

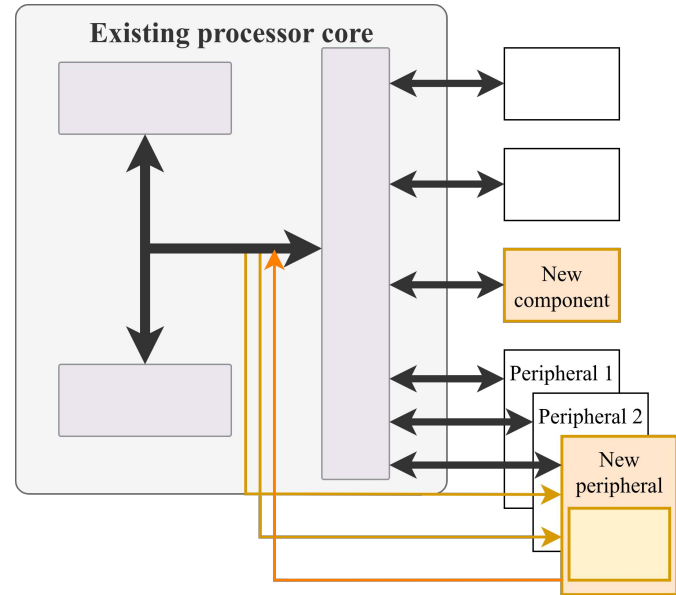
Hardware Cost Evaluation in Systems Security

Jesse De Meulemeester, Quinten Norga,
Frank Piessens, Ingrid Verbauwheide, Marton Bognar

What is hardware cost?

Hardware: for us, **processor** in a computing device

- Extensions: new features, security improvements, ...



What is hardware cost?

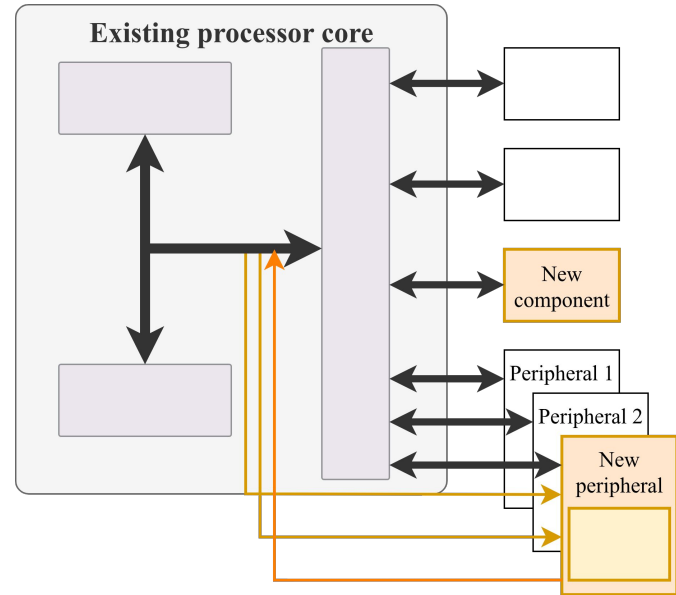
Hardware: for us, **processor** in a computing device

- Extensions: new features, security improvements, ...

How to **evaluate** these changes?

- Will the new processor be twice as big?
- ...consume twice as much battery?
- ...execute the same programs slower?

Try to approximate the impact!



Approximating the impact

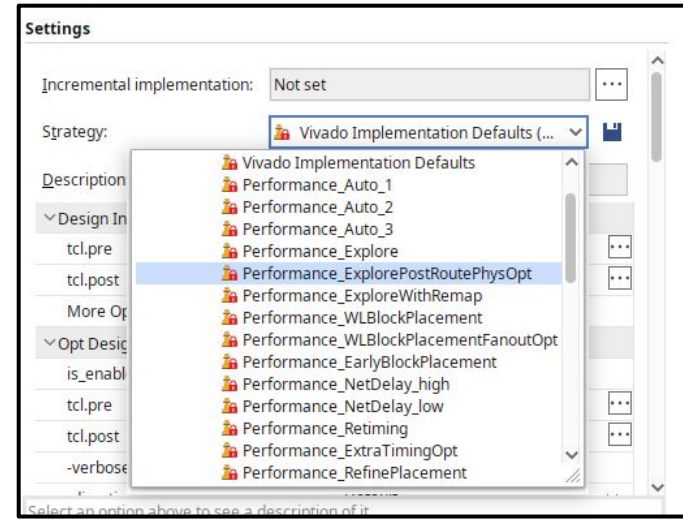
Two main directions:

- Field-Programmable Gate Arrays (**FPGA**)
 - Prototyping, affordable
- Application-Specific Integrated Circuit (**ASIC**)
 - Closer to commercial processes

