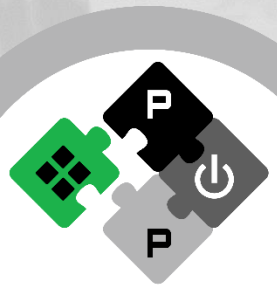


How PULP-based Platforms are Helping Security Research

HPCA 2018 - Barcelona

9.May.2018

Frank K. Gürkaynak

Integrated systems laboratory, ETH Zürich

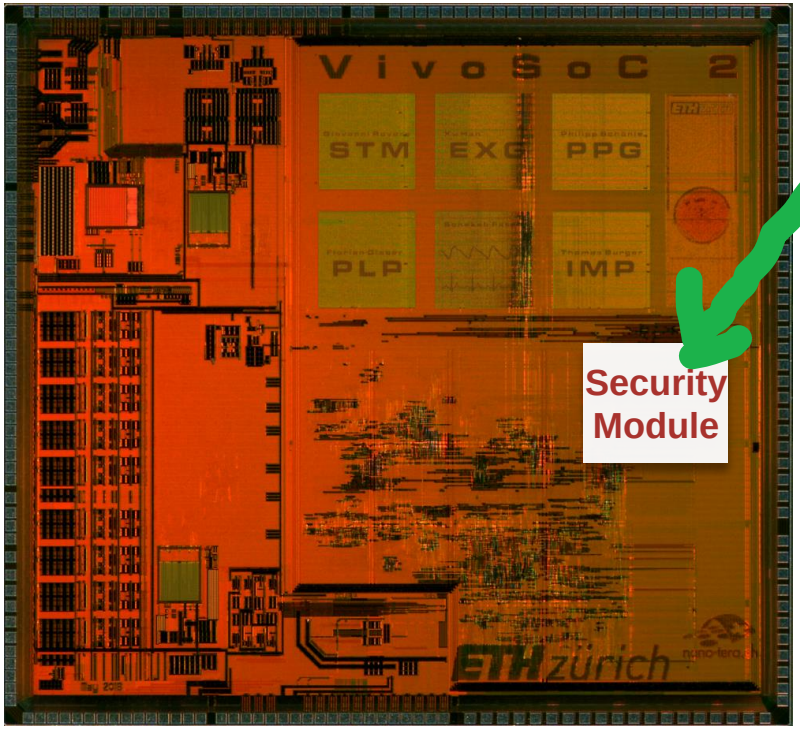
Stefan Mangard

Institute of Applied Information Processing and Communications, TU Graz

Our digital world relies on our ability to secure systems

- **We have to make sure that our data is**
  - Not lost
  - Manipulated
  - Or become visible to parties that are not supposed to have access
- **Therefore we rely on security services such as**
  - Confidentiality
  - Authentication
  - Integrity…
- **But bad guys and problems do not play by the rules**
  - New ideas and attacks to circumvent security services appear daily
  - **Attacks do not** always **come from places** where **we expect** them
  - Active research effort is needed **to keep ahead** of the ‘bad guys’

The entire system needs to be considered for security



VivoSoC2, Biomedical signal Acquisition SoC, SMIC130, 4.7mm x 4.7mm
http://asic.ethz.ch/2016/Vivosoc2.html

https://meltdownattack.com/

- Security of the system is not limited to "one part"
- Recent attacks have demonstrated this to everyone

PULP

IAIK TU Graz ETH

Current HW only supports security through obscurity

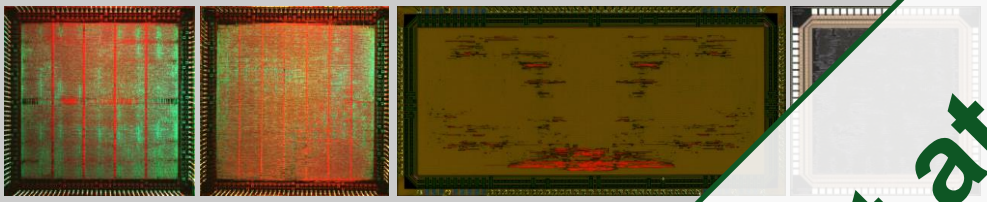
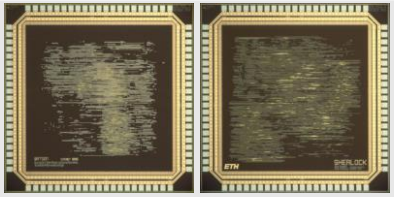
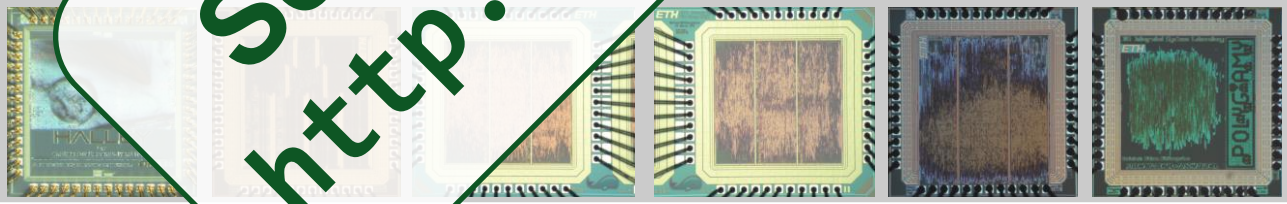
- **Hardware is a critical for security, we need to ensure it has no holes**
  - Being able to see what is really inside will improve security
- **An open approach has proven itself in SW Why should HW be any different?**
  - If you really want, you can still 'obscure' HW, but open HW gives you a choice!
  - Many bugs, **features with unintentional consequences** can hide inside HW
- **Open HW will allow a larger community to verify building blocks**
  - Better verification, more reliable hardware

RISC-V open systems are an asset for security research

- Open ISA standard, ongoing work on security extensions
- An architecture that is up to date and relevant
- Already used by many, potential to be one of the prevalent architectures

- Complete openly available systems based on RISC-V
- Written in System Verilog
- Offers interesting opportunities for extensions and accelerators.

ETH Zürich has a rich history in Cryptographic Hardware

AES	
E-Stream	
SHA-3	
CEASAR	
ECC	

See complete list at http://asic.ethz.ch

PULP

IAIK TU Graz ETH

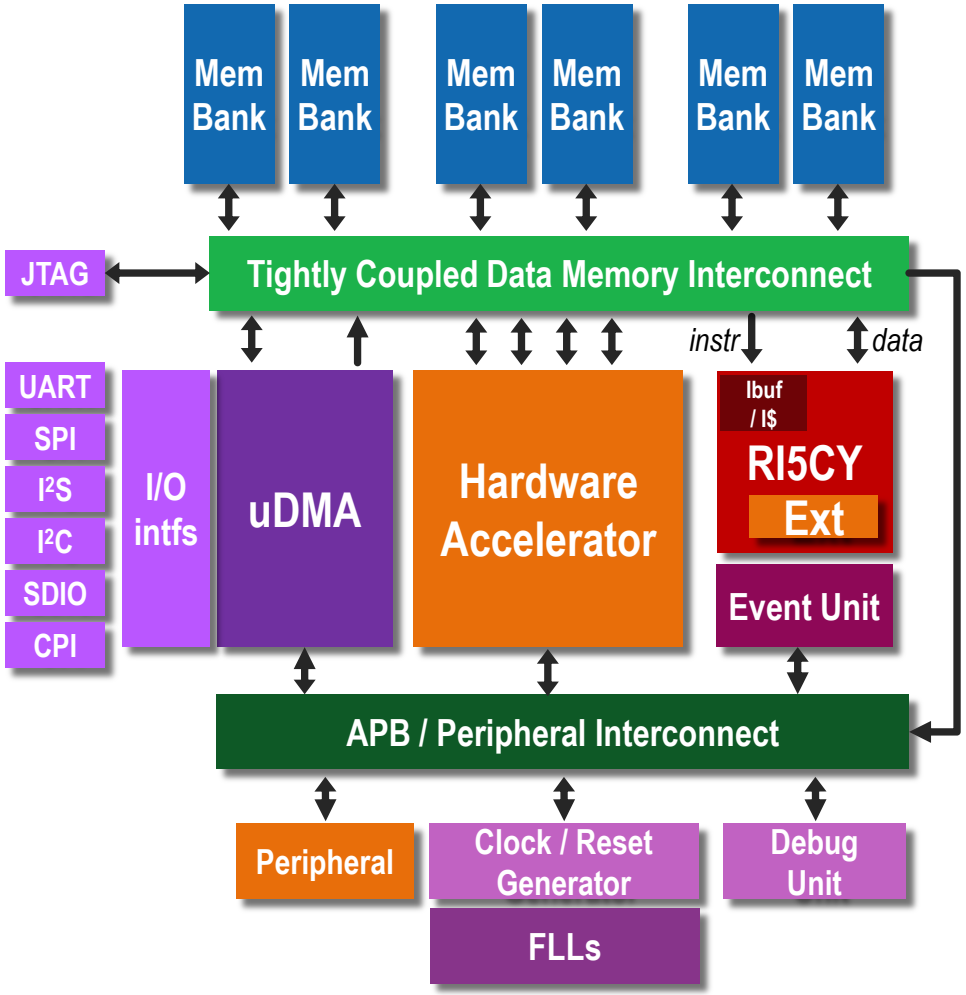
Key challenge: get enough data for your crypto units

