

PULP PLATFORM

Open Source Hardware, the way it should be!

How RISC-V can help in security research

Frank K. Gürkaynak, ETH Zürich

26th IEEE European Test Symposium

Special Session 4: Security, Reliability and Test Aspects of the RISC-V Ecosystem



<http://pulp-platform.org>



@pulp_platform

ETH zürich



Will RISC-V solve your security issues?

NO

... but it can help

Seems like a short talk, what is on the menu?

- Who am I, what does the Parallel Ultra Low Power project do?
- How do we see security issues?
- How can open source HW and RISC-V help?
- What have we been doing in this field?
- A brief summary

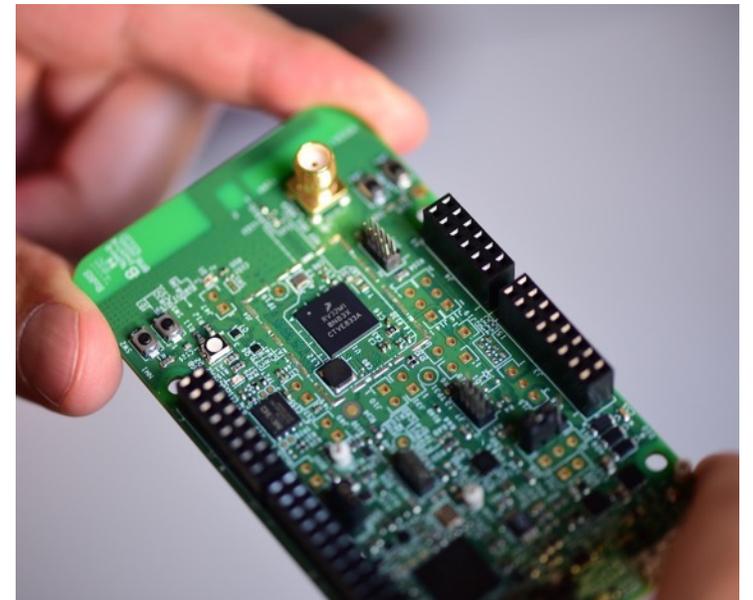
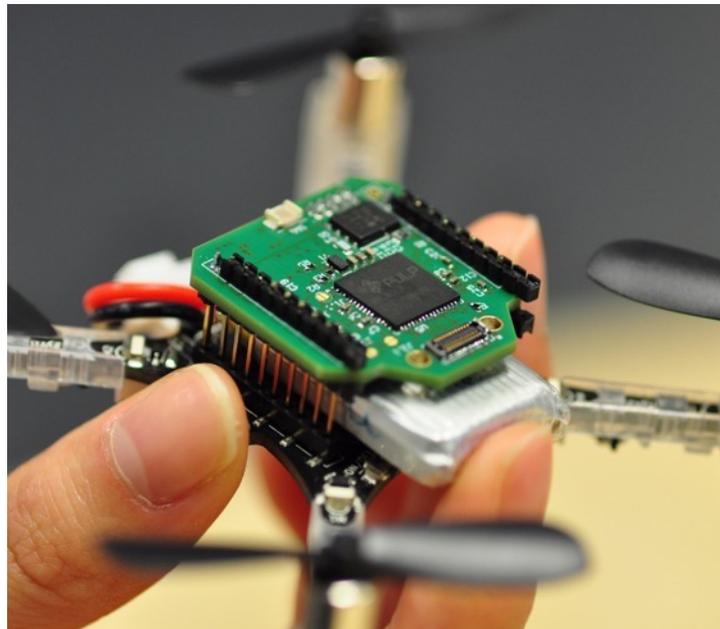
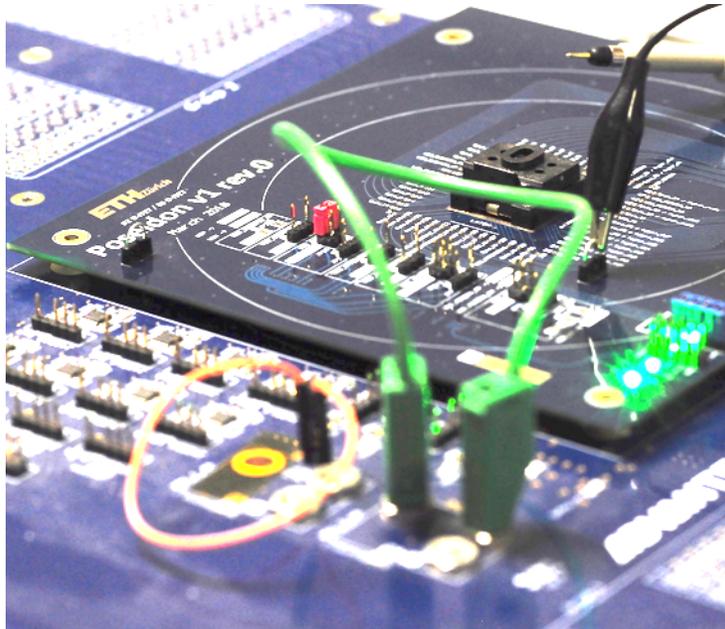
I am part of the PULP project since 2013