A taste of the options

FPGA synthesis in Xilinx Vivado

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	75
xc7s50csga324-1	324	210	32600	65200	75
xc7s50csga324-1IL	324	210	32600	65200	75
xc7s50csga324-1Q	324	210	32600	65200	75
xc7s50fgga484-2	484	250	32600	65200	75
xc7s50fgga484-1	484	250	32600	65200	75
xc7s50fgga484-1IL	484	250	32600	65200	75



**Can the results be
reproducible, fair, and
meaningful?**

Literature: Hardware 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								
2020	●	●	○	○	○	○	●	○	●	○	●	○	●	●	○		
2020	●	●	○	○	○	○				●	○	○	○	○	○	○	○
2020	●	○	○	○	○	○				○	○	○	○	○	○	○	○
2021	●	●	○	●	○	○				○	○	○	○	○	○	○	○
2021	●	○	○	○	○	○				○	○	○	○	○	○	○	○
2021	●	●	○	○	○	○	●	●	○	●	●	○	○	○	○		
2022	●	●	○	○	○	○	●	●	●	●	●	○	●	●	○		
2022	●	○	○	○	●	○				○	○	○	○	○	○	○	○
2022	●	○	○	○	○	○				○	○	○	○	○	○	○	○
2023	●	●	○	○	○	●				○	○	○	○	○	○	○	○
2023	●	●	○	○	○	○				○	○	○	○	○	○	○	○
2023	●	●	○	○	○	○	●	●	○	○	○	○	○	○	○		
2023	●	●	○	○	○	○	●	●	○	○	○	○	○	○	○		
2024	●	●	○	○	○	○	●	●	○	●	●	○	○	●	○		
2024	●	●	○	○	○	○				○	○	○	○	○	○	○	○

Cryptography

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	●	●	●	●	●	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○

Literature: Hardware 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
2020	●	●	○	○	○	○				○	●	○
2020	●	●	○	○	○	○				●	●	○
2020	●	○	○	○	○	○	●	○	●	●	●	○
2021	●	●	○	●	○	○				○	●	○
2021	●	●	○	○	○	○				●	●	○
2021	●	●	○	○	○	○	●	●	○	○	●	○
2022	●	●	○	○	○	○				●	●	○
2022	●	○	○	○	●	○				●	●	○
2022	●	●	○	○	○	○	●	●	●	○	●	○
2023	●	●	○	○	○	○				●	●	○
2023	●	●	○	○	○	○				○	○	○
2023	●	●	○	○	○	○	●	●	○	●	●	○
2024	●	●	○	○	○	○				●	●	○
2024	●	●	○	○	○	○				●	●	○



Fewer reported metrics

Cryptography

Paper	Implementation Metrics						Metadata					
	FPGA						ASIC					
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform	Config
CHES 2024	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○

Literature: Hardware 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
2020	●	●	○	○	○	○				○	●	○
2020	●	●	○	○	○	○				○	●	○
2020	●	○	○	○	○	○	●	○	●	○	●	○
2021	●	●	○	○	○	○				○	●	○
2021	●	●	○	○	○	○				○	●	○
2021	●	●	○	○	○	○	●	●	○	○	●	○
2022	●	●	○	○	○	○				○	●	○
2022	●	○	○	○	○	○				○	●	○
2022	●	○	○	○	○	○	●	●	●	○	●	○
2023	●	●	○	○	○	○				○	●	○
2023	●	●	○	○	○	○				○	●	○
2023	●	●	○	○	○	○	●	●	○	○	●	○
2024	●	●	○	○	○	○				○	●	○
2024	●	●	○	○	○	○				○	●	○



Fewer ASIC evaluations

Cryptography

Paper	Implementation Metrics						Metadata					
	FPGA						ASIC					
	LUT	FF	DSP	BRAM	Crit. Path	Other	GE / Area	Crit. Path	Other	Toolchain	Platform	Config
CHES 2024	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○
	●	●	○	○	○	○				○	●	○

Literature: Hardware 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						
2020	●	●	○	○	○	○	○	●	○	○	○	○
2020	●	●	○	○	○	○	○	●	○	○	○	○
2020	●	○	○	○	○	○	●	○	○	○	○	○
2021	●	●	○	○	○	○	○	●	○	○	○	○
2021	●	●	○	○	○	○	○	●	○	○	○	○
2021	●	●	○	○	○	○	○	●	○	○	○	○
2022	●	●	○	○	○	○	○	●	○	○	○	○
2022	●	○	○	○	○	○	○	●	○	○	○	○
2022	●	○	○	○	○	○	○	●	○	○	○	○
2023	●	●	○	○	○	○	○	●	○	○	○	○
2023	●	●	○	○	○	○	○	●	○	○	○	○
2023	●	●	○	○	○	○	○	●	○	○	○	○
2024	●	●	○	○	○	○	○	●	○	○	○	○
2024	●	●	○	○	○	○	○	●	○	○	○	○