- **Cryptographic accelerators when examined alone can easily**
  - Reach Multi-Gbit throughput
  - Occupy small area (tens of kGE)
  - Achieve excellent numbers in **throughput** per **mm^2** per **Watt** (or any other metric)
- **Example Trivium (stream cipher from e-Stream):**
  - Achieves more than **18 Gbit/s** throughput
  - Occupies a bit more than **6 kGE** (0.145mm^2)
  - In a (now) very old **250nm technology**
- **But how do we get so much data in and out of there?**
  - Need to **couple** accelerator to the rest of the system **efficiently**

F.K Gürkaynak, P Luethi, N Bernold, R Blattmann, V Goode, M Marghitola, “Hardware Evaluation of eSTREAM Candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, ZK-Crypt”, eSTREAM: the ECRYPT Stream Cipher Project 15, 2006

PULP provides multiple opportunities to add extensions

- **Typical PULPissimo system**
  - Similar organization for multi-core
- **Adding new instructions**
  - Directly implemented in core
- **Peripherals to the APB bus**
  - Standard interface
- **HW Accelerators with direct memory access**
  - Best performance
  - Programmed through APB bus
  - Number of TCDM access ports determines max. throughput

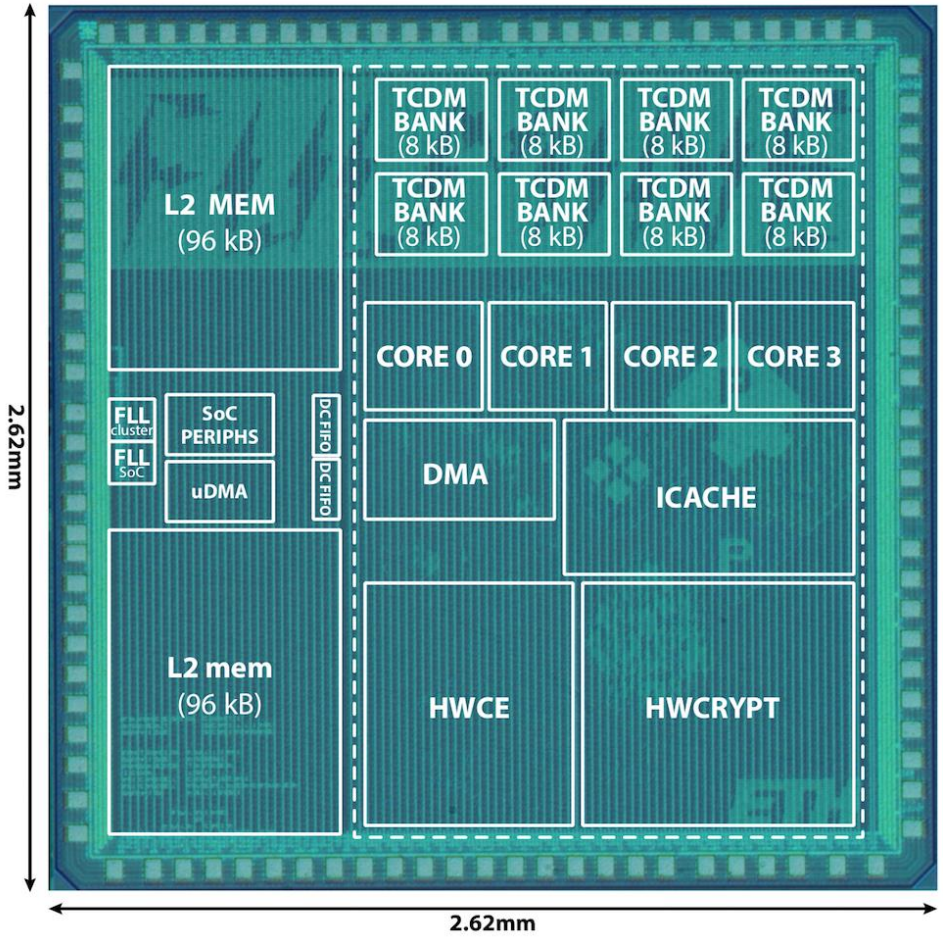


PULP

IAIK TU Graz ETH

Fulmine: Our IoT processor with accelerators

- **Implemented in UMC 65nm**
  - 2 TCDM ports 64 bits/cycle
- **AES unit (2 rounds/cycle)**
  - Supports, ECB, XTS modes
  - 0.38 cpb (8 kByte block)
  - @0.8V and 84 MHz
    - 1.76 Gbit/s
    - 120 pJ per byte (entire chip)
- **Other features**
  - SHA-3 based authenticated encryption (3 rounds/cycle)
  - Leakage resilience (see next slides)
  - HW Convolution Engine for NN.

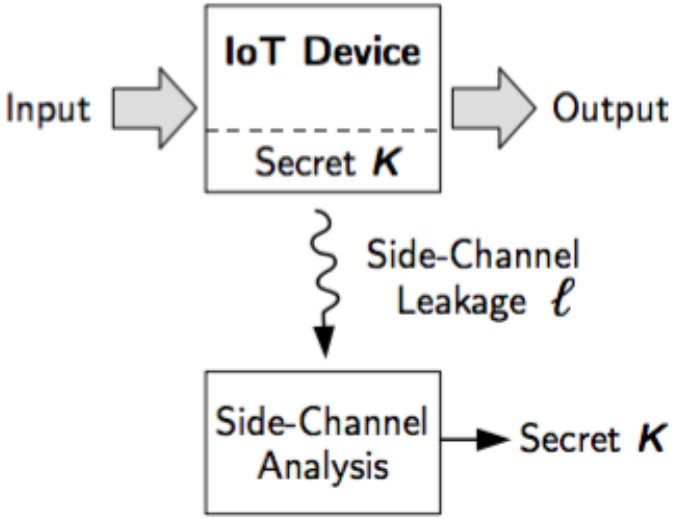


F. Conti et al., "An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 64, no. 9, pp. 2481-2494, Sept. 2017.

PULP IAIK TU Graz ETH

Side channel attacks are a major problem for security

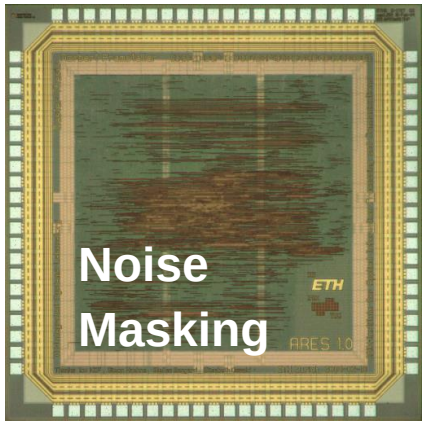
- **Once an otherwise secure algorithm is implemented it gets physical properties**
  - Power consumption
  - Electromagnetic radiation
  - Differences in execution speed
  - Memory/cache footprint

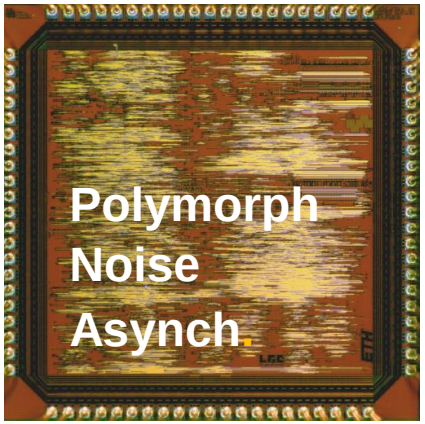


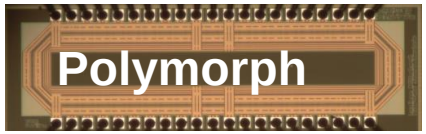
- **Measurements on implementations may leak additional information**
  - Attacks are successful if measurements reveal secrets of the algorithm
  - Rely on many measurements and statistics
  - Many are non invasive, cheap to implement, surprisingly effective
  - Does not always need physical access to the device (remote timing attacks)
- **Difficult to counter, algorithmically they do not exist**

Research at ETH Zürich against side-channel attacks

- **Power by far the most common side-channel attack for CMOS**
  - Power consumption of CMOS gates depends on its operands.
- **To protect yourself you can try to:**
  - Add **noise** to make measurements difficult
  - Implement **masking**/**sharing** techniques to de-correlate secrets from input data
  - Change the way the operation is organized randomly (**polymorphism**)
  - Use **digital logic** with circuit **styles** that have (less) data dependent consumption





