

KU LEUVEN





HW implementation challenges for post-quantum cryptography on Cyber-Physical-Systems

Prof. Dr. Ir. Ingrid Verbauwhede
CSP, Alghero, Italy
September, 2026



Belfort

Slide acknowledgement: All past and present PhD students!
 Special acknowledgement: Thomas Pönnelmann, Bart Preneel



Ingrid Verbauwhede

KU LEUVEN



- Professor KU Leuven (UCLA)
- Research group COSIC: birth of AES
- IEEE, IACR fellow
- 2x ERC advanced grant: CATHEDRAL, BELFORT

“Hardware Acceleration for Computing on Encrypted Data”

- IEEE SSCS Pederson Award, 2023 *for pioneering contributions to energy-efficient and high-performance secure integrated circuits and systems.*
- 2025 FWO excellence award

UCLA



Belfort

Belfort

Belfort

KU LEUVEN

Research topics at COSIC – HARDWARE

- Implementation challenges of next generation cryptography
 - **Post-quantum** cryptography
 - Efficient, secure, attack resistant
- **Confidential compute: weakness**
 - Badram.eu
 - BatteringRam.eu
 - DDROP
- **Computing on Encrypted Data**
 - Hardware acceleration
 - Fully Homomorphic Encryption
 - ERC Belfort
- **Circuits and technology**
 - TRNG, PUFs



3



Belfort

KU LEUVEN

Outline

- (Symmetric and) Public Key cryptography
- Link to quantum computers
- Side note: Quantum Key Distribution: technology looking for a problem
- Post-quantum cryptography
 - Standardization efforts
 - Implementation challenges
- Post-quantum secure computing on encrypted data
- Conclusions



4



Belfort

KU LEUVEN

Introduction: symmetric key

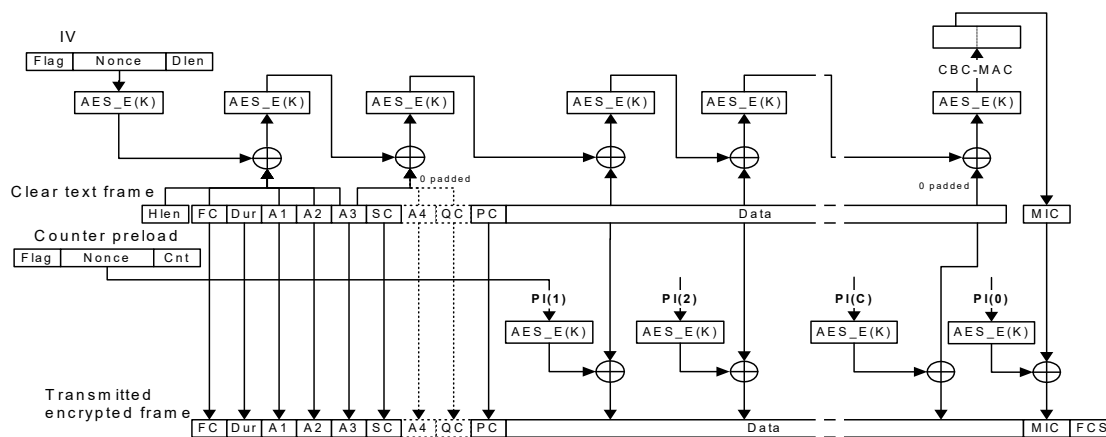
- Alice and Bob SHARE a secret key
- Alice and Bob trust each other
- “Out of band” beforehand exchanged the key
- Used for high throughput and performance
- (Simplified view)



[Alice and Bob, copied from B. Preneel]

Example: CCM (Counter + CBC MAC) mode

- Encryption & MAC creation (802.11 WLAN)
- MIC = Message Integrity Check is same as MAC



Public-key cryptography

- Digital signatures
 - Digital fingerprint for an electronic document or message
 - Public key for verification and private key to sign
 - Proves who signed it and that the message wasn't changed
- Public-key encryption
 - Allows sending a secret message without sharing a secret key first
 - Public key for encryption and private key for decryption



[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum



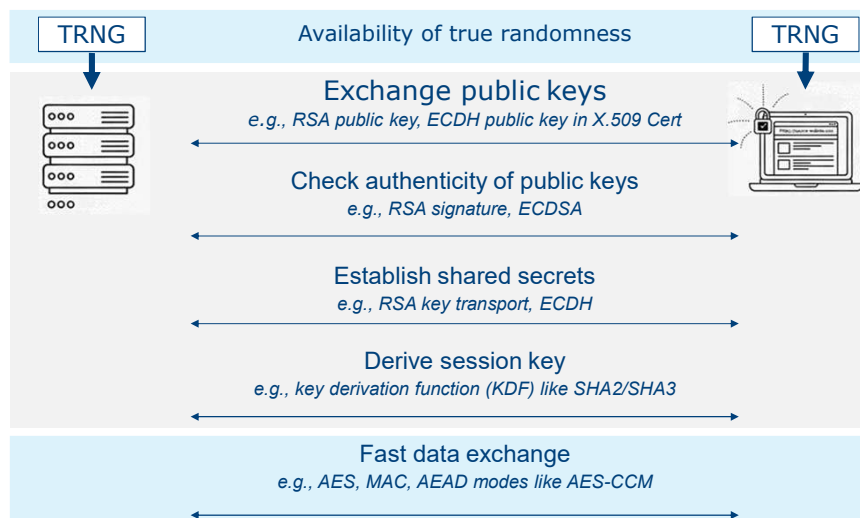
KU LEUVEN

Use Case 1: Simplified key exchange

- Analog part
(not in scope)

- Challenge
 - Latency
 - Complexity
 - Agility
 - Caching

- Challenge
 - Throughput



[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum



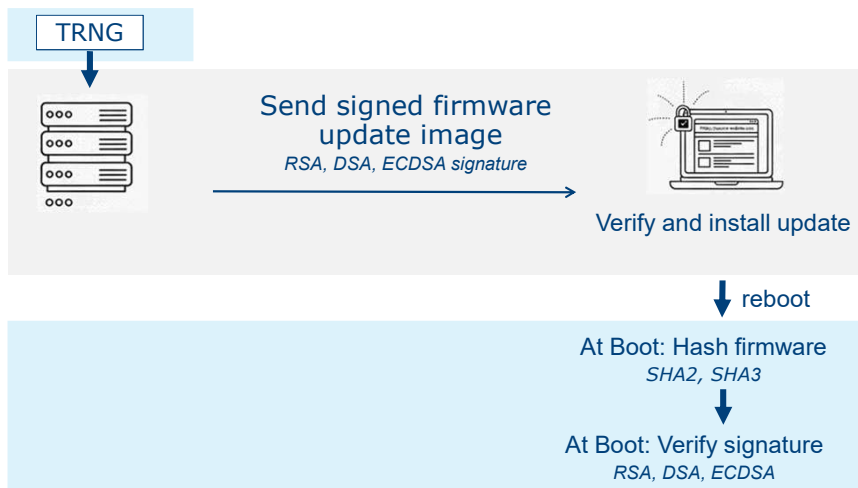
KU LEUVEN

Use Case 2: Secure Boot

- Analog part
(not in scope)

- Challenge
 - Complexity
 - Agility

- Challenge
 - Throughput
 - Parallelism
 - System impact



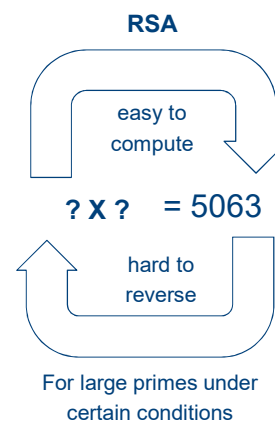
[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum


KU LEUVEN

Security of public-key cryptography

- Cryptographic security is deeply rooted in “one-way-functions”
 - Simple to compute in one direction, but extremely challenging in the reverse
 - **RSA (Rivest–Shamir–Adleman) cryptosystem**: Multiplying two prime numbers is straightforward but factoring the product is hard
 - **ECC (Elliptic Curve Cryptography)**: Hardness of the elliptic curve discrete logarithm problem
- Traditional cryptographic protocols and key lengths are designed to be
 - Efficiently executable on minimal hardware
 - Virtually impossible to break even with the most powerful conventional computing systems



[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum


KU LEUVEN

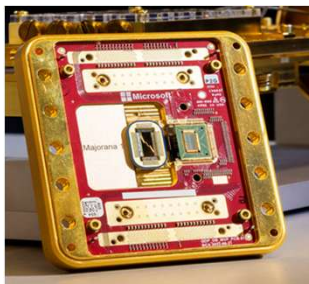
Quantum computing

11

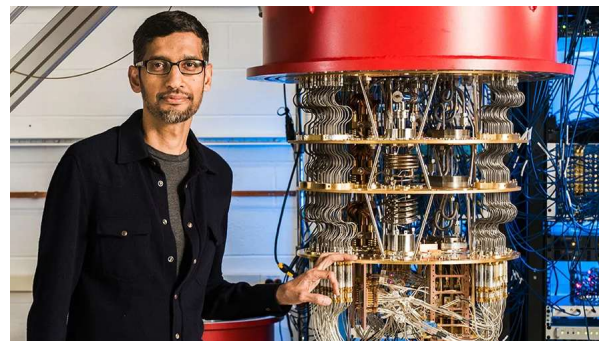


KU LEUVEN

Quantum computing



Microsoft:
Majorana 1,
Feb 2025



Google:
"Willow" Dec 2024

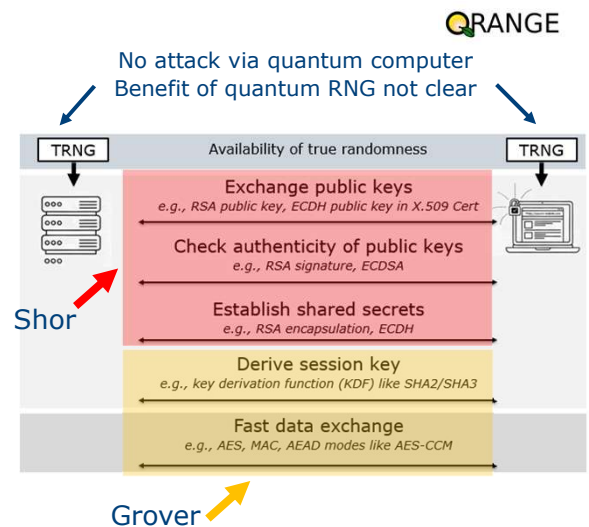
- New technology in development
- Based on principles of quantum mechanics
- Works on superposition of 0 and 1, entanglement
- Extremely efficient for some mathematical problems



KU LEUVEN

A threat to cryptography

- Quantum computers can potentially break current encryption methods using algorithms like Shor's
- Vulnerable encryption algorithms include:
 - RSA (Rivest–Shamir–Adleman)
 - Elliptic curve cryptography (ECC)
- Symmetric schemes (e.g., AES, KDFs) impacted by Grover's but less affected
 - Impact under discussion
 - Mitigated by moving to larger keys (e.g., **AES-256**)



[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum

**KU LEUVEN**

Real or overstated threat?