Missing toolchain configuration

Cryptography

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

Literature: Hardware 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.
2020	●	●	○	○	○	○				○	●	○	●	●	○
2020	●	●	○	○	○	○				○	●	○	○	○	○
2020	●	○	○	○	○	○	●	○	●	○	●	○	○	○	○
2021	●	●	○	●	○	○				○	●	○	○	○	○
2021	●	●	○	○	○	○				○	●	○	○	○	○
2021	●	●	○	○	○	○	●	●	○	○	●	○	○	○	○
2022	●	●	○	○	○	○				○	●	○	○	○	○
2022	●	○	○	○	●	○				○	●	○	○	○	○
2022							●	●	●	○	●	○	○	○	○
2023	●	●	○	○	○	●				○	●	○	○	○	○
2023	●	●	○	○	●	○				○	●	○	○	○	○
2023							●	●	○	○	●	○	○	○	○
2024	●	●	○	○	○	○				○	●	○	○	○	○
2024	●	●	○	○	○	○				○	●	○	○	○	○

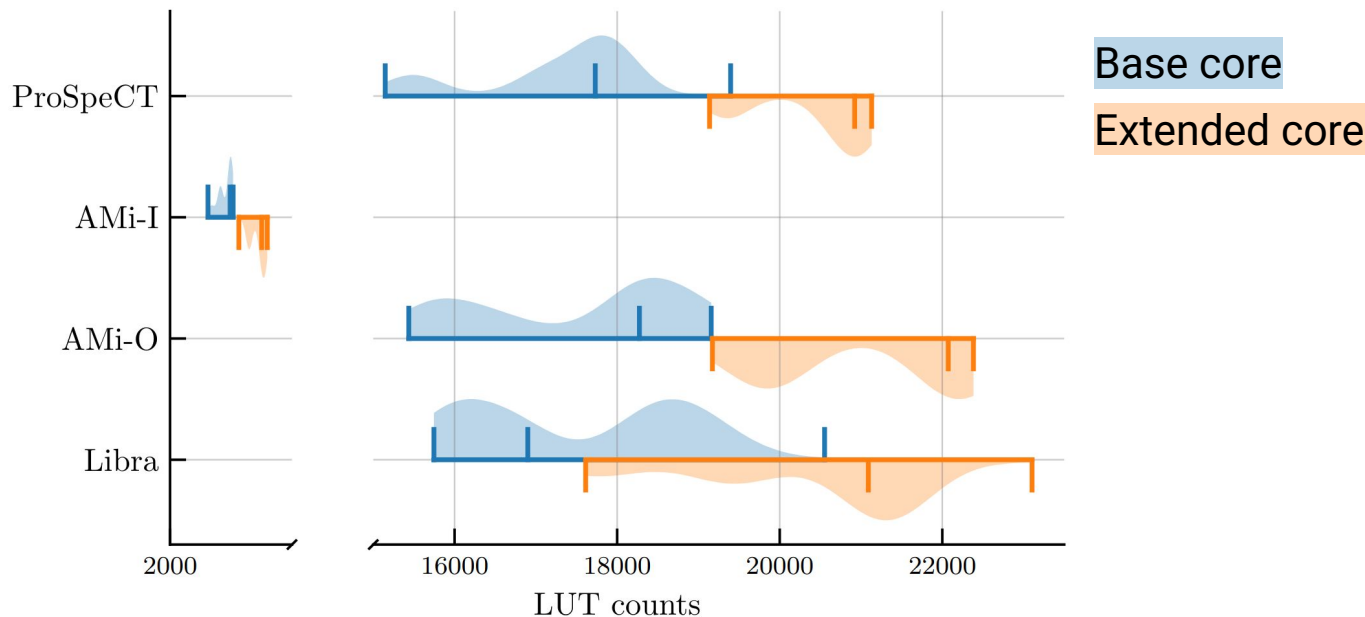


Unfair comparison due to different configurations

Cryptography

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	●	●	●	●	●	○				○	●	○	○	○	○
	●	●	●	●	●	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○
	●	●	○	○	○	○				○	●	○	○	○	○

Case study: Why detailed config is needed



Same designs for different optimization configurations

Our proposal: Open-source ASIC toolchain

Single area metric (mm² instead of FPGA components)

Open-source: easier **reproduction**

Future work: more metrics!

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%)

Results of the **EVAL-HD** toolchain

Summary and conclusion

- Literature study on hardware cost evaluation
 - Little consistency in systems security
 - Can lead to misleading conclusions
- Proposed way forward
 - Learn from other fields
 - Use reproducible flows



Paper:

<https://mici.hu>

EVAL-HD:

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

Data set:

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