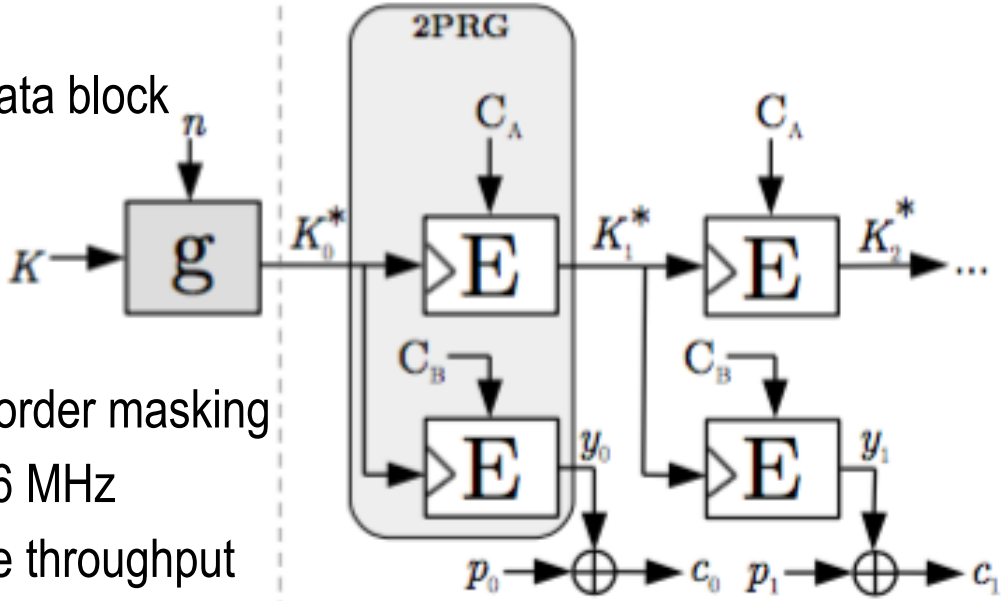


PULP

IAIK TU Graz ETH

Leakage Resilient Cryptography in a PULP accelerator

- **Reduce Attack surface**
  - A new key (**K***) is generated per data block
- **Encryption example**
  - Based on 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



- **Demonstrated that strong side channel resilience within power budget of IoT Systems**
  - Implemented and tested in **Fulmine** (from earlier slides)
  - Also includes a solution for Authenticated Encryption

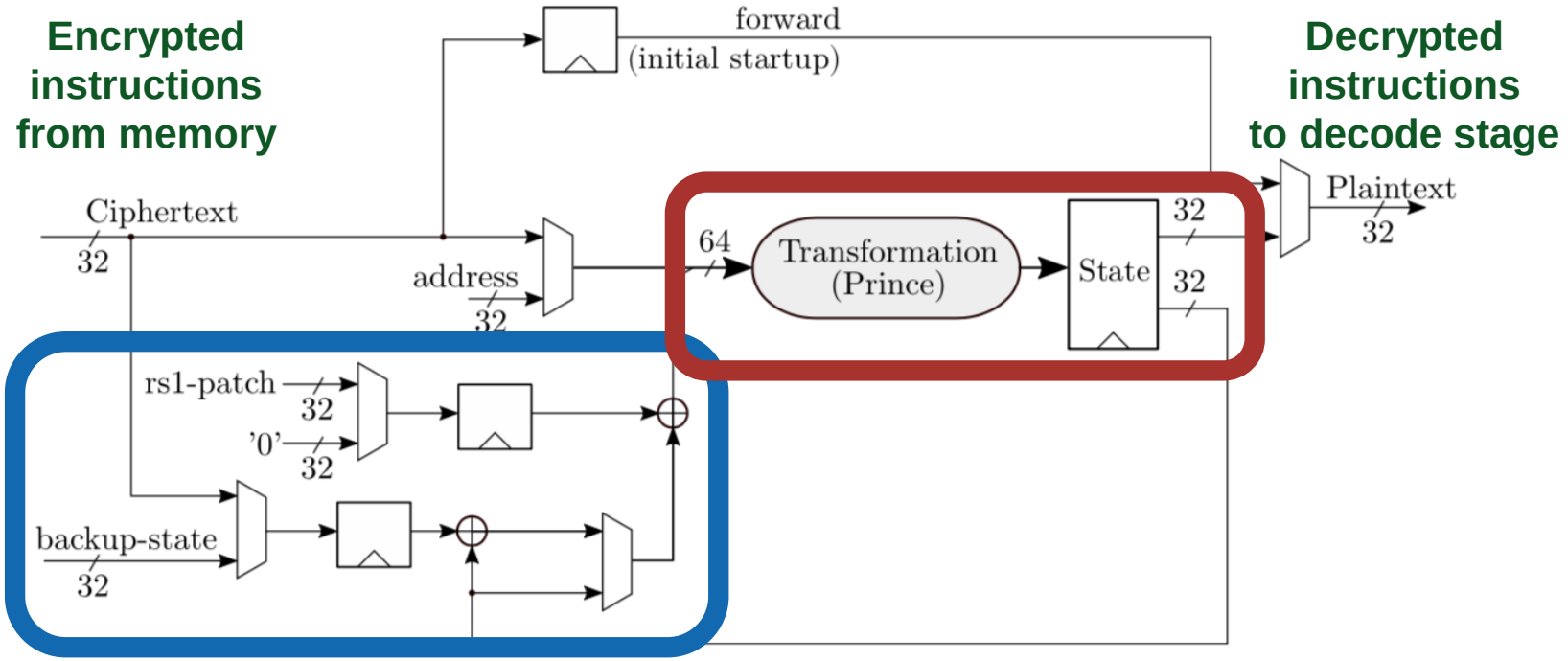
Robert Schilling, Thomas Unterluggauer, Stefan Mangard, Frank Gürkaynak, Michael Muehlberghuber, Luca Benini, "High-Speed ASIC Implementations of Leakage-Resilient Cryptography", DATE 2018

PULP IAIK TU Graz ETH

Attacks that target the control flow are a serious problem

- **Can be realized in both HW and SW**
  - A successful attack on a processor changes the order of executed instructions
  - Can be used to execute malicious code
  - Jump over security checks
- **HW attacks can be realized by controlling environment**
  - Clock or voltage glitches
  - Injecting electromagnetic pulses
- **Small IoT devices more vulnerable**
  - They operate in potentially hostile environment
  - Have less resources to withstand attacks from a capable adversary

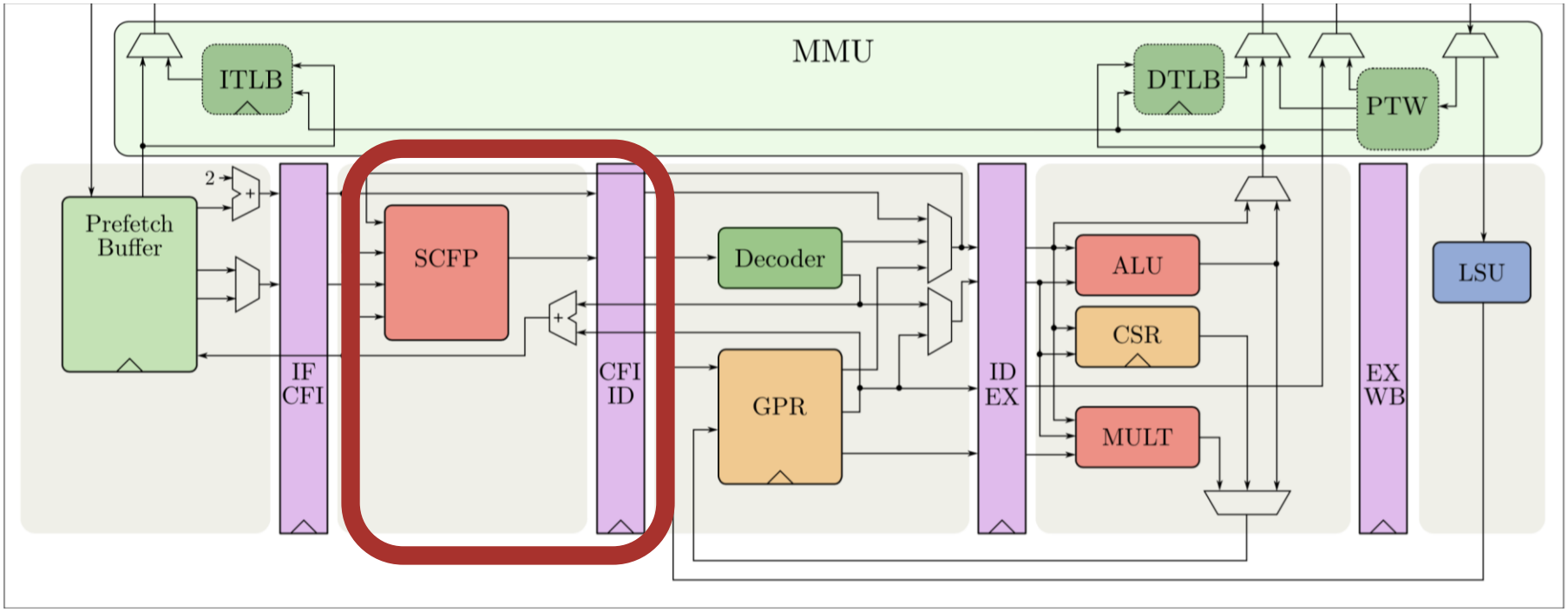
Sponge based control flow protection (SCFP)