- Luca wanted to work on **NEW** energy efficient architectures
 - Keywords were: parallel processing, near threshold operation, energy efficiency
 - Parallel **U**ltra **L**ow-**P**ower platform was born
- Large group of **60 people** in ETH Zurich and University of Bologna
 - Working on technology, IC design, architecture, programming, and applications.
- Experienced in ASIC design. We have **41 PULP ASICs** taped out
 - Recent chips in 22nm, 40nm and 65nm
 - See the complete list at <http://asic.ethz.ch>



Our ASICs have different use cases

- Chips characterized on an IC tester (*Poseidon 22nm*)
- Research demonstrators (*Nano drone with Mr. Wolf*)
- Industrial uses of our cores/peripherals (*open-isa.org Vega board*)



PULP has released a large number of IPs

RISC-V Cores

RI5CY	Ibex	Snitch	Ariane
32b	32b	32b	64b

Peripherals

JTAG	SPI
UART	I2S
DMA	GPIO

Interconnect

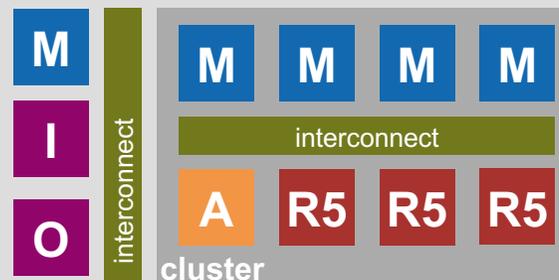
Logarithmic interconnect
APB – Peripheral Bus
AXI4 – Interconnect

Platforms



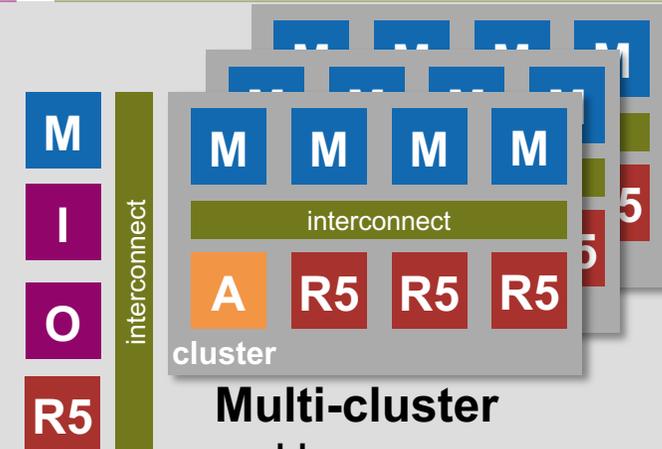
Single Core

- PULPino
- PULPissimo



Multi-core

- Fulmine
- Mr. Wolf



Multi-cluster

- Hero
- Open Piton

IOT

HPC

Accelerators

HWCE
(convolution)

Neurostream
(ML)

HWCrypt
(crypto)

PULPO
(1st order opt)

Committed to open source from day one

- **Our goal was to release everything (we could) as open source**
 - There are still discussions on what can be released (HDL source, scripts, netlist, GDS)
 - PULP has been using a **permissive** Solderpad license since the beginning
- **Our first open source release was in February 2016 (PULPino)**
 - Very simple microcontroller using a single 32-bit RISC-V core (RI5CY)
- **As of now (start of 2021) we have released:**
 - Single core platforms: PULPino, PULPissimo
 - Cluster-based multi-core platforms: OpenPULP, HERO, Open Piton + Ariane
 - And a range of RISC-V cores, peripherals, accelerators and interconnect solutions

Open HW for security and safety is popular

- **The PULP project is a very good platform for collaboration**
 - It is open source, has been silicon proven and can be used for quite powerful systems
 - We have many discussions with project partners about possible projects
- **More than half of the project ideas we discuss are on**
 - Securing processors against side-channel attacks
 - Implementing systems with improved safety and reliability
- **Based on this experience:**
 - Allow me to make some comments on the pros and cons of OpenHW / RISC-V in security

Securing systems is a **VERTICAL** problem

Abstraction Layer	Example	Attacks
Service	E-Voting service	Legal challenges
Users	Voters	Social engineering
Application	Swiss Post	Bugs / backdoors in SW
Algorithms / libraries	RSA / openssl	Weaknesses in Algorithms
Operating Systems	seL4	Privilege elevation
Architecture	NXP - i.MX	Memory/cache attacks
Microarchitecture	ARM - Cortex	Attacks on control flow
Digital Electronics	Adders, gates, FPGAs, ASICs	Side channel leakage
Physics	Electrons, Quantum states	Environment