- Arguments for being real:
 - Shor's algorithm can factor large numbers exponentially faster than classical algorithms
 - Significant progress in quantum computing research and development
- Arguments for being overstated:
 - Current quantum computers are not powerful enough to break
 - Quantum noise and error correction challenges may be blocking ?
- Conclusion
 - Preparation is key: Develop and deploy quantum-resistant cryptographic algorithms to ensure long-term security

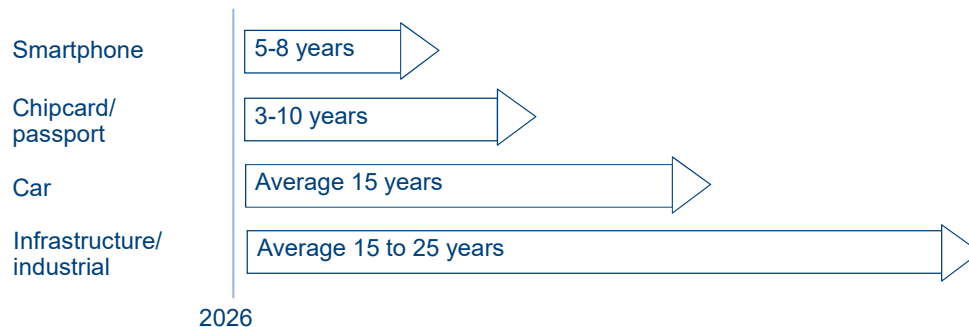
[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum

**KU LEUVEN**

Quantum threat is an engineering issue

- Why is the transition necessary
 - “Store now and decrypt later” attacks
 - Long lifetime of products with semiconductor content



[Thomas Pöppelmann]

Fundamentals of Cryptography for Chip Designers: Classical to Post-Quantum



KU LEUVEN

Sidestep: Quantum Key Distribution

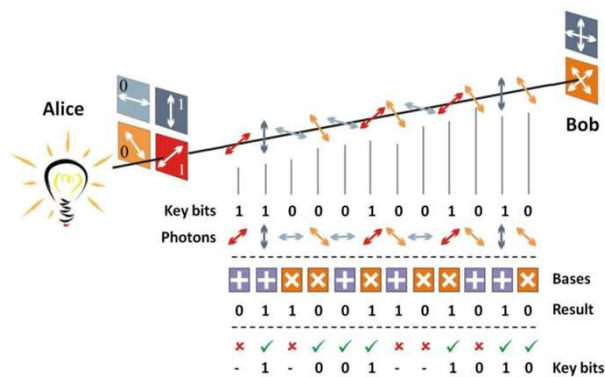
16



KU LEUVEN

Why not Quantum Key Distribution (QKD)?

- Example BB84 protocol



<https://arxiv.org/pdf/1611.03529.pdf>

[Bart Preneel, Nigel Smart]

17



Original Quantum Cryptographic Apparatus built in 1989
transmitted information secretly over a distance of about 30 cm.

Turing Award 2026

Pros and cons

- Pros:
 - Laws of physics rather than mathematics/complexity theory
 - Single photon based: optical communication (via fiber or free-space)
- Cons:
 - Needs authenticated channel for prior shared key (computational security)
 - Too slow: need AES for bulk encryption (computational security)
 - Limited distance: Quantum repeaters



Trusted node

Trusted node



[Bart Preneel, Nigel Smart]

18

Quantum cryptography: negative

“The advantage of trusted-node schemes is that they provide access for lawful intercept, as required by many nation states, and they are already being installed.”

Quantum Technologies Flagship Intermediate Report, 2017



[Bart Preneel]



KU LEUVEN

What does the NSA say? [2021]

<https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>

NSA **does not recommend the usage of quantum key distribution** and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

Quantum key distribution and Quantum cryptography vendors—and the media—occasionally state bold claims based on theory—e.g., that this technology offers “guaranteed” security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD/QC, and the engineering required to balance these fundamental issues has extremely low tolerance for error. **Thus, security of QKD and QC is highly implementation-dependent rather than assured by laws of physics.**

[Bart Preneel]



KU LEUVEN

Position Paper on Quantum Key Distribution

Position France, NL,
Sweden, Germany

French Cybersecurity Agency (ANSSI)

Federal Office for Information Security (BSI)

Netherlands National Communications Security Agency (NLNCSA)

Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

21



KU LEUVEN

Industry: Dec 1, 2025

<https://bughunters.google.com/blog/googles-commitment-to-a-quantum-safe-future-why-pqc-is-googles-path-forward-and-not-qkd>

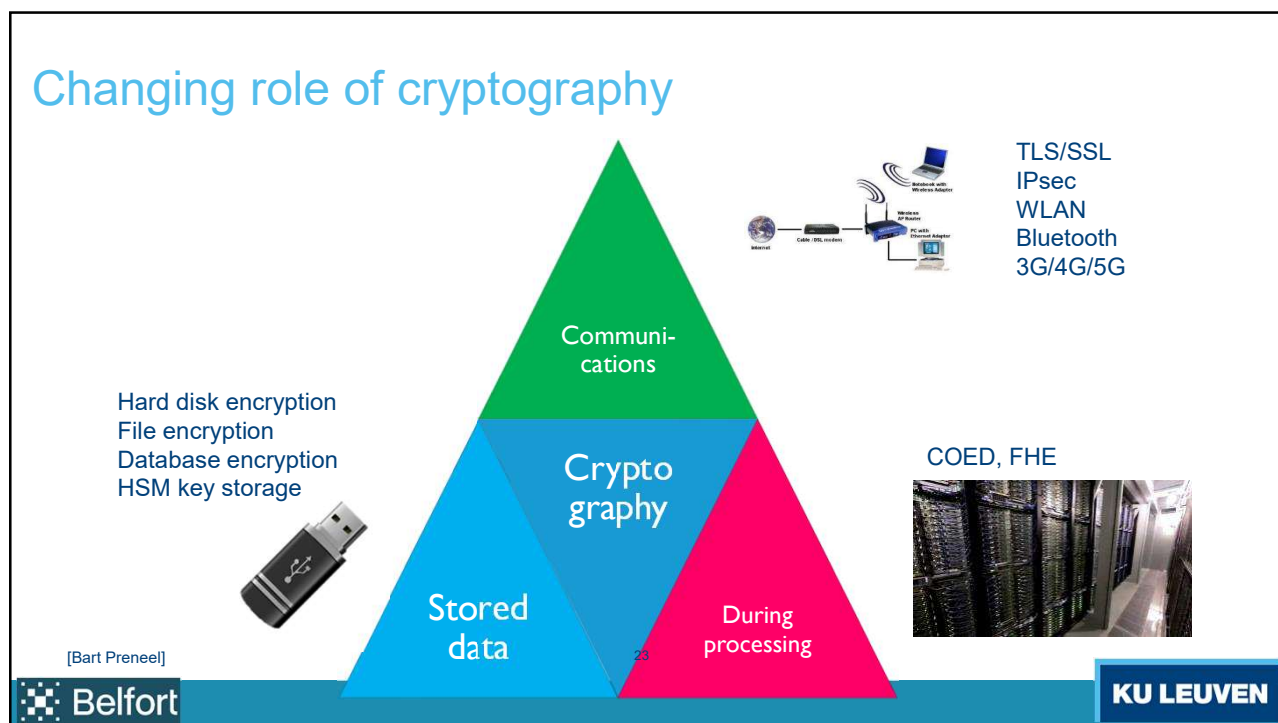
Google's Commitment to a Quantum-Safe Future: Why PQC is Google's Path forward and not QKD

At Google, we are committed to research and innovation, and that includes proactively addressing future security threats. In accordance with this principle, we have been a strong proponent of post-quantum cryptography (PQC) for years, starting with our early experiments in Chrome in 2016. At present, we are actively rolling out the PQC algorithms standardized by the U.S. National Institute of Standards and Technology (NIST) as our primary quantum-safe technology. Our focus is on solutions that are secure, scalable, and ready for both today's and tomorrow's challenges.

While PQC is our chosen path forward, it is not the only technology being discussed for a quantum-resistant future. Another approach that has gained attention is Quantum Key Distribution (QKD). As part of our commitment to thorough research and providing the best security for our users, we have closely evaluated QKD. In this post, we will share our assessment of the QKD technology and explain why we believe PQC is the more mature and scalable solution for our needs.



KU LEUVEN



Public-Key Post-quantum cryptography

24

Belfort

KU LEUVEN

Link to Semiconductor

- US CHIPS and Science Act
- September 2022



REPORT TO THE PRESIDENT

Revitalizing the U.S.

Semiconductor Ecosystem

Executive Office of the President
President's Council of Advisors on
Science and Technology

September 2022






(e) Semiconductors and System Security

Criminal and state-sponsored cyber-attacks pose increasing threats to the United States. To enable the implementation of secure systems, every aspect of the system must be considered including ~~sensors, data converters, computing, memory, storage, and communications~~, while providing robustness against side-channel attacks and ensuring security of supply chains. There is a ~~tremendous opportunity for the design of secure semiconductor chips~~. To maximize effectiveness, security must be pursued as an integral part of design, not as an add-on after the chip is designed.

Academia, industry and government stakeholders have an opportunity to standardize a trusted approach for systems implementation. The specific opportunity is to bring together algorithm and software/systems designers with chip designers in a center of excellence, to develop the next generation of secure systems. Although ~~open-source security approaches~~ are the best for innovation and transparency, they remain ~~unpalatable for the industry~~. We must address this reluctance in a way that enables the United States to continue to be the global leader in standardized security approaches.