- Sponge based construction to decrypt **instructions**
  - AEE Light with 32 bit **state** and 32 bit capacity in APE mode
  - Used **Prince** for permutation allowing single cycle execution
- **Attacker** needs to **change** both instruction and **state** simultaneously
- Possible to add '**patch**' values for branches and function calls

PULP IAIK TU Graz ETH

Modified RI5CY core (REMUS) with Control Flow Integrity

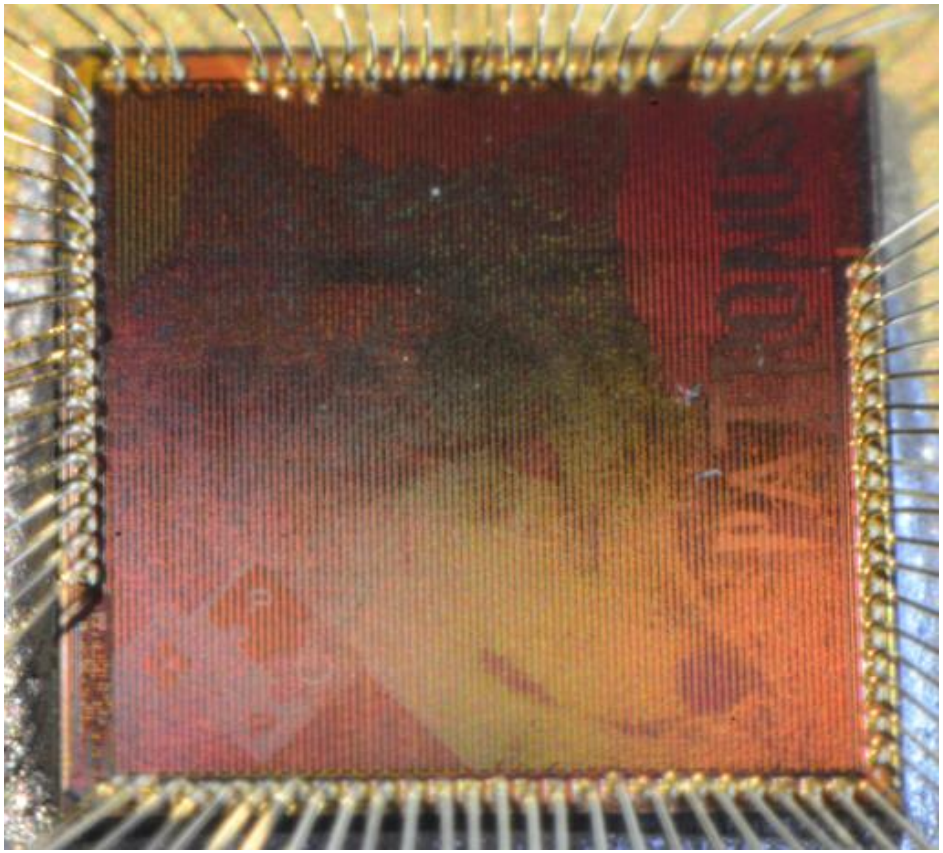


- One **additional pipeline stage** (SFCP)
- Instruction is decrypted with the '**State**' of the Sponge prior to decode
- '**State**' is updated with every instruction and used to **decode** next one
- Modification to execution flow will quickly result in illegal instructions

PULP IAIK TU Graz ETH

Patronus: PULPissimo chip with Control Flow Integrity

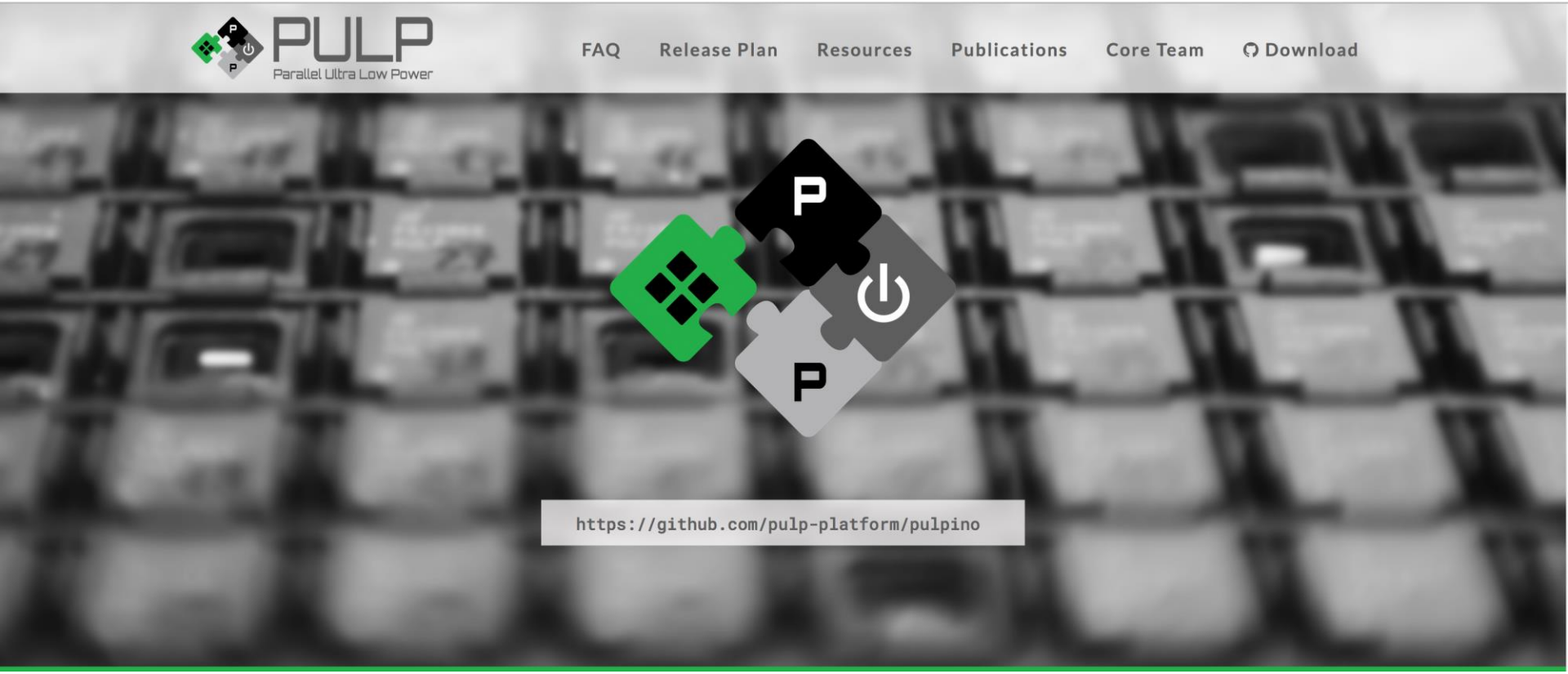
- Implemented in UMC65nm
  - Chip back and tested
- Only 25-35% power/area overhead
- **Additional instructions** for branches added as instruction set extensions
- About 10% runtime overhead due to patches and additional commands
- Probability of **illegal instruction trap** when instruction altered
  - 91.51% within 1 cycle
  - 99.19% within 2 cycles
  - **99.95%** within 3 cycles
- Supports **privilege spec** 1.9.1
- Ported **SeL4** to run on Patronus



Publication with TU-Graz in preparation

PULP IAIK TU Graz ETH

Open source HW is helping security research, join in!