Security issues at ALL Levels

Open source HW

Solutions are needed at **MULTIPLE** levels

- Hardware is **only one part** of the system
 - In some cases security problems are caused by multiple levels interacting with each other
- Open source hardware can **help** provide solutions
 - Many application / libraries / operating system solutions rely on open source software
 - Open source hardware broadens the scope of what can be done
 - But it can not solve all the issues alone
- **It is important to understand what it can and can not deliver**
 - We have seen that people have unrealistic expectations from open source hardware
When these are inevitably not met, open source HW gets unfairly criticized in the end

How can open source HW help?

- Know what is **really** inside
- More and independent **verification** of blocks
- Be able to **experiment** without constraints
- **Share** the information freely
- Fairer **benchmarking**

- After all: **Open source SW has proven useful**
why should open source HW be different?



Knowing how things exactly work is vital

- From the “ZombieLoad” paper

From section 3.2, emphasis added for this presentation

*“While we identified some necessary building blocks to observe the leakage (cf. Section 5), we **can only provide a hypothesis on why** the interaction of the building blocks leads to the observed leakage. As we could only observe data leakage on Intel CPUs, we assume that this is indeed an implementation issue (such as Meltdown) and not an issue with the underlying design (as with Spectre).”*

- Closed implementations hide/abstract many secrets from users

- Being able to see inside and run experiments are vital for safety and security experts

M. Schwarz, M. Lipp, D. Moghimi, J. Van Bulck, J. Stecklina, T. Prescher, D. Gruss, “ZombieLoad: Cross-Privilege-Boundary Data Sampling”, arXiv:1905.05726

It is not that cores from XYZ are insecure

- **Most commercial processors have well thought out solutions**
 - In most likelihood better than anything we have in open source hardware
- **But a security researcher does not always have access**
 - Work and insights can not be shared freely between researchers
 - Experimenting (an important part of research) is limited, you work with what is given
 - Results and changes can not be verified independently
- **This is where open source hardware can help the most**

Enter RISC-V to the rescue

- RISC-V Foundation established in 2015
 - ETH Zürich is a **founding member**
 - More than 275 members
- ISA is essentially a document
 - Defines 32/64/128 bit architectures
 - What are the instructions, what effect do they have
- ISA divided into several extensions
 - Working groups decide and work on the definitions
 - Several are **ratified**, work continues on others

Name	Description
I	Integer
E	Integer with 16 registers
C	Compressed Instructions
M	Multiplication
F	IEEE 32b floating point
D	IEEE 64b floating point
Q	IEEE 128b floating point
A	Atomic instructions
V	Vector extensions
P	Packed SIMD extensions
B	Bit manipulation
...	and more

RISC-V foundation only defines the ISA

- The ISA is free, implementations **can be done by anyone**
 - ETH Zürich specializes in efficient SystemVerilog based open source implementations
 - **RI5CY**: 32bit Micro-processor with DSP extensions (will be part of OpenHW Core-V)
 - **ibex**: 32bit minimal processor (maintained by LowRISC)
 - **Ariane**: 64 bit Linux capable core (will be part of OpenHW Core-V)
 - There are many others (SiFive, Codaip, Andes, WesternDigital, IIT-Madras,.. and more)
 - Implementations **can also be commercial**, it is only the ISA that is open
- The foundation is working on a set of compliance tools
 - Only foundation members are allowed to officially call their implementations RISC-V

What is so special about RISC-V

- It is **FREE**
 - Everybody can build, sell, and make RISC-V cores available
- **It is a modern design, no historical baggage**
 - Some of the more common ISAs (ARM, Intel..) have been around for 20+ years
Newer implementations, still need to be compatible to older designs.
 - RISC-V benefited from the mistakes made by others, cleaner design
 - Major design decisions have been properly motivated and explained
- **Reserved space for extensions, modular**
- **Open standard**, you can help decide how it is developed

Are RISC-V processors better than XYZ?

- **Actual performance depends on the implementation**
 - RISC-V does not specify implementation details (on purpose)
- **It is a modern design, should deliver comparable performance**
 - If implemented well, it should perform as good as other modern ISA implementations
 - In our (ETH Zürich) experiments, we see no weaknesses when compared to other ISAs
 - It also is not magically 2x better
- **High-end processor performance is not much about ISA**
 - Implementation details like technology capabilities, memory hierarchy, pipelining, and power management are more important.