We envision a research agenda in this area that should include, but is not limited to, the following: (1) design for fully secure end-to-end hardware and software solutions that are secure against various forms of attacks on operation, data, and communications; (2) security in the chip design tool chain that would enable end-to-end security solutions to be verified by design; (3) secure hardware supply chain covering chip fabrication, packaging, and system integration; (4) implementation of post-quantum cryptography; (5) implementation of low-power cryptography for secure communications and transactions; and (6) other privacy preserving hardware implementations for processing encrypted data.




Post-quantum cryptography

We envision a research agenda in this area that should include, but is not limited to, the following: (1) design for fully secure end-to-end hardware and software solutions that are secure against various forms of attacks on operation, data, and communications; (2) security in the chip design tool chain that would enable end-to-end security solutions to be verified by design; (3) secure hardware supply chain covering chip fabrication, packaging, and system integration; (4) implementation of post-quantum cryptography; (5) implementation of low-power cryptography for secure communications and transactions; and (6) other privacy preserving hardware implementations for processing encrypted data.

27

Challenge: NIST Post-quantum Cryptography KEM and Digital Signatures Algorithm standardization



FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

[\[FIPS 204\]](#)

Category: Computer Security

Subcategory: Cryptography

FIPS 205

Federal Information Processing Standards Publication

[\[FIPS 205\]](#)

Stateless Hash-Based Digital Signature Standard

Category: Computer Security

Subcategory: Cryptography

- Challenge: implementations
 - **Multiple** schemes
 - Efficient in HW, SW,
 - Replace old non-PQ public key
 - Resistant to non-quantum side-channel and fault attacks

28

NIST PQC “the road ahead” March 2025

FIPS 203

ML-KEM

(Based on CRYSTALS-Kyber)

- A module learning with errors (MLWE)-based key encapsulation mechanism (KEM)
- Good performance in different platforms
- An algorithm for key establishment in security protocols

FIPS 204

ML-DSA

(Based on CRYSTALS-Dilithium)

- A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm
- Good performance, simple implementation, moderate public-key and signature size, suitable for general applications

FIPS 205

SLH-DSA

(Based on SPHINCS+)

- Not require to keep track of any state between signatures
- Solid security, signatures are longer compared with ML-DSA

FIPS 206

FN-DSA

(Based on FALCON)

- Hash and sign paradigm
- Smaller bandwidth and fast verification but more complicated implementation

New KEM: HQC
(Hamming Quasi Cyclic)
“back-up”

- Under development
- (hopefully by summer)

March 2025

Published August 2024!

The 2nd Round candidates

NIST

More DSA options

May 14, 2026: reduce to 9 candidates

Multivariate	MPC in-the-head				Lattice	Code	Symmetric	Isogeny
UOV	MinRank	SD/Rank-SD	PKP	MQ				
Mayo	Miracle	Bu	Park	MQOM	Hawk	Cas	FAEST	SQsign
QR-UOV		SDiH				Lees		
SNOVA								
UOV								

N

First feasibility: SABER – LWR scheme

- CICC 2022
 - Polynomial Multiplier
 - SHA3/SHAKE

Chip Specification	
Technology	65nm LP
Supply Voltage	0.7-1.1 V
Package	Wire-Bond (Glob-Top Encapsulation)
Die Size	2mm X 1mm
Cryptographic Core	
Total Area	0.158mm ²
Memory Size	10.1875KB
Memory Type	Dual Port Low Power Low Leakage On-chip TSMC SRAM
Max. Frequency	160MHz
Hash Function	SHA-3
PRNG	SHAKE
Avg. Power	333.9uW @10MHz, 0.7V
Supply Decap.	60pF MOS
Scan Chain Interface	207b

Belfort

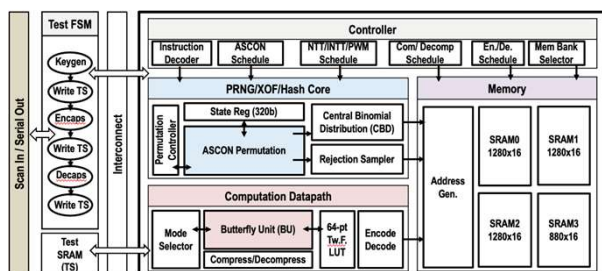
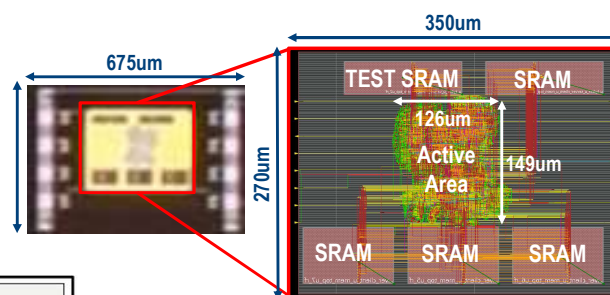
KU LEUVEN

Ingrid Verbauwhede

15

Lightweight MLWE

- ISSCC 2026
- Hash function ASCON
- NTT unit
- ...



We envision a research agenda in this area that should include, but is not limited to, the following: (1) design for fully secure end-to-end hardware and software solutions that are secure against various forms of attacks on operation, data, and communications; (2) security in the chip design tool chain that would enable end-to-end security solutions to be verified by design; (3) secure hardware supply chain covering chip fabrication, packaging, and system integration; (4) implementation of post-quantum cryptography; (5) implementation of low-power cryptography for secure communications and transactions; and (6) other privacy preserving hardware implementations for processing encrypted data.

Attacker ignores the rules & goes for the weakest link: SIDE CHANNEL ATTACKS

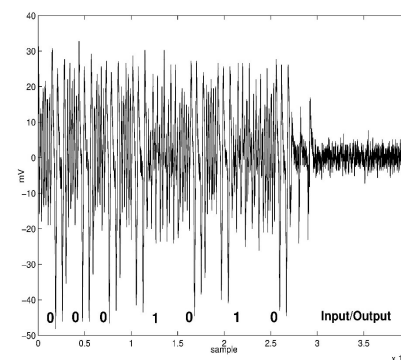
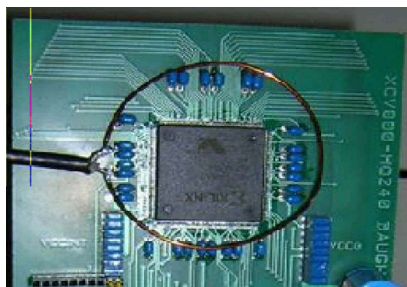
33



KU LEUVEN

Side channel attack: *Insecure* ECC implementation

SEMA attack: Simple Electromagnetic Attack

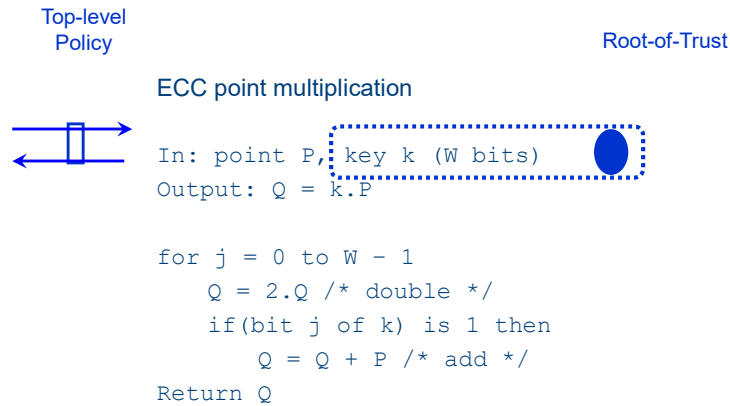


[E. Demulder EUROCON 2005]



KU LEUVEN

Example: Elliptic Curve Crypto implementation



Insecure ECC implementation

ECC point multiplication

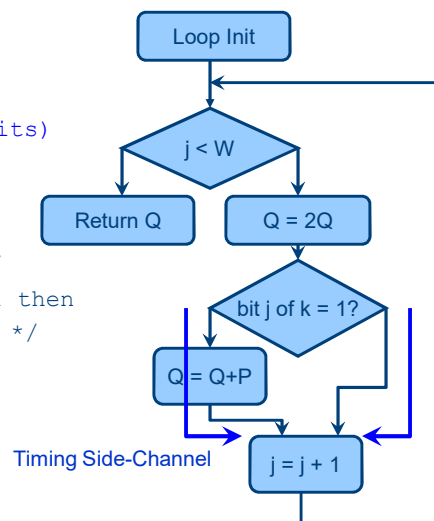
In: point P, key k (W bits)

Output: $Q = k \cdot P$

```

for j = 0 to W - 1
  Q = 2.Q /* double */
  if (bit j of k) is 1 then
    Q = Q + P /* add */
Return Q

```

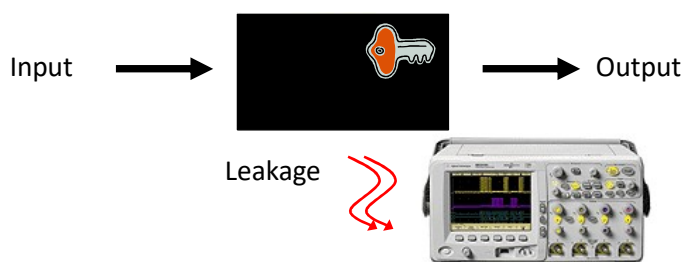


Countermeasure: balance equations

BASIC CONCEPT SIDE CHANNEL ATTACK

Side channel leakage

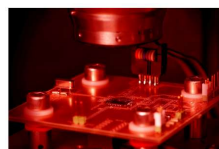
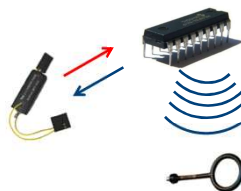
- Physical attacks $\neq$ Cryptanalysis
(gray box, physics) (black box, maths)



- Observe physical quantities in the device's vicinity and use additional information during cryptanalysis

Some Side-Channels (not exhaustive)

- Timing
 - Overall or "local" execution time
- Power, Electromagnetic radiation
 - Predominant: CMOS technology
 - Consumes power when it does something, transistors switch
 - Electric current induces an EM field
- More exotic but shown to be practical
 - Light, Sound, Temperature



Side channel leakage

- Side-channel leakage
 - Is not intended
 - Information leakage was not considered at design time of algorithm
 - Leaked information is not supposed to be known
 - Can enable new kind of attack
- Often, optimizations enable leakage
 - CMOS and dynamic power consumption
 - Caches, branches, branch prediction and timing behavior
 - Optimized multipliers and timing behavior
 - Many more

Side channel analysis: main idea



“Breaking into a Safe is hard, because one has to solve a single, very hard problem...”