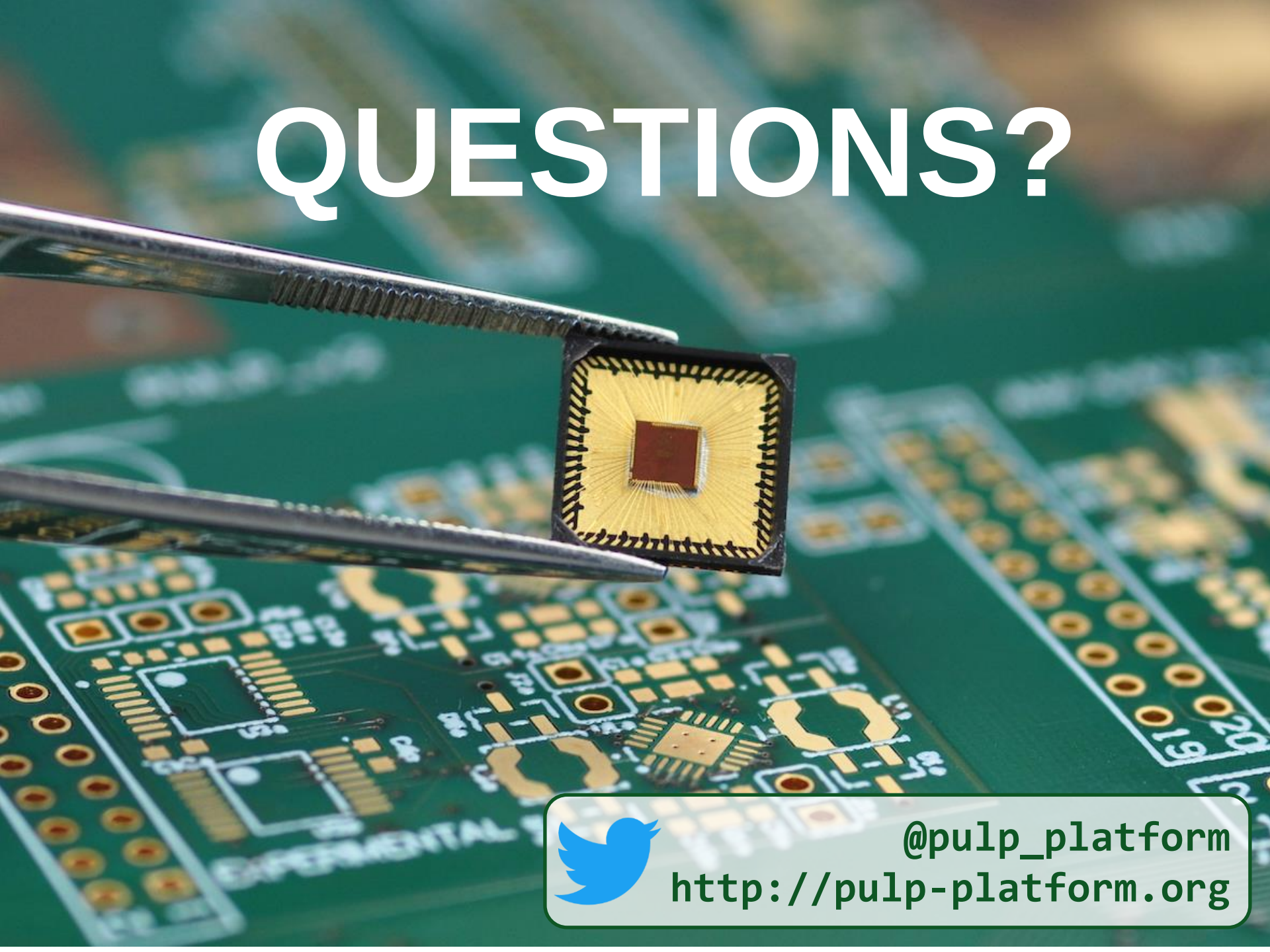


Download our PULP systems from our GitHub page

https://github.com/pulp-platform

PULP

IAIK TU Graz ETH


QUESTIONS?
@pulp_platform
http://pulp-platform.org

Reserve slides

Finally for HPC applications we have multi-cluster systems

RISC-V Cores

- RI5CY 32b
- Micro riscy 32b
- Zero riscy 32b
- Ariane 64b

Peripherals

- JTAG
- SPI
- UART
- I2S
- DMA
- GPIO

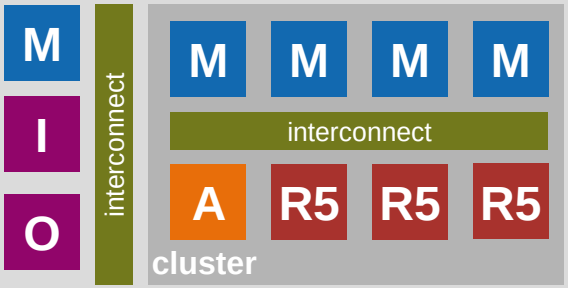
Interconnect

- Logarithmic interconnect
- APB – Peripheral Bus
- AXI4 – Interconnect

Platforms

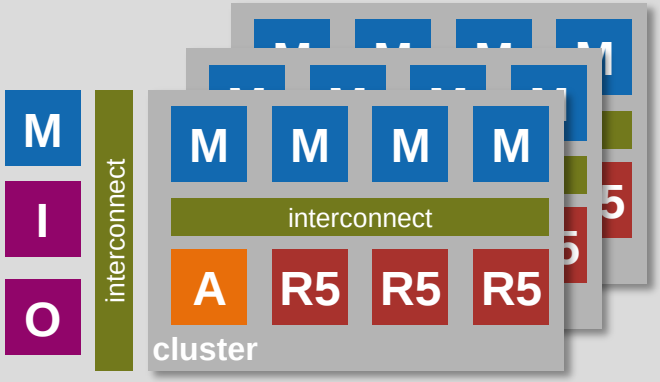
Single Core

- PULPino
- PULPissimo



Multi-core

- Fulmine
- Mr. Wolf



Multi-cluster

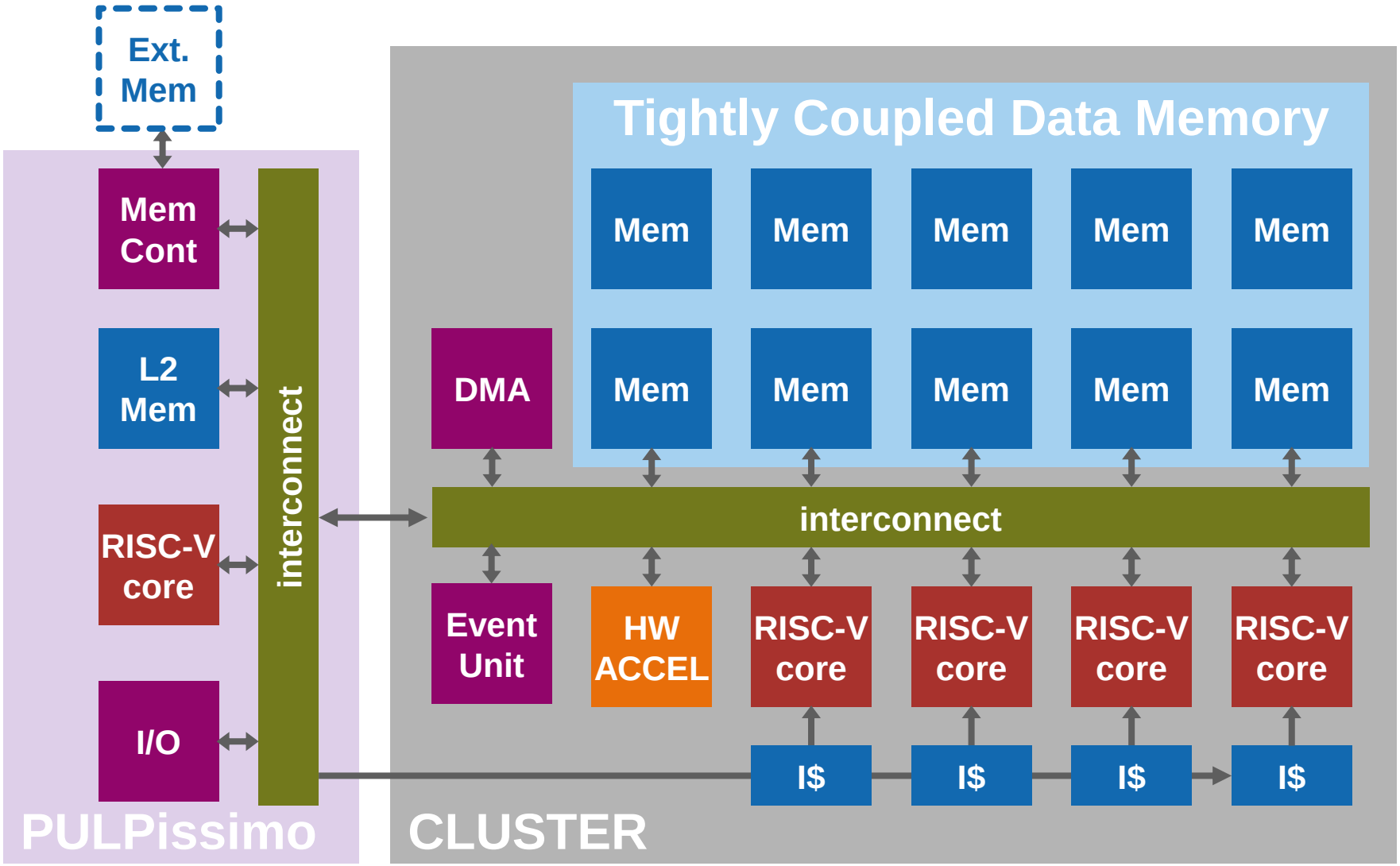
- Hero

IOT → HPC

Accelerators

- HWCE (convolution)
- Neurostream (ML)
- HWCrypt (crypto)
- PULPO (1st order opt)