Examples of our security related work

- Various projects based on Open Source HW and RISC-V
 - Accelerators
 - Side-channel security
 - Control Flow Integrity
 - Replication and ECC for data safety
 - Securing processors against covert/timing channels
- Agile collaboration with many partners helped a lot

Leakage resilient cryptography

- Reduce Attack surface

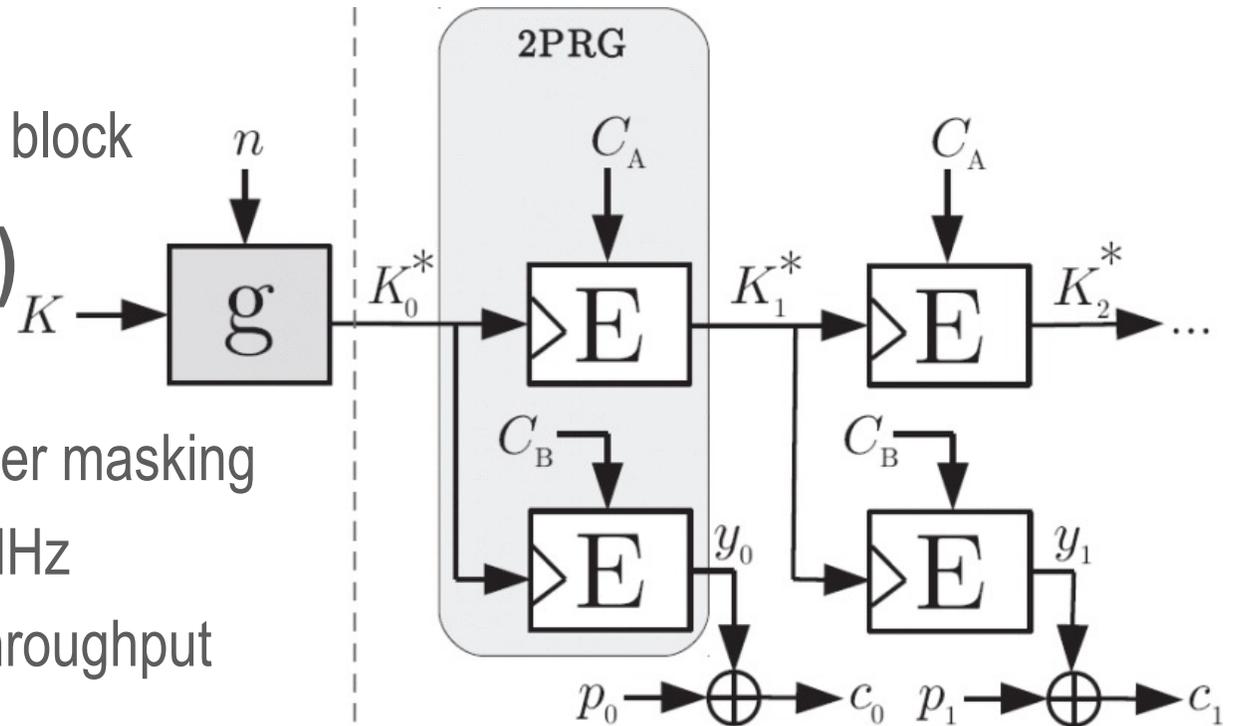
- A new key (K^*) is generated per data block

- Encryption example (2PRG)

- E function is AES
- g finite field multiplication with 1st order masking
- Max throughput 5.29 Gbit/s @ 256 MHz
- Needs 2x Block ciphers for same throughput

- Strong side channel resilience **within IoT Power budget**

- Implemented and tested on actual ASICs



Robert Schilling, Thomas Unterluggauer, Stefan Mangard, Frank Gürkaynak, Michael Muehlberghuber, Luca Benini, "High-Speed ASIC Implementations of Leakage-Resilient Cryptography", DATE 2018