“Divide et impera!”

“Things are different if it is possible to solve many small problems instead...”



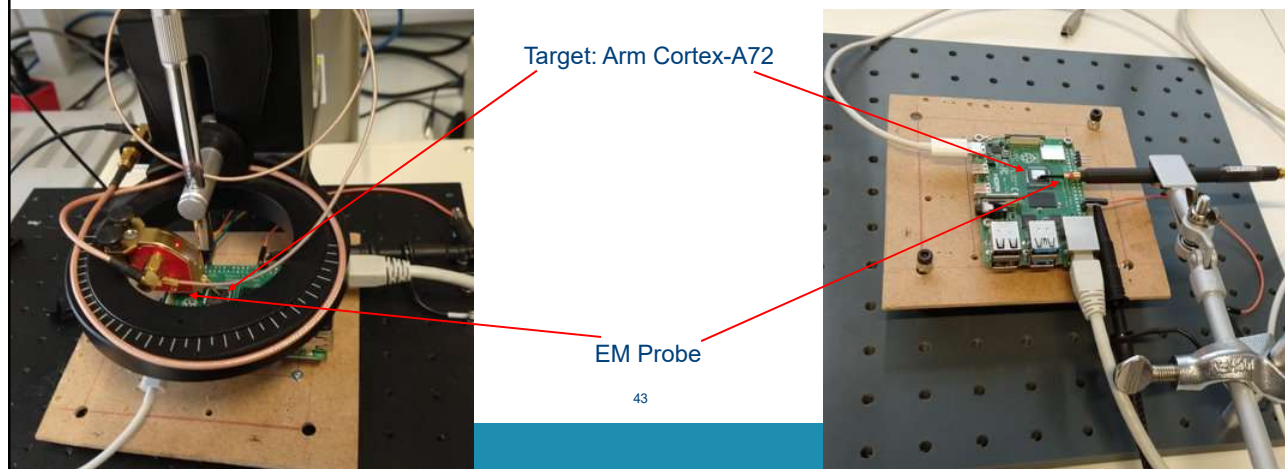
Latest attack vectors

- Spectre (2019): abuse speculative execution of micro processors
 - Several variants
 - Applies/applied to Intel, AMD, ARM
 - Abuses/reads ‘left-overs’ in the cache
- SpectrEM (2023): Physical transient execution attack
- BADRAM (2025): interface CPU vs DRAM <https://badram.eu/>
- BATTERINGRAM (2025): <https://batteringram.eu/>

[1] J. De Meulemeester, A. Purnal, L. Wouters, A. Beckers and I. Verbauwhede, “**SPECTRE-EM: Exploiting ElectroMagnetic Emanations during Transient Execution**”, Usenix Security, 2023.

SpectrEM – A physical transient execution attack

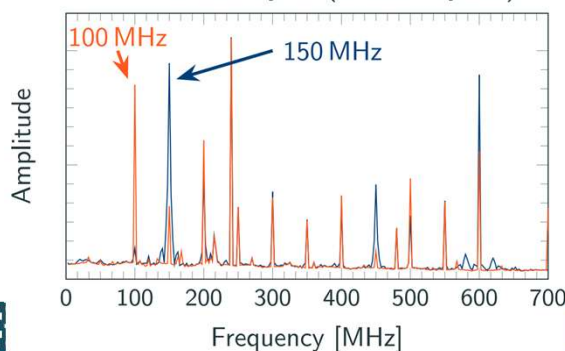
- Extract transiently accessed secrets through physical covert channels



SpectrEM – Electro Magnetic covert channels

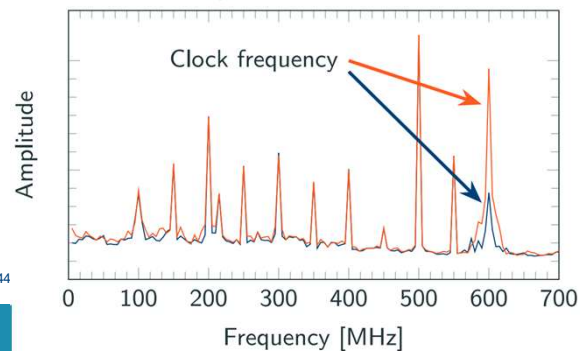
Operand-dependent timings

- Example: `udiv`
 - Divide by 0 (4 clock cycles)
 - Divide by -1 (6 clock cycles)



Control flow dependency

- Nested branch prediction
 - Correct prediction
 - Misprediction

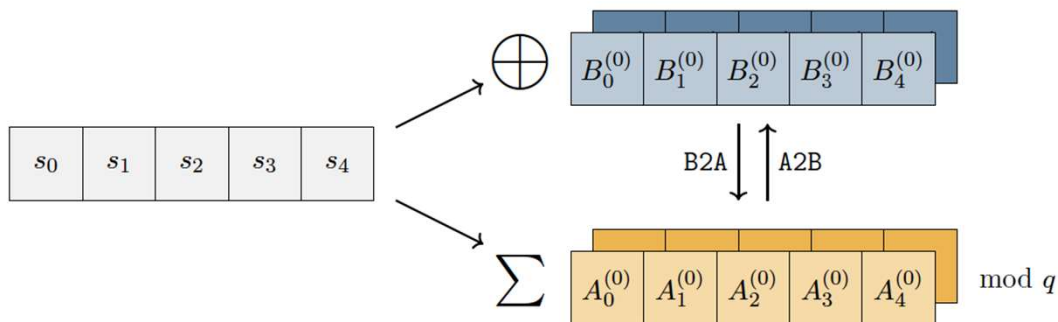


Assume you fixed all the timing problems: code is 'constant' time, what is next

COUNTERMEASURE MASKING

45

Arithmetic and Boolean masking



Conversion: Arithmetic to Boolean (A2B) or Boolean to Arithmetic (B2A)

- [1] J. D'Anvers, M. Van Beirendonck and I. Verbauwhede, "Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations", IEEE Trans on Comp 72(2), pp. 321-332, 2023.
 [2] Q. Norga, J. D'Anvers, S. Kundu and I. Verbauwhede, "X2X: Low-Randomness and High-Throughput A2B and B2A Conversions for $d+1$ shares in Hardware", IACR Cryptology ePrint Archive 2024(114), 40 pages, 2024.

Masking in practice is HARD

- Experiment: first order SW masked AES evaluated for:
 - Regular **in-order** Cortex M4/M3
 - Side-channel leakage, timing
 - Randomness requirements

Paper title	Published venue	masking method
Provably Secure Higher-Order Masking of AES	CHES 2010	boolean
Higher order masking of look-up tables	Eurocrypt 2014	boolean
All the AES You Need on Cortex-M3 and M4	SAC 2016	boolean
Consolidating Inner Product Masking	Asiacrypt 2017	inner product
First-Order Masking with Only Two Random Bits	CCS-TIS 2019	boolean
Side-channel Masking with Pseudo-Random Generator	Eurocrypt 2020	boolean
Detecting faults in inner product masking scheme	JCEN 2020	inner product
Fixslicing AES-like Ciphers	TCHES 2021	boolean

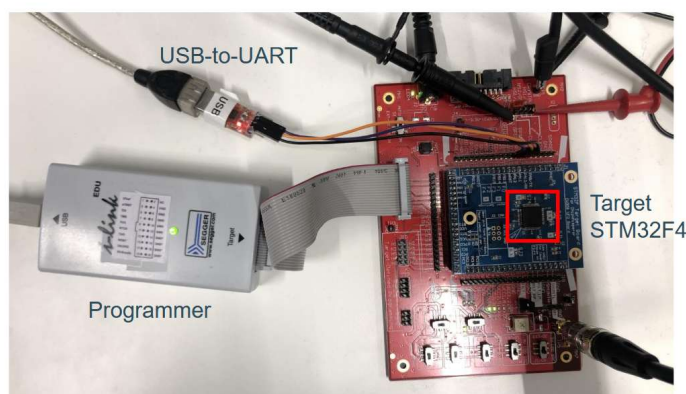
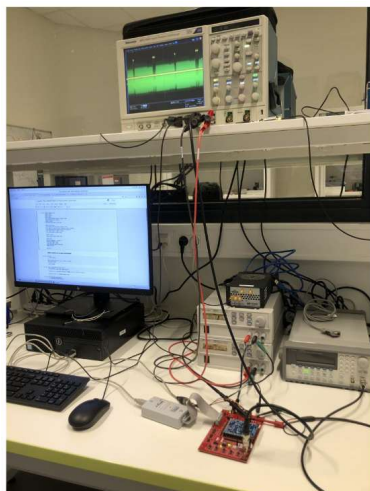
[A. Becker, L. Wouters, Cosade 2022]

47



KU LEUVEN

Set-up in the lab



48



KU LEUVEN

Results [Cosade 2022]

- Key recovery with first order attack ●
- Incorrect TRNG instantiations ●
- Benchmarking issues ●
- Software bugs ●

	Paper title	Published venue	masking method
●	Provably Secure Higher-Order Masking of AES	CHES 2010	boolean
●	Higher order masking of look-up tables	Eurocrypt 2014	boolean
●	All the AES You Need on Cortex-M3 and M4	SAC 2016	boolean
●	Consolidating Inner Product Masking	Asiacrypt 2017	inner product
●	First-Order Masking with Only Two Random Bits	CCS-TIS 2019	boolean
●	Side-channel Masking with Pseudo-Random Generator	Eurocrypt 2020	boolean
●	Detecting faults in inner product masking scheme	JCEN 2020	inner product
●	Fixslicing AES-like Ciphers	TCHES 2021	boolean

