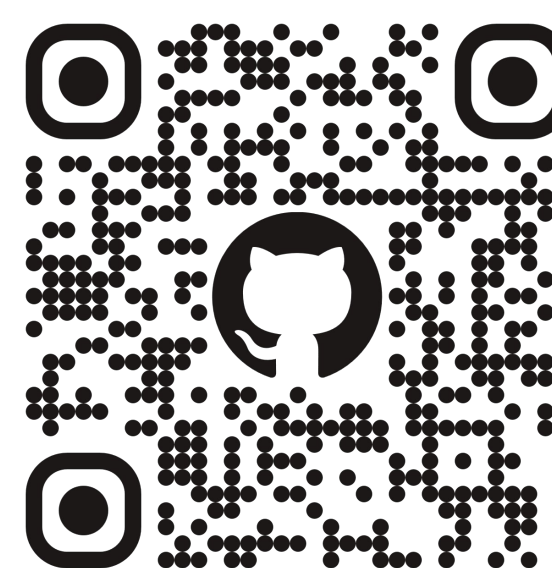
EVAL-HD: an open-source toolchain

- **EVAL-HD: Open-source** tool for hardware cost evaluation
- Uses the Yosys synthesis tool with nangate-45nm cell library
- Reports single area metric & maximum clock frequency
 - **More representative** of production processes
- **Easy-to-use** Python interface

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%)

Resources

This poster is based on the findings from the paper "Jesse De Meulemeester, Quinten Norga, Frank Piessens, Ingrid Verbauwhede, and Marton Bognar. 2025. *Hardware Cost Evaluation in Systems Security*. In Proceedings of the 3rd ACM Conference on Reproducibility and Replicability (ACM REP '25)."



Paper: <https://mici.hu>
EVAL-HD: <https://github.com/KULeuven-COSIC/eval-hd>
Data set: <https://doi.org/10.48804/WCDDKG>