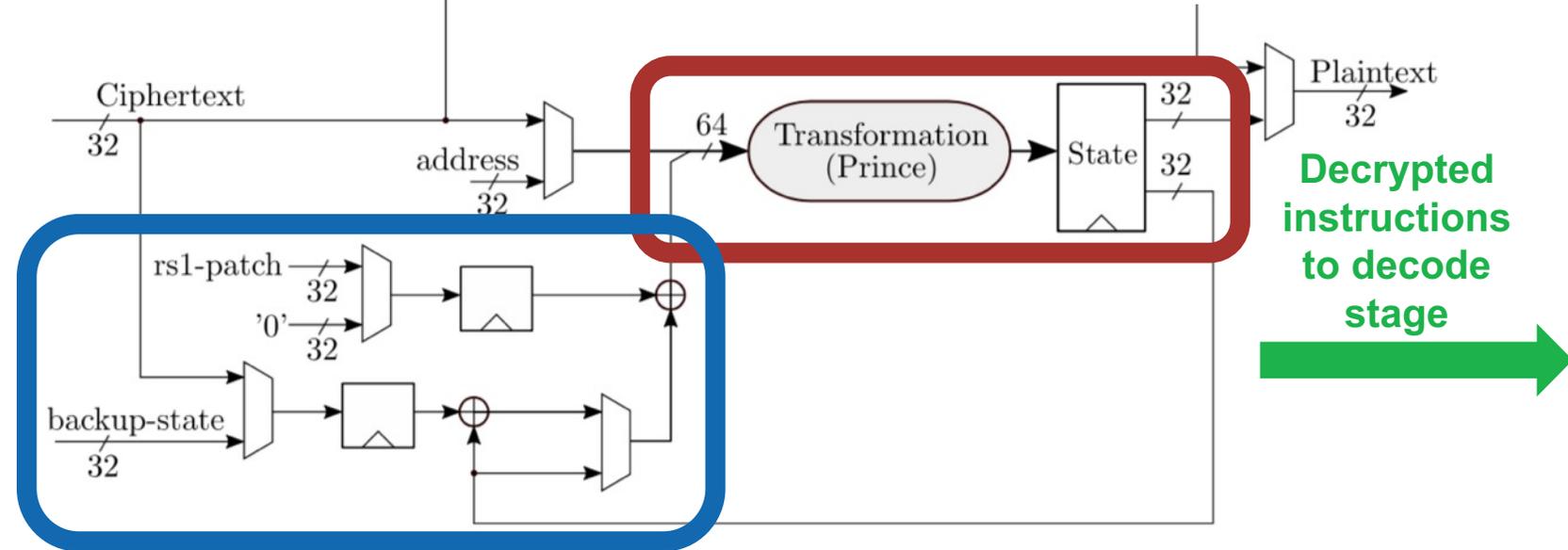
Protecting control flow

forward
(initial startup)