49



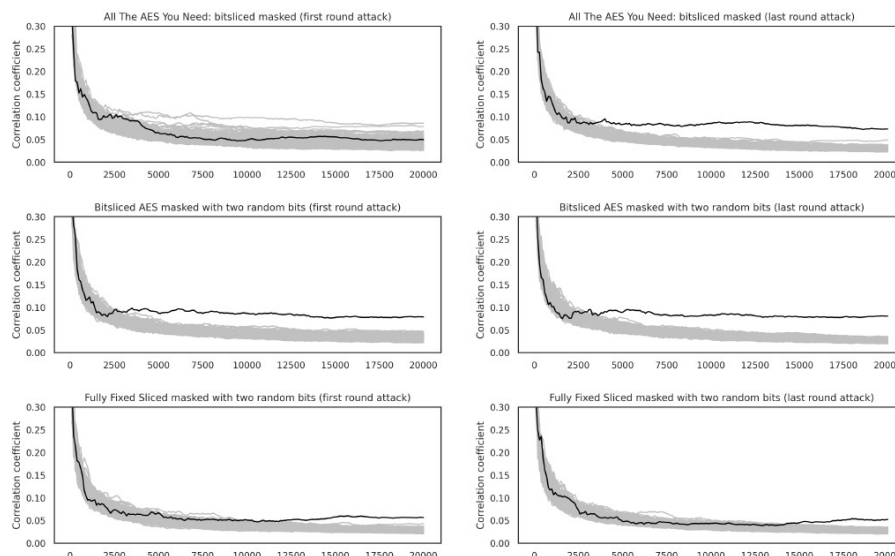
KU LEUVEN

CPA results

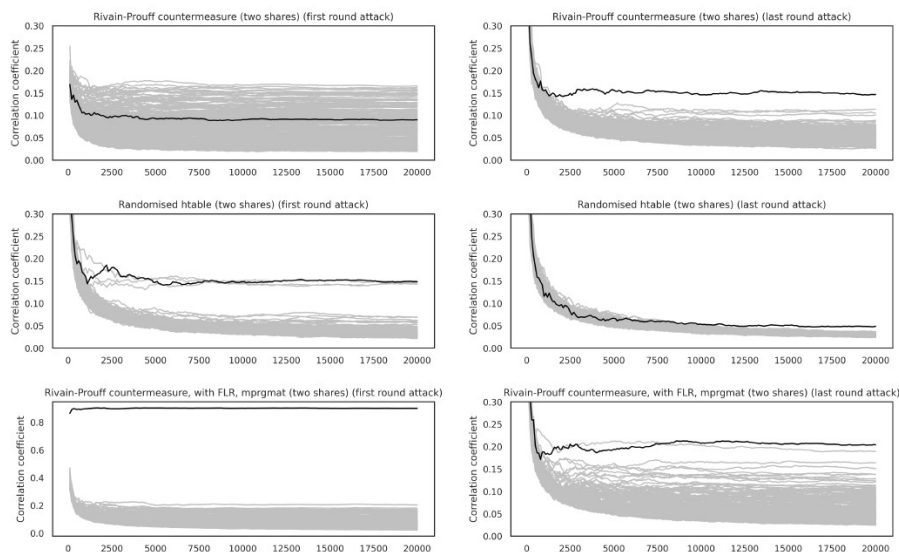
AES Key recovery:

- Byte by byte
- correct byte stands out to 255 other options

X-axis: number of samples
Y-axis: correlation coef



KU LEUVEN



For more details see [COSADE 2022](#)

51

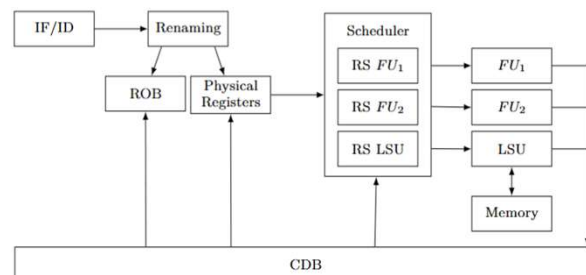
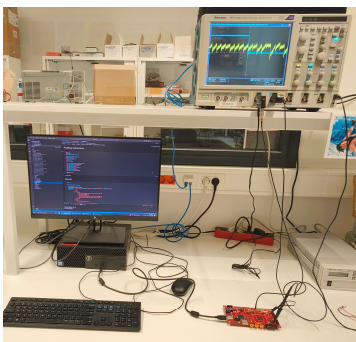


KU LEUVEN

Out of Order architectures: Open-source RISC-V – lab experiments

Proteus RVI32IM softcore on Xilinx Artix-7 FPGA

Configurable from in-order to out-of-order



Bognar et al. "Proteus: An Extensible RISC-V Core for Hardware Extensions" (RISC-V Summit Europe 2023)



KU LEUVEN

Micro-architectural control problem

Secure masking **requires (knowledge and) control** over *when* and *where* data sits



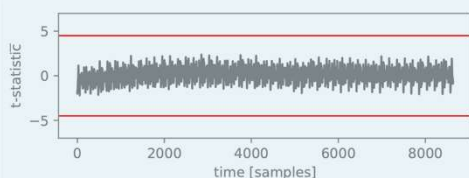
Out-of-order optimizations **removes both those controls**

Example: effect of register renaming on **identical, correctly masked** software code

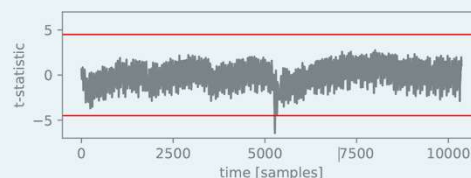
Masking relies on register discipline

Renaming: abstraction of logical registers, out-of-order cores invisible physical registers

No renaming: no leakage



With renaming: clear leakage



[E. Desmet et al. "Masking Out of Order: Side-Channel leaks from Software-Masked Cryptography on Out-of-Order Processors" (2026), IACR Eprint]



KU LEUVEN

Cause: violation of assumptions

- Assumption: shares leak independently
 - Dynamic power consumption
- Leakage caused by the microcontroller breaks this assumption
 - Assume share A is in r0
 - Move share B into r0 (and overwrite share A)
 - Information on $A \oplus B$ is leaked!
- Complex processors: transient execution
- Compiler optimizations
- Coupling through power and ground network
- Below 60nm CMOS 'static' leakage

EDA message:
TOOLS could help here!

54



KU LEUVEN

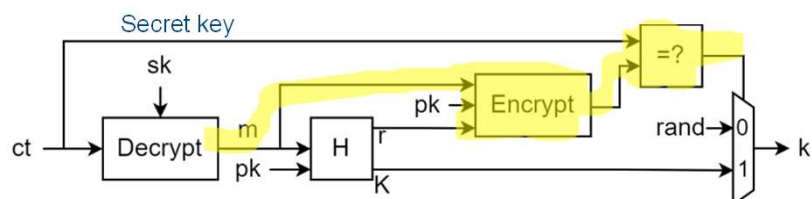
Assume you fixed all the timing problems: code is 'constant' time, what is next

MASKING FOR POST-QUANTUM: DOUBLE CHALLENGE

55

Example: Cost of decapsulation

- ML-KEM = Module Learning Key Encapsulation Module
- Part of session key generation
- FO-transform to resist Chosen-Cipher Text Attacks
 - By means of “re-encryption”
- Downstream needs protection



56

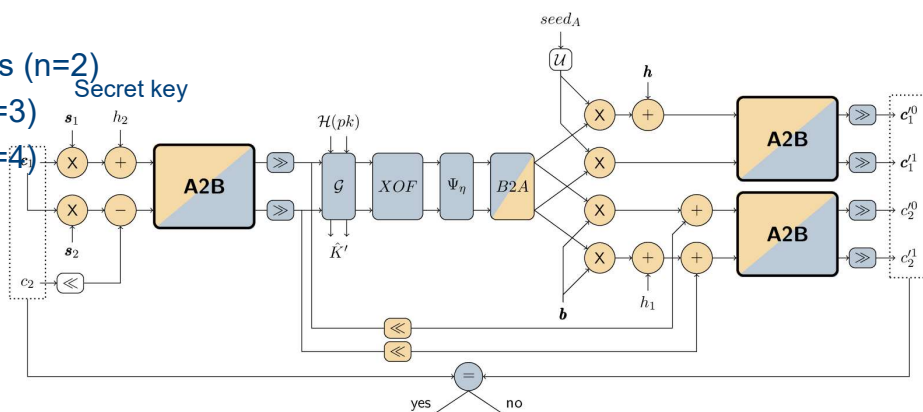
Picture adapted from Thomas Pöppelmann

One A2B conversion cost (Saber)

Requires bit-slicing

- 55-61 K cycles ($n=2$)
- 172-206 K ($n=3$)
- 302-365 K ($n=4$)

+ randomness



[1] J. D'Anvers, M. Van Beirendonck and I. Verbauwhede, "Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations", IEEE Trans on Comp 72(2), pp. 321-332, 2023.

[2] Q. Norga, J. D'Anvers, S. Kundu and I. Verbauwhede, "X2X: Low-Randomness and High-Throughput A2B and B2A Conversions for $d+1$ shares in Hardware", IACR Cryptology ePrint Archive 2024(114), 40 pages, 2024.



57

KU LEUVEN

Challenge: repeat this cost

- For every post-quantum algorithm under consideration
- Some schemes more masking 'friendly'
- Consider out-of-order architectures
- Combine with resistance to fault-attacks

FIPS 203 ML-KEM (Based on CRYSTALS-Kyber)	FIPS 204 ML-DSA (Based on CRYSTALS-Dilithium)	FIPS 205 SLH-DSA (Based on SPHINCS+)	FIPS 206 FN-DSA (Based on FALCON)
- A module learning with errors (MLWE)-based key encapsulation mechanism (KEM) - Good performance in different platforms - An algorithm for key establishment in security protocols	- A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm - Good performance, simple implementation, moderate public-key and signature size, suitable for general applications	- Not require to keep track of any state between signatures - Solid security, signatures are longer compared with ML-DSA	- Hash and sign paradigm - Smaller bandwidth and fast verification but more complicated implementation

New KEM: HQC
(Hamming Quasi Cyclic)

March 2025

Published August 2024!