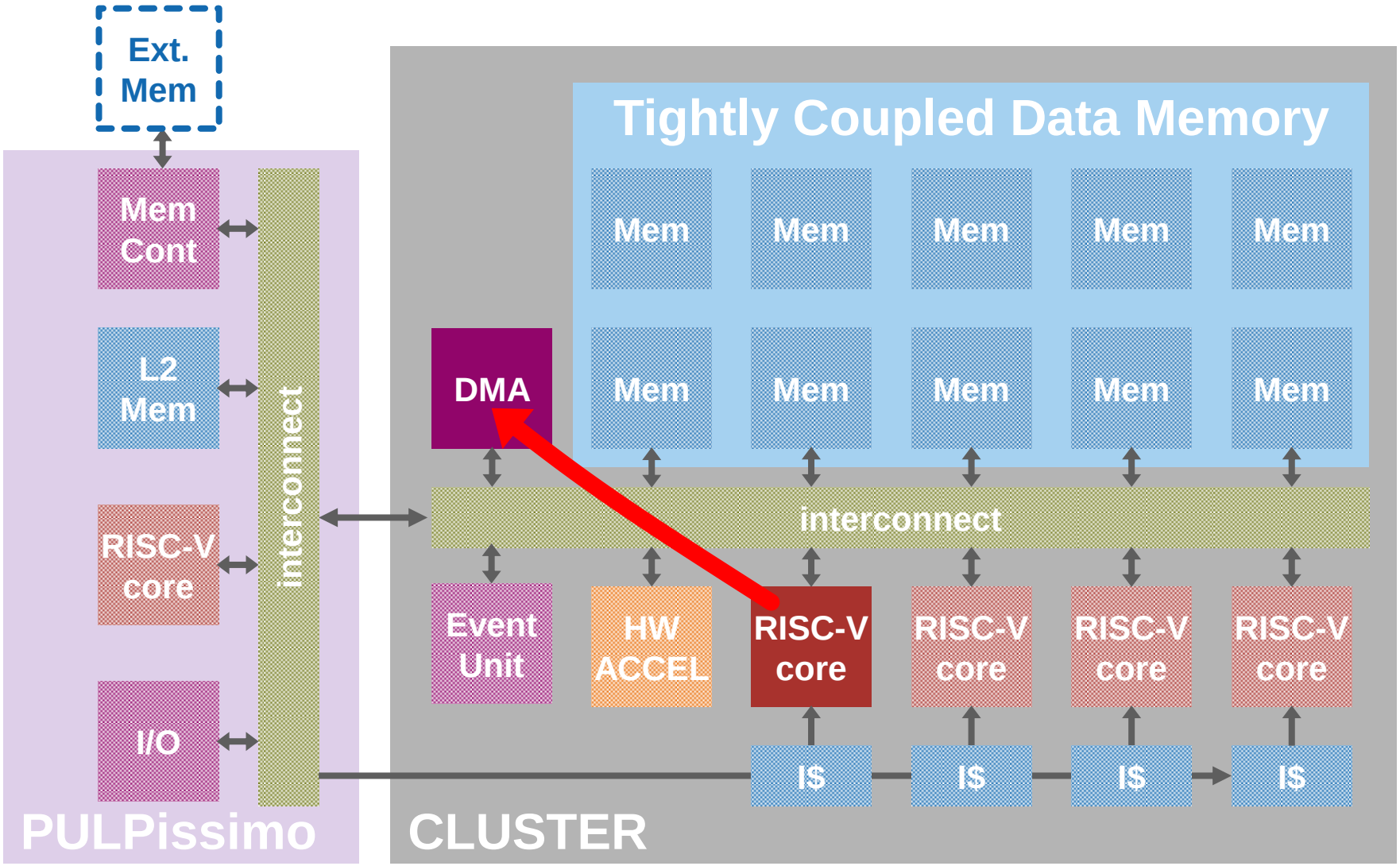
An additional microcontroller system (PULPissimo) for I/O