Encrypted instructions
from memory

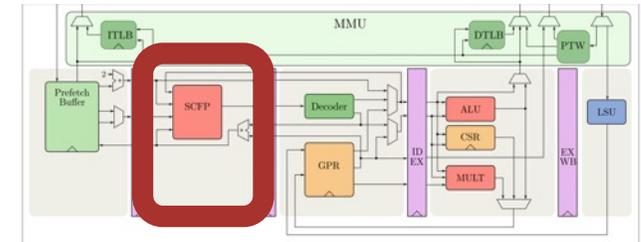


Ability to patch the state
for branches/jumps



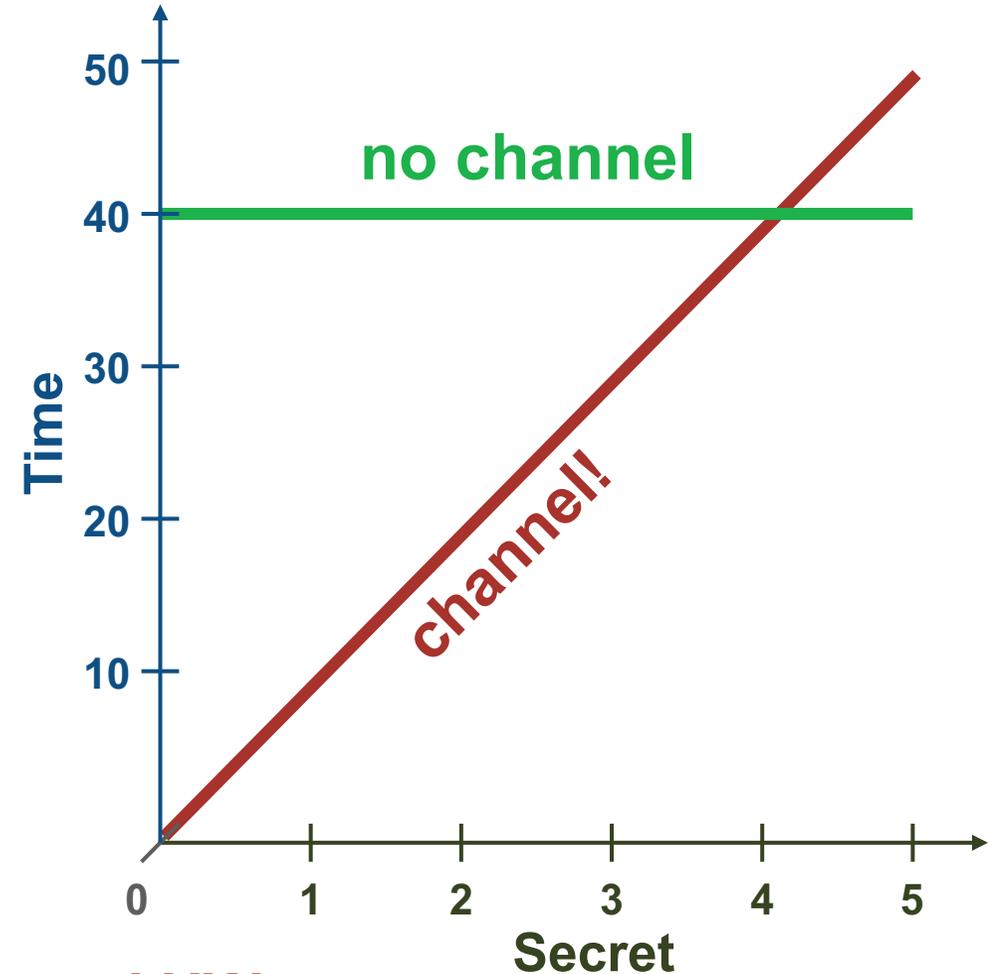
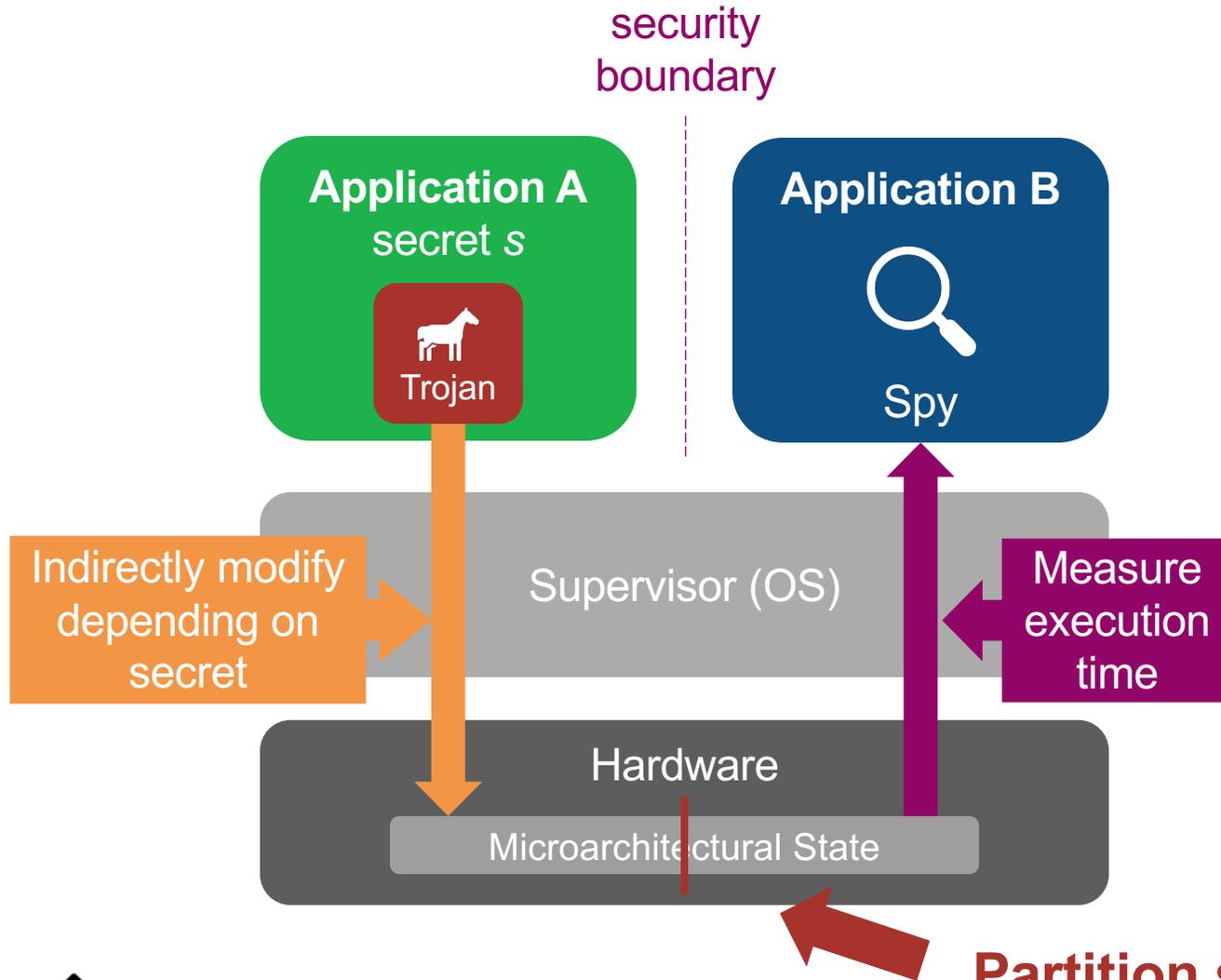
■ Sponge based construction to decrypt instructions

- Only 25-35% power/area 10% runtime overhead
- **Additional instructions** for branches added as extensions