The 2nd Round candidates

NIST

Multivariate	MPC in the head				Lattice	Code	Symmetric	Isogeny
	MinRank	SD-Rank-SD	PKP	HQ				
Maye	Mirath	Ryde	Perk	MQOM	Hawk	Cross	FAEST	SQsign
QR-UOV		SDiH				LESS		
SNOWA								
UOV								



KU LEUVEN



We envision a research agenda in this area that should include, but is not limited to, the following: (1) design for fully secure end-to-end hardware and software solutions that are secure against various forms of attacks on operation, data, and communications; (2) security in the chip design tool chain that would enable end-to-end security solutions to be verified by design; (3) secure hardware supply chain covering chip fabrication, packaging, and system integration; (4) implementation of post-quantum cryptography; (5) implementation of low-power cryptography for secure communications and transactions; and (6) other privacy preserving hardware implementations for processing encrypted data.

59



KU LEUVEN

Changing role of cryptography



Hard disk encryption
File encryption
Database encryption
HSM key storage



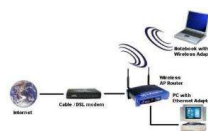
[Bart Preneel]

Stored
data

Communi-
cations

Crypto
graphy

During
processing



TLS/SSL
IPsec
WLAN
Bluetooth
3G/4G/5G

COED, FHE



KU LEUVEN

Fully Homomorphic Encryption

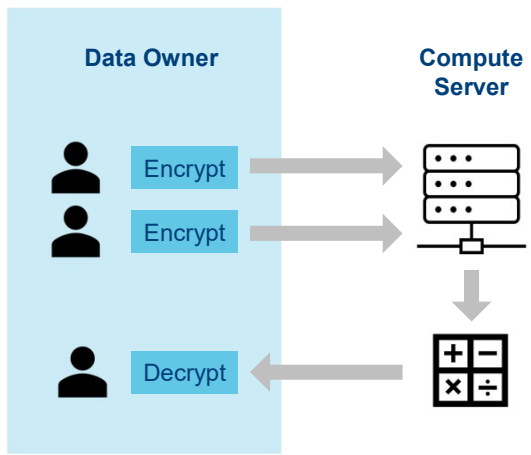


Computing on Encrypted Data

- Data owner encrypts data
- Only one designated party can decrypt
- End-to-end confidentiality
- Post-quantum secure

Application domains

- Finance, Health
- Industrial, Digital Twin
- Machine Learning, AI



The diagram illustrates the workflow of Fully Homomorphic Encryption (FHE). On the left, a light blue box labeled 'Data Owner' contains three user icons. The top two users have arrows pointing to a 'Compute Server' on the right, with labels 'Encrypt' in blue boxes. The 'Compute Server' is represented by a server rack icon. Below the server rack, there is a box containing mathematical symbols: '+', '-', 'x', and '÷'. An arrow points from this box back to the 'Data Owner' box, where a user icon has a 'Decrypt' label in a blue box.

61




FHE Challenge: memory size & memory bandwidth problem



62




Multiple schemes, multiple HW experiments

- **YASHE – Yet Another Somewhat Homomorphic Encryption - 2015**
 - Sujoy Sinha Roy, Kimmo Järvinen, Frederik Vercauteren, Vassil Dimitrov, Ingrid Verbauwhede, "Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation," CHES 2015
- **FV – Fan Vercauteren - 2018**
 - S. Sinha Roy, K. Järvinen, J. Vliegen, F. Vercauteren and I. Verbauwhede, "HEPCloud: An FPGA-Based Multicore Processor for FV Somewhat Homomorphic Function Evaluation", IEEE Trans Comp 67(11), pp. 1637-1650, 2018.
- **BFV – Brakerski Fan Vercauteren - 2020**
 - F. Turan, S. Sinha Roy and I. Verbauwhede, "HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA", IEEE Transactions on Computers 69(8), 12 pages, 2020.
- **BGV – CKKS - 2023 (Darpa DPRIVE)**
 - R. Geelen, M. Van Beirendonck, H. Lima Pereira, B. Huffman, T. McAuley, B. Selfridge, D. Wagner, G. Dimou, I. Verbauwhede, F. Vercauteren and D. Archer, "BASALISC: Programmable Hardware Accelerator for BGV Fully Homomorphic Encryption", IACR TCHES2023(4), pp. 32-57, 2023.
- **CGGI – TFHE – 2023 (ERC grant Belfort)**
 - M. Van Beirendonck, J. P. D'Anvers, and I. Verbauwhede, "FPT: a Fixed-Point Accelerator for Torus Fully Homomorphic Encryption," ACM CCS 2023
- **FINAL bootstrap acceleration on FPGA using DSP-free constant-multiplier NTTs - 2025**
 - Jonas Bertels, Hilder V. L. Pereira, I. Verbauwhede, TCHES₃2025, Issue 3 (see later this week)



KU LEUVEN



BGV experiment: ASIC Acceleration

Darpa DPRIVE Basalisc project

R. Geelen, M. Van Beirendonck, H. Lima Pereira, B. Huffman, T. McAuley, B. Selfridge, D. Wagner, G. Dimou, I. Verbauwhede, F. Vercauteren and D. Archer, "BASALISC: Programmable Hardware Accelerator for BGV Fully Homomorphic Encryption", IACR TCHES 2023(4), pp. 32-57, 2023.



KU LEUVEN

BASALISC Memory Hierarchy



**MAC Acc –
8 KB**

**MAC Register File
– 128 KB**

**Cipher Text Buffer –
64 MB**

ON CHIP

**CTB fits 3 ciphertext pairs
(one cipher text pair around 21MB)**

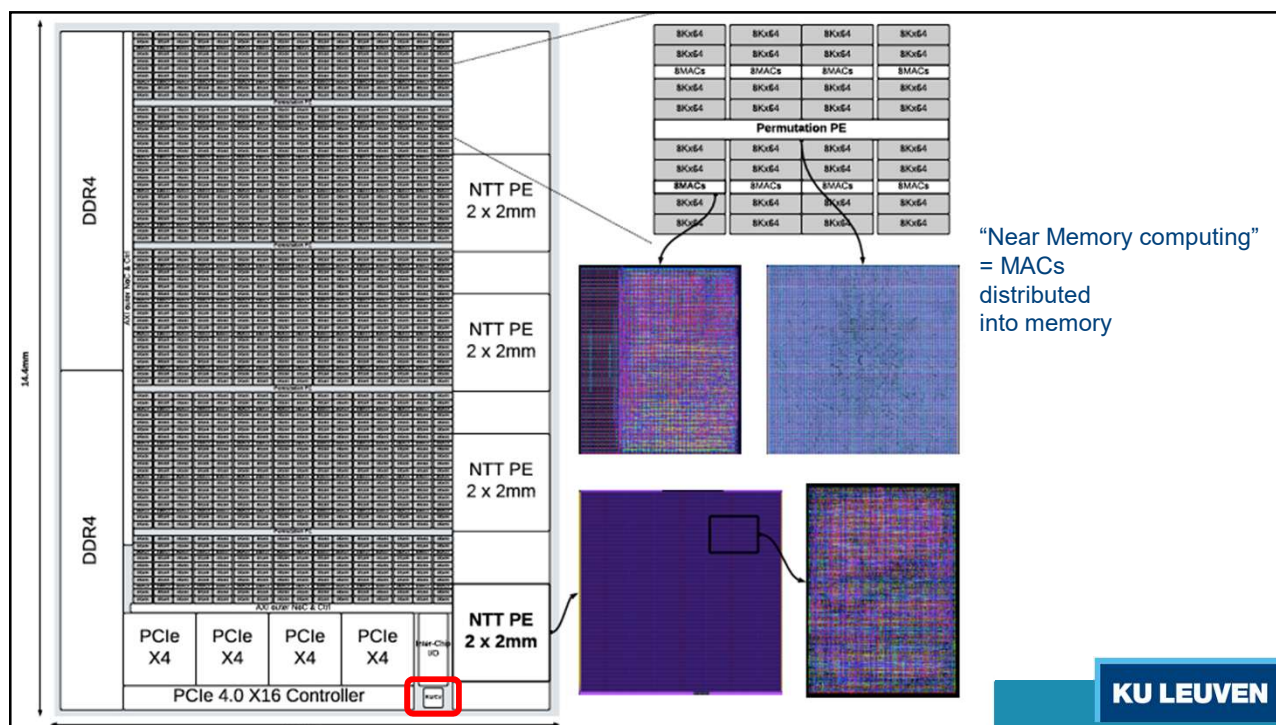
One Key switch key 112MB does not fit

DDR – 256 GB

ON BOARD



KU LEUVEN





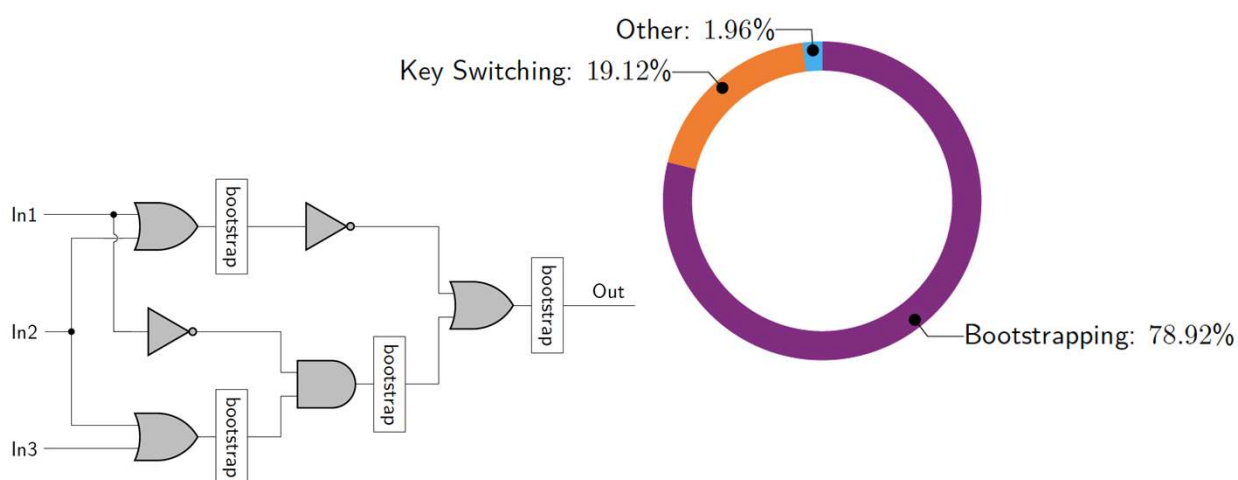
TFHE experiment: FPT - FPGA Fixed Point Accelerator