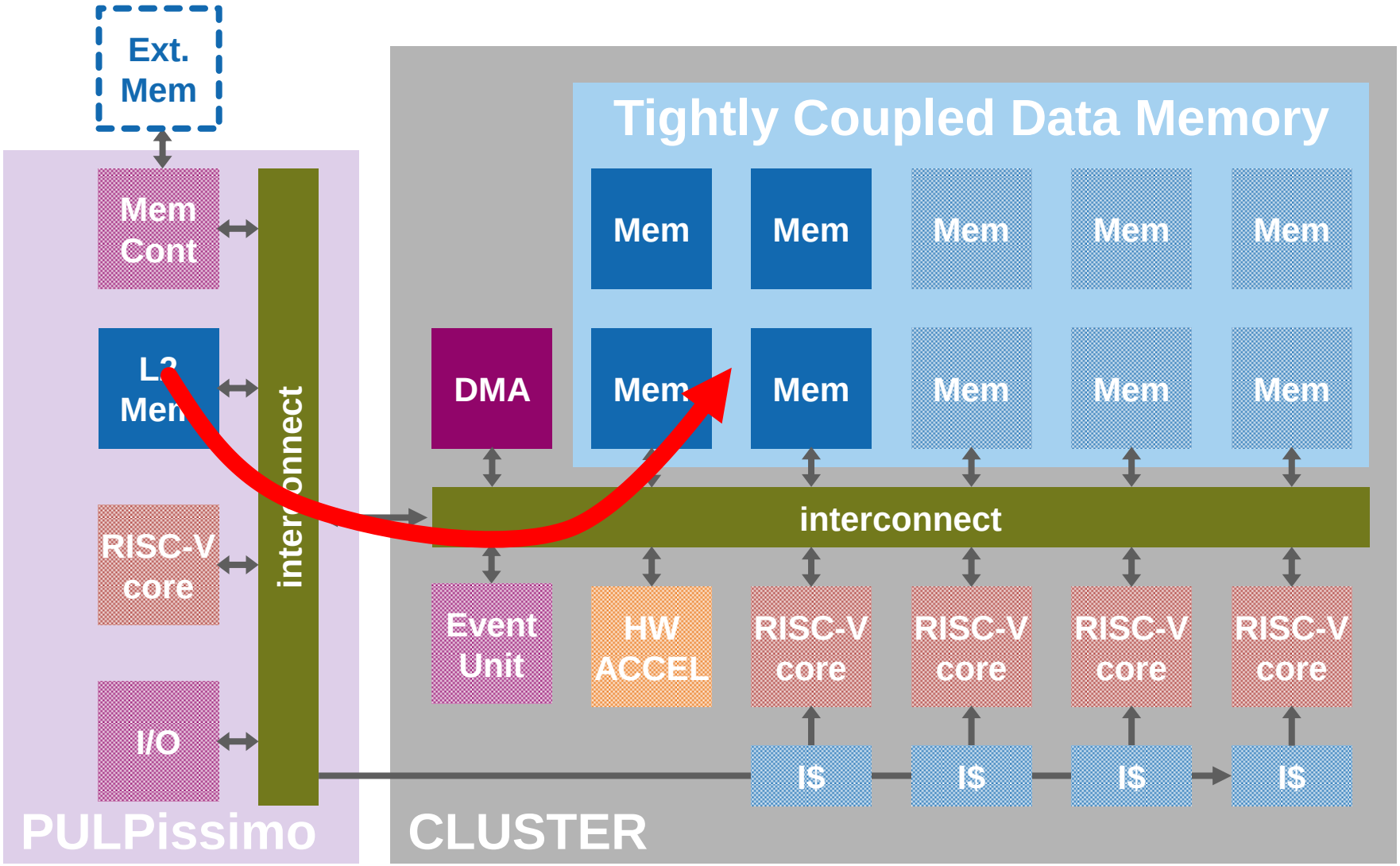
PULP

IAIK TU Graz ETH

How do we work: Initiate a DMA transfer



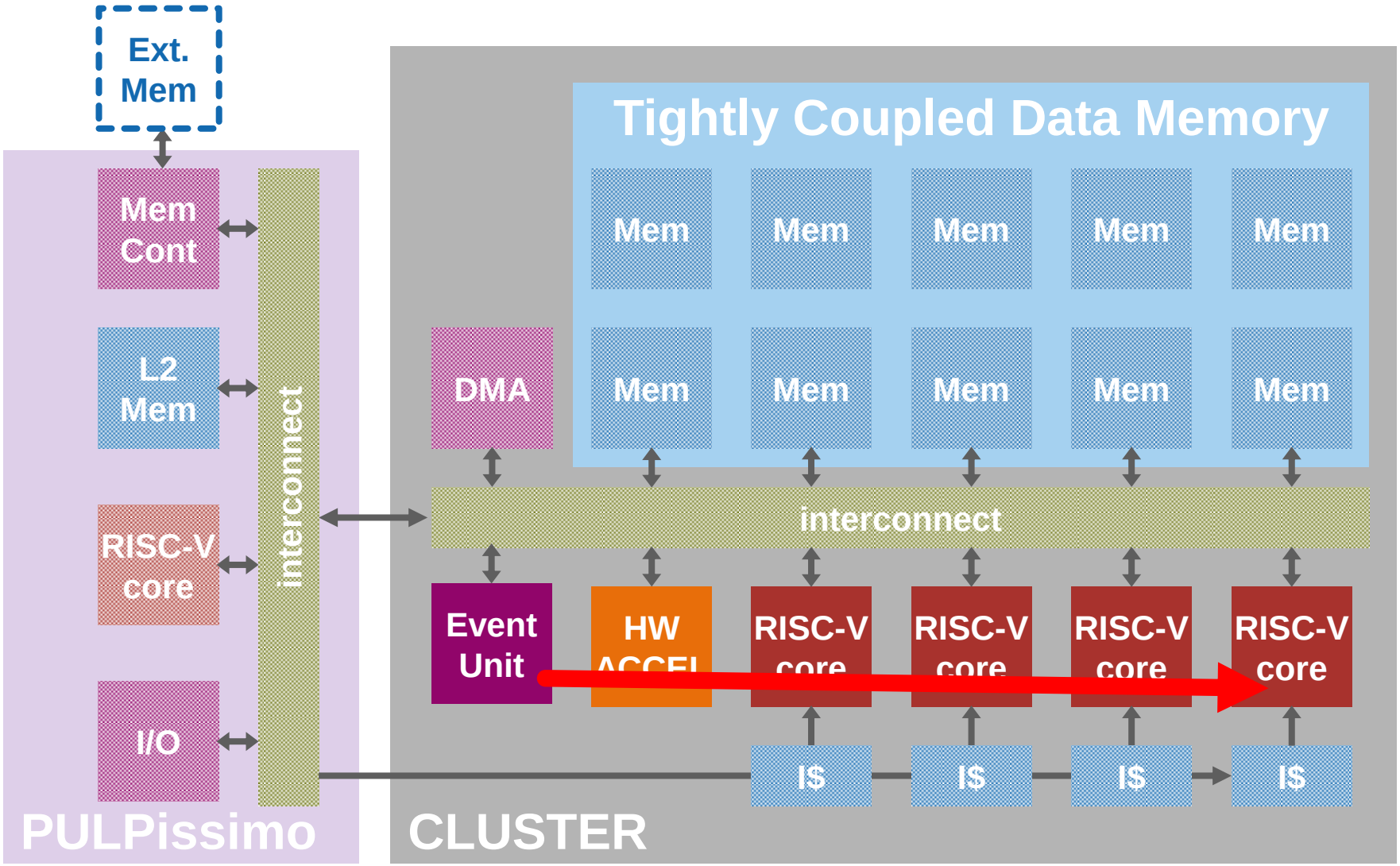
Data copied from L2 into TCDM



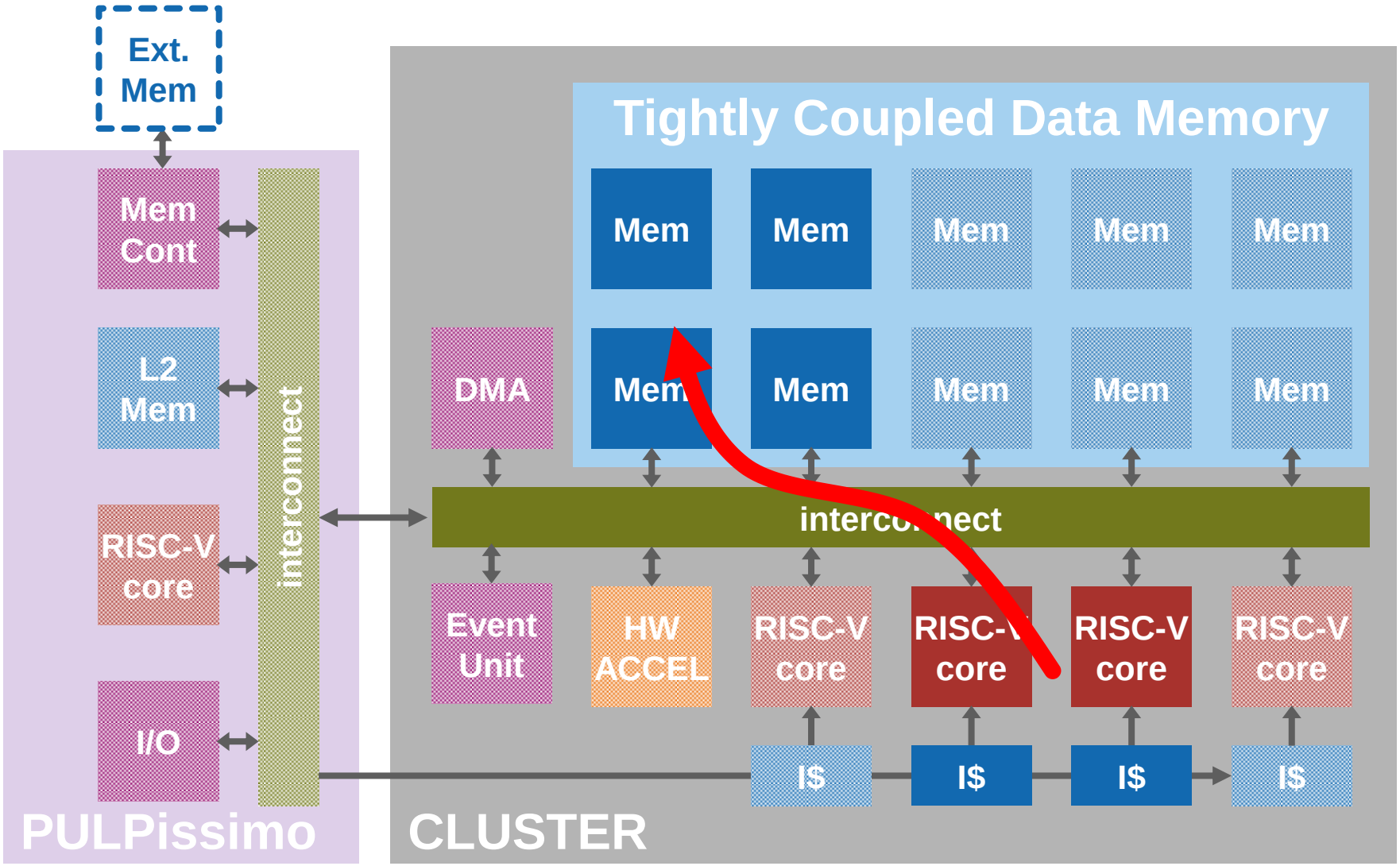
PULP

IAIK TU Graz ETH

Once data is transferred, event unit notifies cores/accel



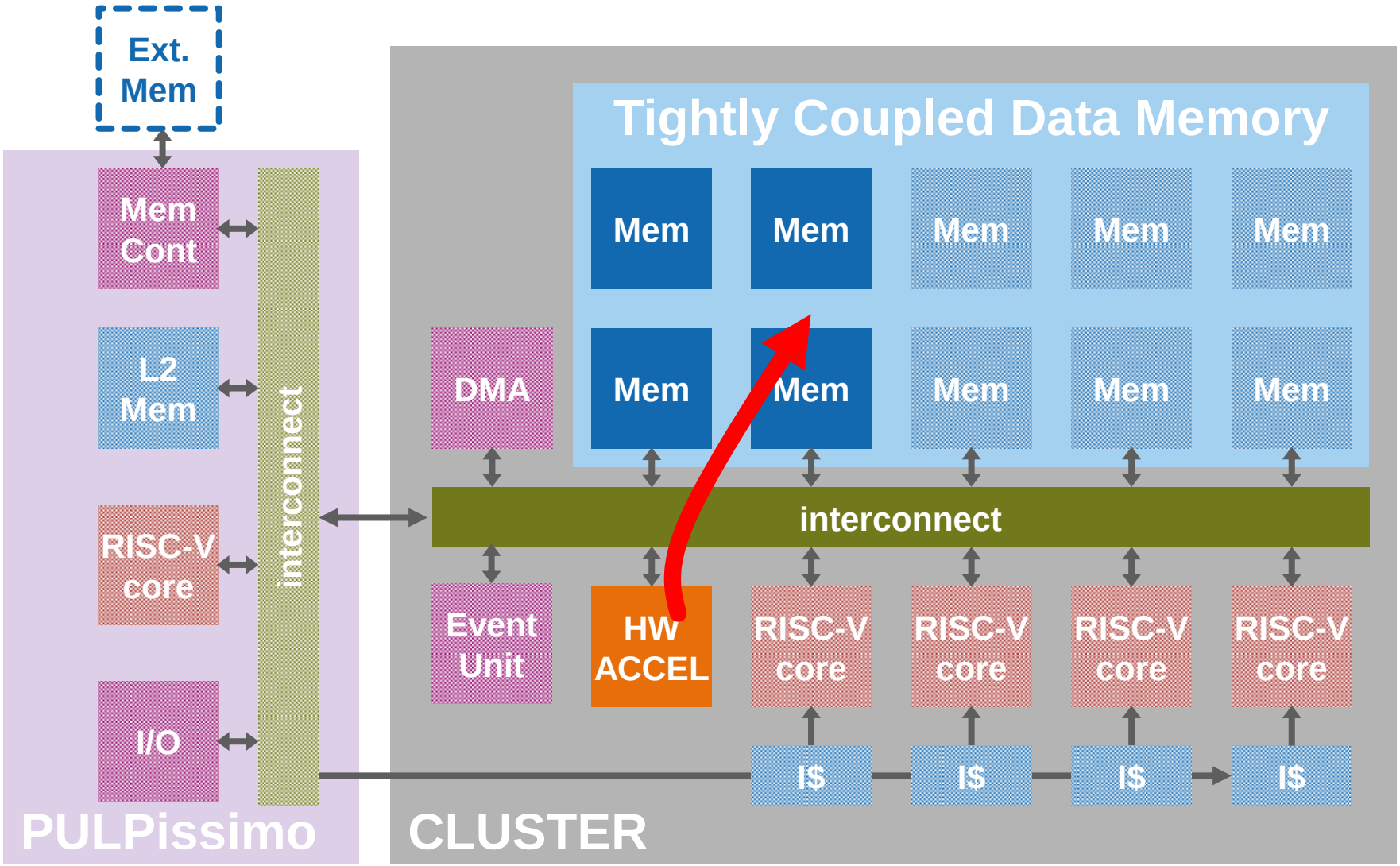