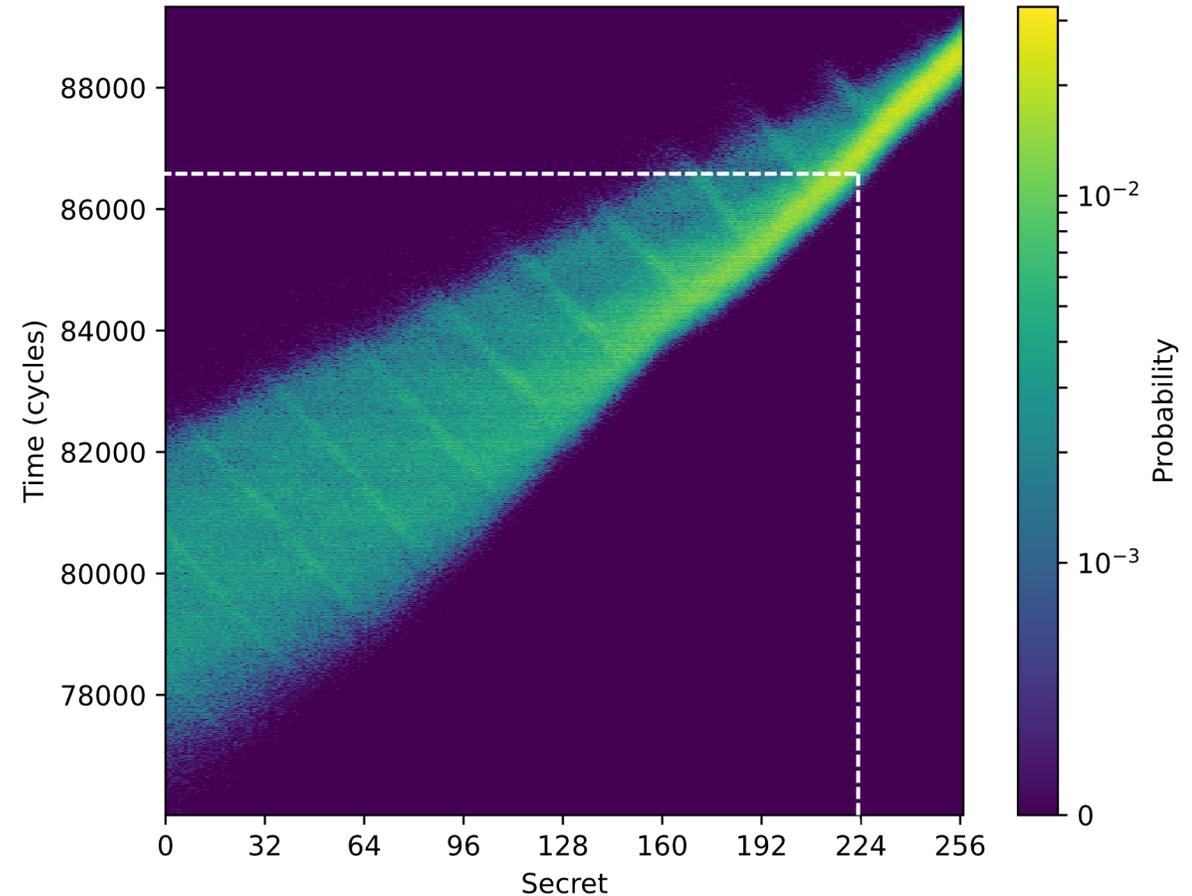


■ Attacker has to **change** instructions and **state** at the same time

Microarchitectural Timing Channels



- **Simple processor not enough**
 - Most covert channels are due to performance optimizations in high performance processors
 - Ariane (6 stage, in-order 64bit RISC-V)
- **Many sources for channels**
 - Data/Instruction Cache, Branch table, Lookaside buffers, replacement policies
- **Working seL4 port on Ariane**



How open source helped us in our projects

- **Start from a working system, no need to reinvent everything**
 - Our 32bit microcontrollers are quite mature, Ariane runs Linux and Sel4
- **Easy to extend with accelerators and custom blocks/memories**
 - Platforms designed for heterogeneous acceleration (PULPissimo, OpenPULP, HERO)
- **Not limited by previous design choices**
 - Do you want to have 2 additional bits for your registers, drop instructions, add new ones?
- **Full source code allows you to observe/record everything**
 - Not limited to which performance counters, timers are available, build add/your own
- **Possible to exploit the results commercially**

Not everything is perfect, still work to do

- **Modern attacks exploit features of high performance processors**
 - Current open source offerings not at the same level of high-end commercial processors
 - At the moment, no out of order, multi-issue, SMP systems within PULP ecosystem
 - Designing such cores is not really our research goal
- **Standards of RISC-V will continue to evolve (slowly..)**
 - Standards are discussed openly, this takes time, specifications evolve before being ratified
- **Providing support to all users is not our strength**
 - We try our best, but our main workforce are Ph.D. students that need to do research
 - Get community involved in supporting what we have released so far... and...