ERC Advanced Grant Belfort, FWO, CCS 2023

67
Belfort

KU LEUVEN

Challenge: TFHE Bootstrap acceleration

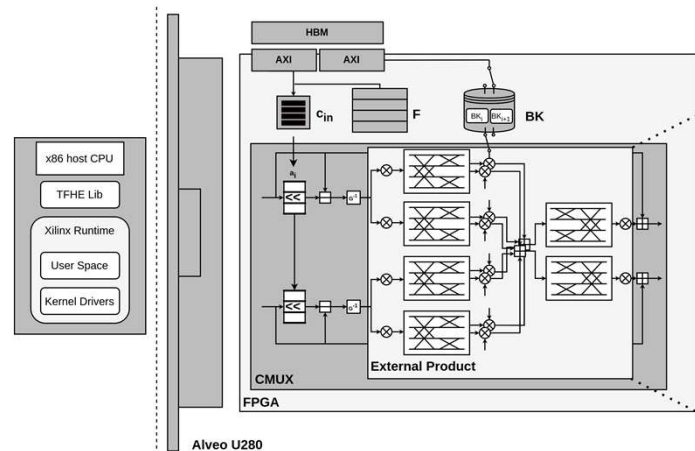


Belfort

KU LEUVEN

Turn **Communication** bound to **Computation** bound! Streaming processor architecture

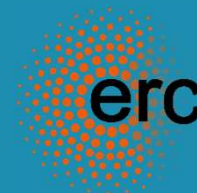
- Accelerate Bootstrapping by **pipelined streaming processor**
- Programmable (at FPGA level):
 - Adapt to security parameter set
 - Adapt to batch size/streaming width



69

[CCS 2023]

CKKS experiment: GPU platform

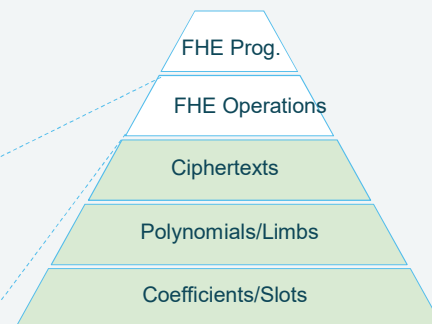
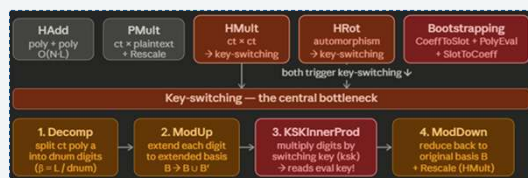


CKKS memory size, memory bandwidth problem

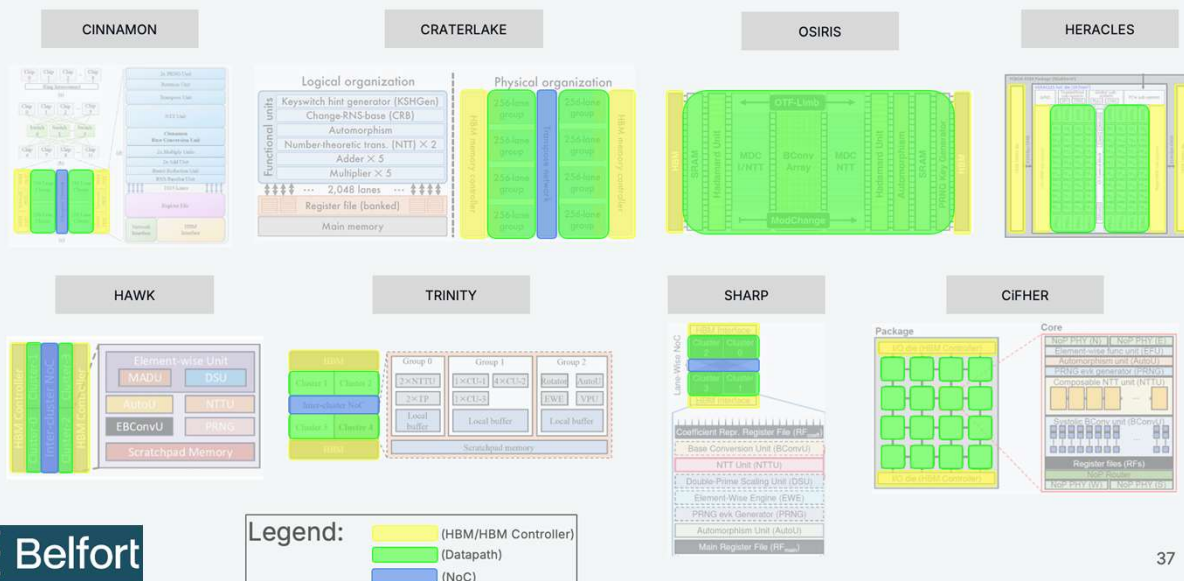
→ Parameters:

N : Polynomial size – 64K (2^{16})
 Q, P : Initial modulus (), Aux. modulus () – 1000 bits
 L : Max. mult. level (# of RNS bases) – 26 to 48
 alpha : Digit size (in decomposition)
 dnum : # of digits ($\sim L/\alpha$)

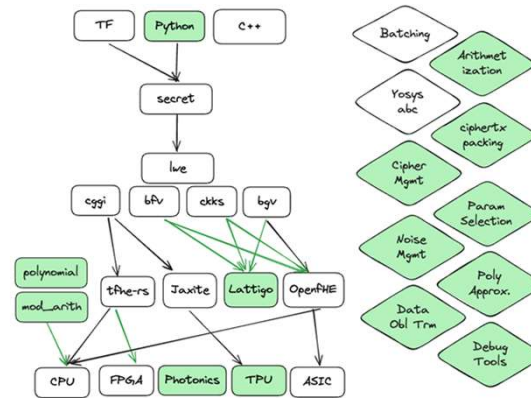
→ Operations: data movement operations



CKKS architectures across literature: design – simulation – silicon (Heracles)

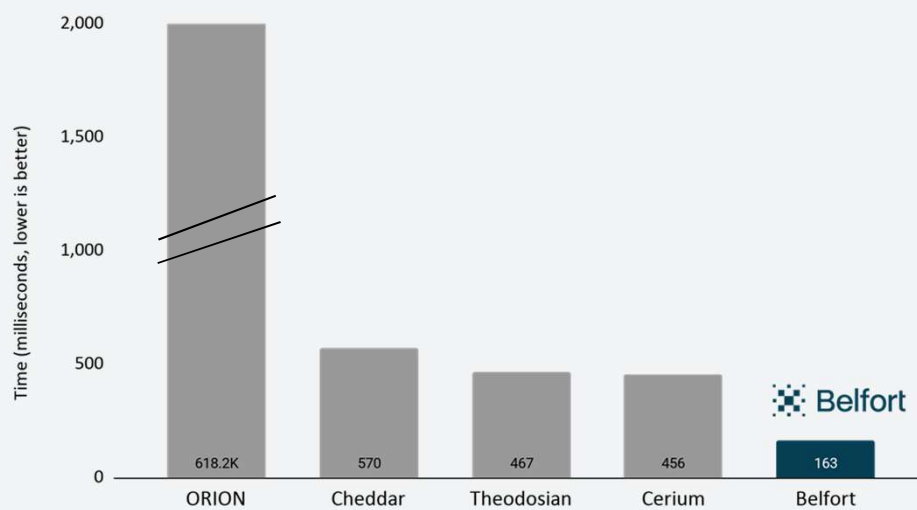


HW/SW co-design - FHE Design Environment Ecosystem is forming



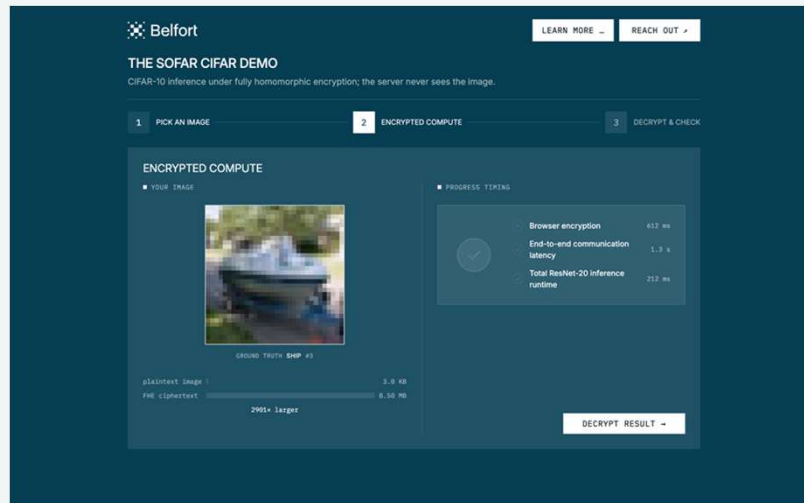
KU LEUVEN

ENCRYPTED IMAGE CLASSIFICATION: RESNET



74

IMAGE CLASSIFICATION: LIVE TO TRY

 Belfort

<https://sofar.belfortlabs.cloud/>

75

POC WITH SWIFT: DETECTING FRAUD USING FUZZY MATCHING

SHARED WITH MASTERCARD LIGHTHOUSE | 24/08/2026

Encrypted Transactions:

Bank transfers happen encrypted on SWIFT



Fraud detection: Public databases are checked for malicious individuals



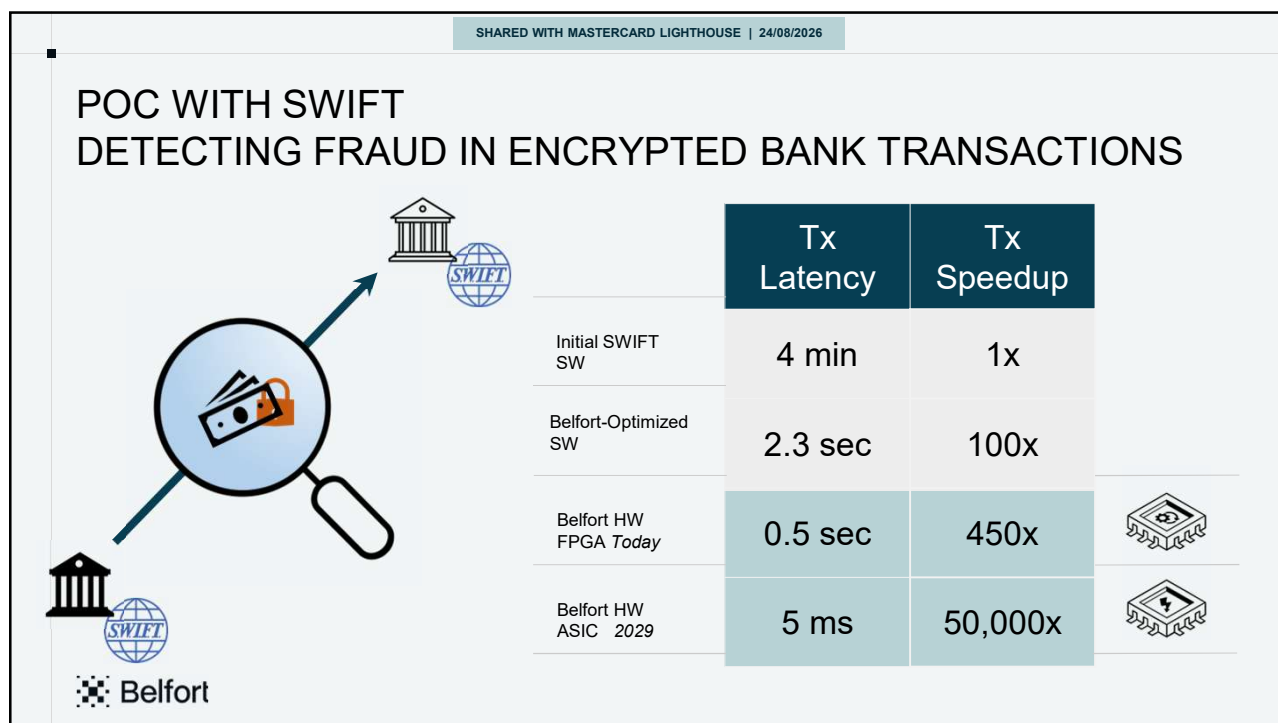
- Lena Hartwell
- Marcus Obi
- Sofia Trevelyan
- Declan Murrough
- Yuki Tanabe
- Ewan Caldecott

Fuzzy Matching: Levenshtein
used to check transactions
against public databases

		<i>f</i>	<i>r</i>	<i>i</i>	<i>d</i>	<i>a</i>	<i>y</i>
<i>m</i>	0	1	2	3	4	5	6
	1	1	2	3	4	5	6
<i>o</i>	2	2	2	3	4	5	6
<i>n</i>	3	3	3	3	4	5	6
<i>d</i>	4	4	4	4	3	4	5
<i>a</i>	5	5	5	5	4	3	4
<i>y</i>	6	6	6	6	5	4	3

 Belfort

76



Conclusions – post-quantum cryptography

- Public key cryptography = essential building block
 - Used for communication, storage, computing on encrypted data
 - NIST, Korea, China standardization processes
- QKD: only solves part of the problem
- Post-quantum cryptography
 - NIST new algorithms: need for attack resistant implementations
 - Be Flexible: support multiple algorithms
 - Mandatory transition: better be ready
- New PQ Computing on Encrypted Data, holy grail
 - Fully Homomorphic Encryption = post-quantum secure mathematics
 - No secret dependent operations in the cloud

78

Extra Material

79

Belfort

KU LEUVEN

FIRST SIMPLE HARDWARE ATTACK

80 [Slide courtesy: J. Balasch]

Belfort

KU LEUVEN

Example 1:

- 4-digit PIN verification



- 10000 possible combinations
- On average 5000 attempts necessary
- Typically only 3 attempts allowed (counter)
- Probability of correct guess: 3/10000

```

FUNCTION check (USER_PIN, CORRECT_PIN)
  FOR i=1 TO PIN_LENGTH
    IF USER_PIN[i] != CORRECT_PIN[i]
      RETURN -1
  ENDFOR
  RETURN 0

```

81

```

MAIN FUNCTION
...
IF check(...) == -1
  COUNTER++
ELSE
  COUNTER = 0
...

```

A timing attack

- Execution time of *check(...)* leaks information



- Test random PIN, measure time N
- Change first PIN digit, measure time N'
 - If N == N' both digit guesses are wrong
 - If N > N' the first digit guess was correct
 - If N < N' the new digit guess is correct

- Average 5 (worst case 10) attempts per digit
- Average 20 (worst case 40) attempts per PIN
- ... but recall that only 3 attempts are allowed

82

Next step: PIN example



MAIN FUNCTION

```
...
IF check(...) == -1
    COUNTER++
ELSE
    COUNTER = 0
...
```

- Attacker can target the main function with the aim of obtaining unlimited attempts
 - Disconnect power supply before increasing counter
 - "Skip" instructions using glitches
 - ...

83

[Slide courtesy: J. Balasch]

Similar idea:



- Secure memories with authentication
- R/W EEPROM access requires authentication
- Recording of failed authentication attempts (AACs)
- Commercial applications for anti-counterfeiting

DESIGN FLAW:

Authentication counters are updated *after* key-related computations

J. Balasch, B. Gierlichs, R. Verdult, L. Batina, and I. Verbauwhede, "Power Analysis of Atmel CryptoMemory - Recovering Keys from Secure EEPROMs", In *Topics in Cryptology - CT-RSA 2012*, pp. 19-34. Springer, 2012.

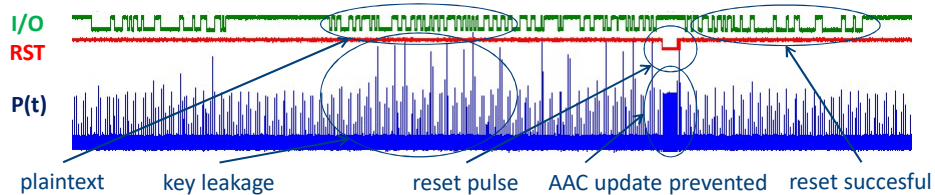
DESIGN FLAW:

Authentication counters are updated after key-related computations

ATTACK DESCRIPTION:

- 1) Send random known plaintext for authentication
- 2) Prevent AACs from updating by injecting pulse on reset line
- 3) Collect multiple power traces
- 4) Recover secret authentication key using DPA

Less than
20 minutes



BADRAM, (BADRAM.EU)
BATTERINGRAM.EU



BadRAM

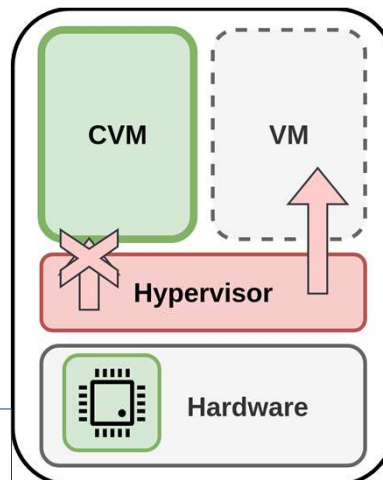
Practical Memory Aliasing Attacks on Trusted Execution Environments

Trusted Execution Environments?

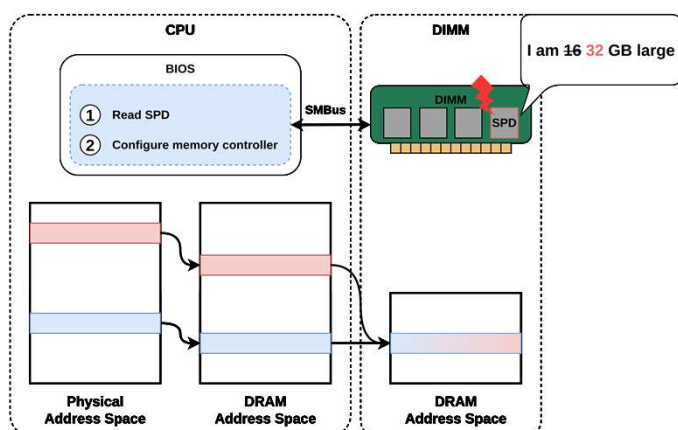
- Root of trust = Hardware
- Without TEEs cloud provider has full access to VMs
- Aim: TEEs lock out the cloud provider
- Aim: Enable computing on private data in the cloud
- **However** strong attacker model enables a vast amount of attacks

[2] J. De Meulemeester, L. Wilke, D. Oswald, T. Eisenbarth, I. Verbauwhede, & J. Van Bulck. (2025). BadRAM: Practical memory aliasing attacks on trusted execution environments. In 2025 IEEE Symposium on Security and Privacy (SP) (pp. 4117-4135).

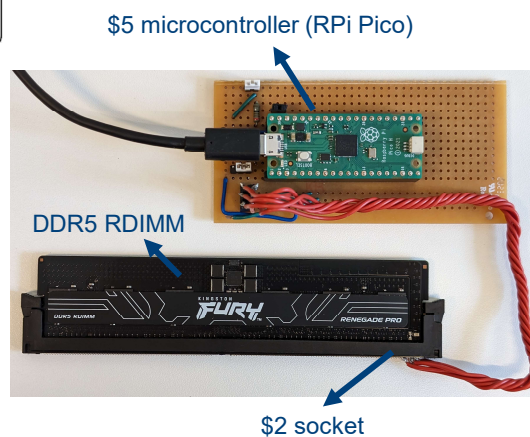
87



BadRAM – Practical Memory Aliasing



88



BadRAM – Memory Encryption in Practice



TEE	Encryption	Scalable	Guarantees		
			Confidentiality	Integrity	Freshness
Intel Classic SGX	AES-CTR	✗	✓	✓	✓
Intel Scalable SGX	AES-XTS	✓	✓	✗	✗
Intel TDX	AES-XTS	✓	✓	✓	✗
AMD SEV-SNP	AES-XEX	✓	✓	✗	✗
Arm CCA	AES-XEX/QARMA	✓	✓	✗	✗

- Result: no integrity
- Attack works for DDR4, DDR5
- AMD firmware patches
- Follow-up work: Battering Ram

89

The END

90