Cores can work on the data transferred



PULP

IAIK TU Graz ETH

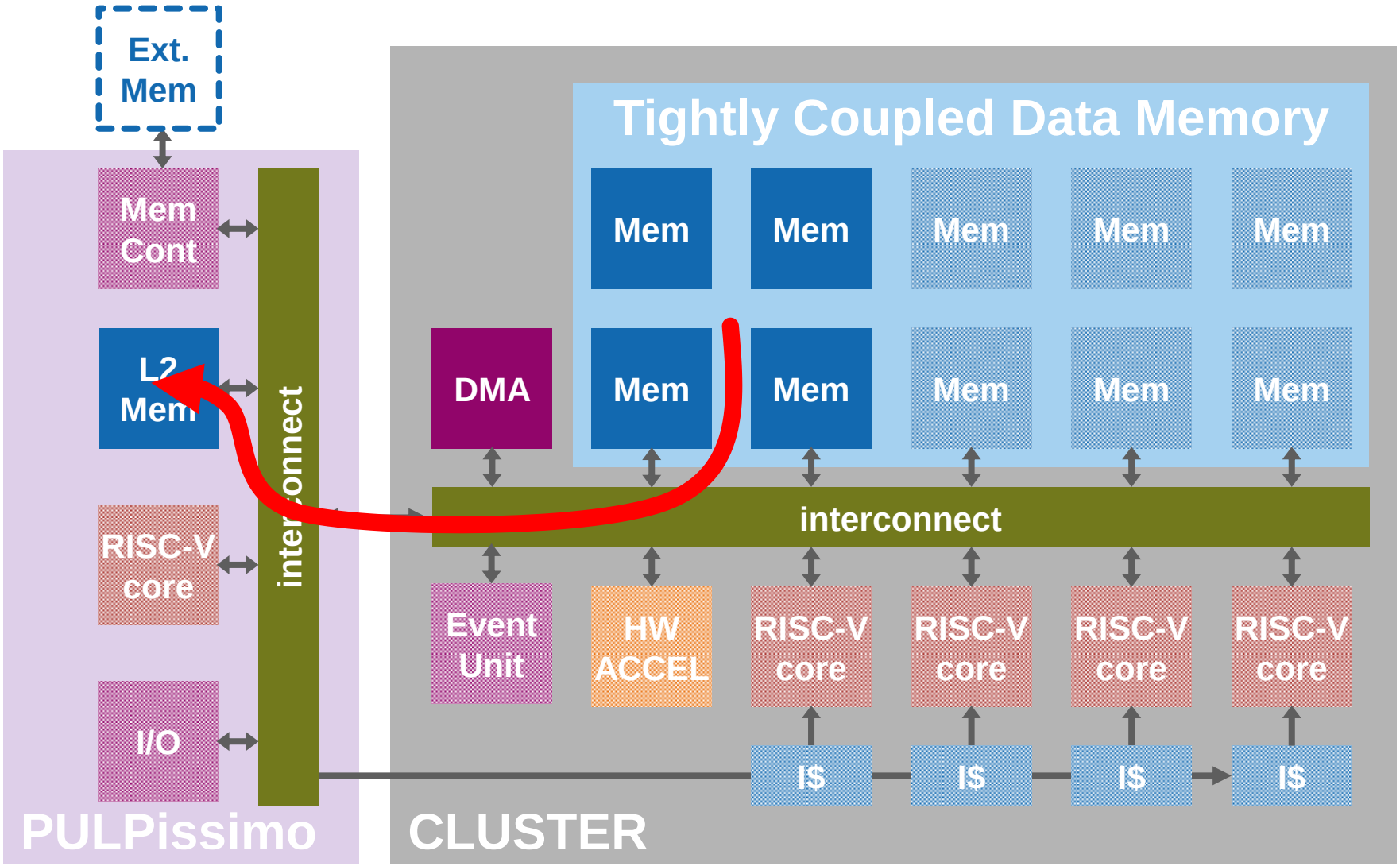
Accelerators can work on the same data



PULP

IAIK TU Graz ETH

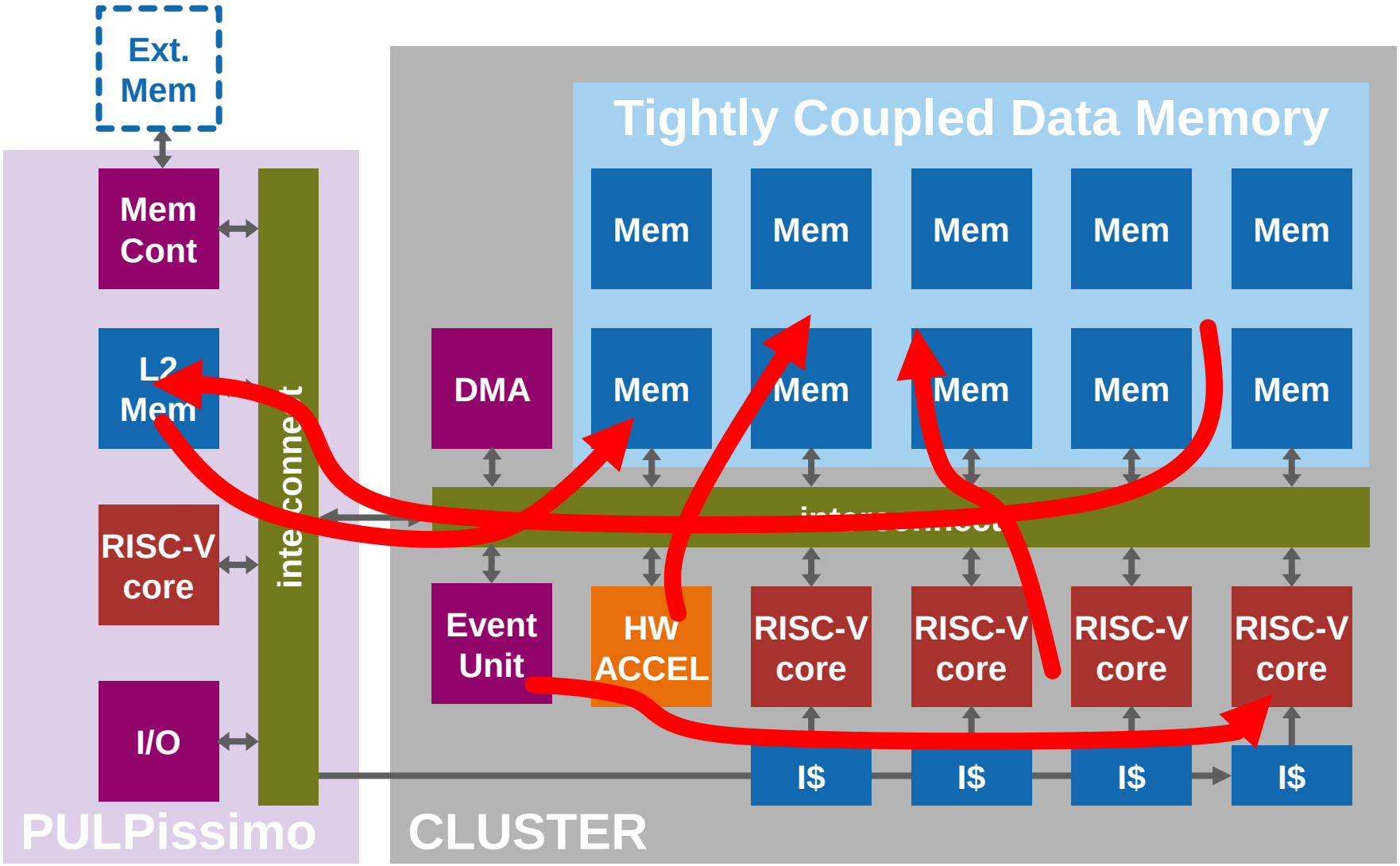
Once our work is done, DMA copies data back



PULP

IAIK TU Graz ETH

During normal operation all of these occur concurrently



PULP

IAIK TU Graz ETH