Open Titan project



- Open source Root of Trust project led by LowRISC

“OpenTitan is the first open source project building a transparent, high-quality reference design and integration guidelines for silicon root of trust (RoT) chips”

- Many partners involved



- ETH Zurich has contributed their 32bit RISC-V core (Ibex)



OpenHW Group



OpenHW Group is a not-for-profit, global organization driven by its members and individual contributors where HW and SW designers collaborate in the development of open-source cores, related IP, tools and SW such as the CORE-V Family of cores.

- **OpenHW has taken over and is supporting RI5CY and Ariane**
 - Better verification, documentation, user support, unfortunately horrible names.
- **More to come, many active partners working on improvements**

Open HW group members



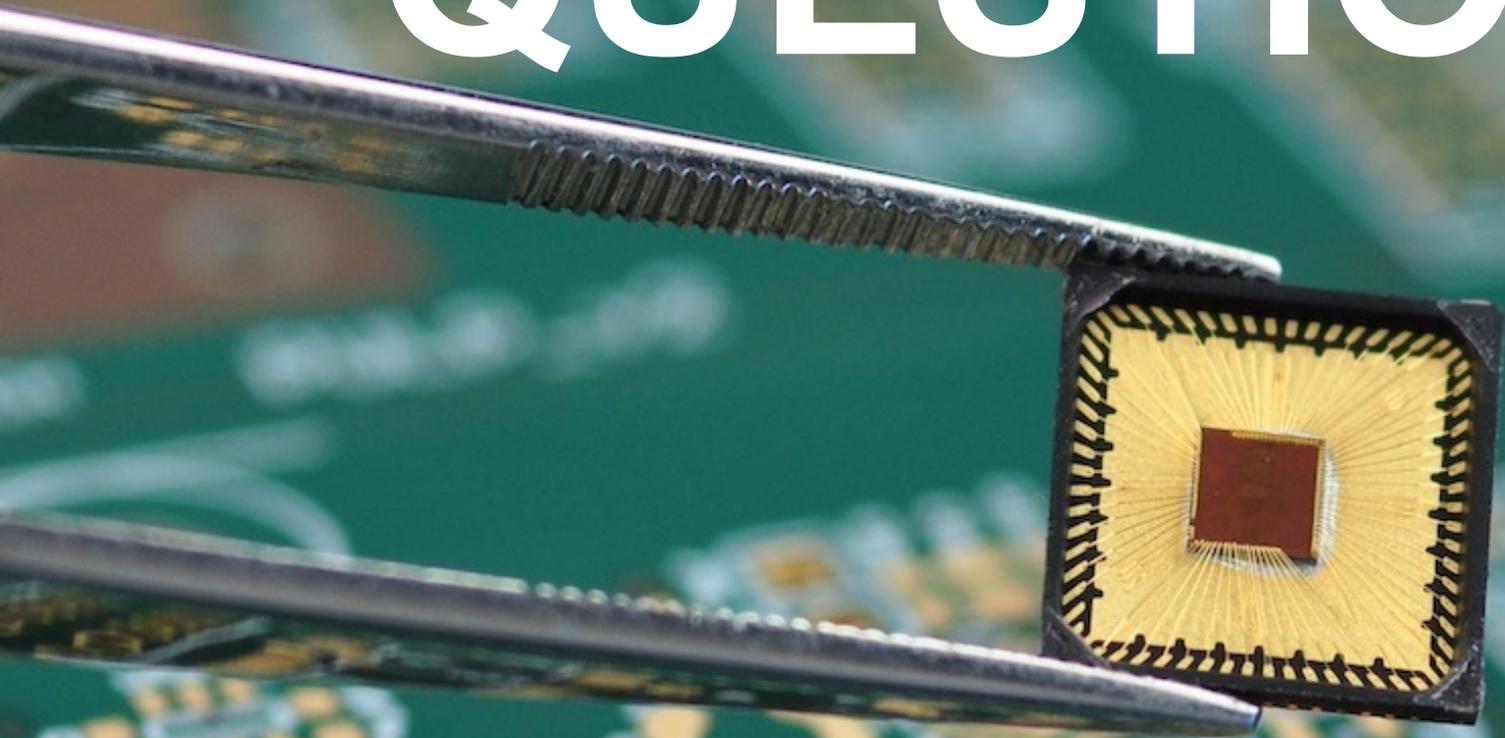
Open source HW is a great tool for security

- **Investigate, observe, change and share**
 - Great toolbox to test and validate ideas, develop new concepts
- **Platforms with good maturity (and great price/performance)**
 - Huge effort by industry supported non-profits to getting additional manpower to make it even better underway
- **Permissive licensing does not put burdens on commercialization**
- **Access our releases through GitHub**



https://github.com/pulp_platform

QUESTIONS?



@pulp_platform
<http://pulp-platform.org>