

Demi-Journée PQC • April 3rd, 2023

Secure hardware implementations of Lattice-based cryptography

Rafael Carrera Rodriguez

Supervised by Pascal Benoit, Florent Bruguier & Emanuele Valea



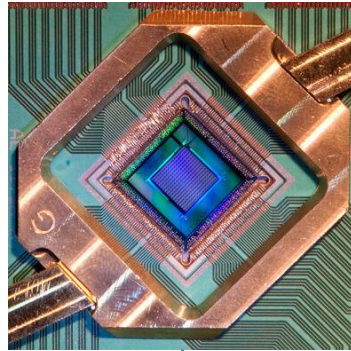
Outline

- Context and Problematic
- Attack on hardware implementation of CRYSTALS-Kyber
- Implementation and analysis of protected Number Theoretic Transform

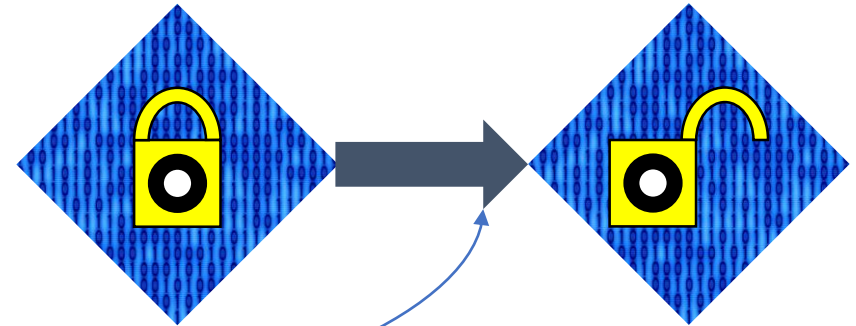
Quantum Computing vs. Classic cryptography

- Superposition
- Entanglement

Quantum computing



Classic Public-Key Cryptography



Shor's Algorithm

New algorithms needed
(Post quantum
cryptography)

Lattice-based Cryptography

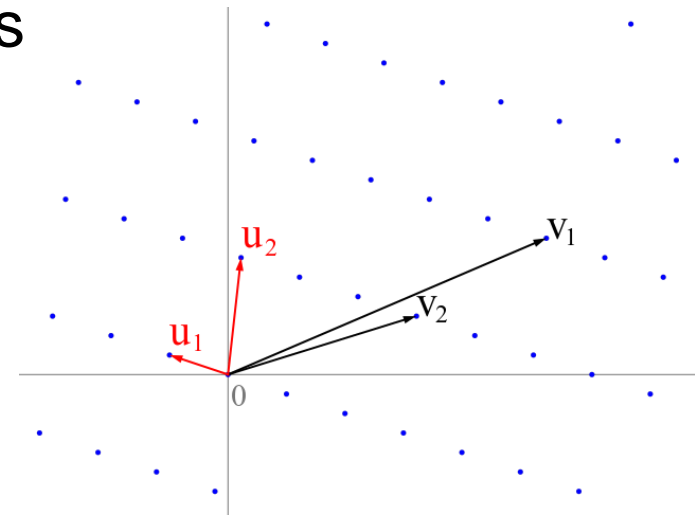
A lattice is defined as the set:

$$L(\mathbf{b}_1, \dots, \mathbf{b}_n) = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i, x_i \in \mathbb{Z} \right\}$$

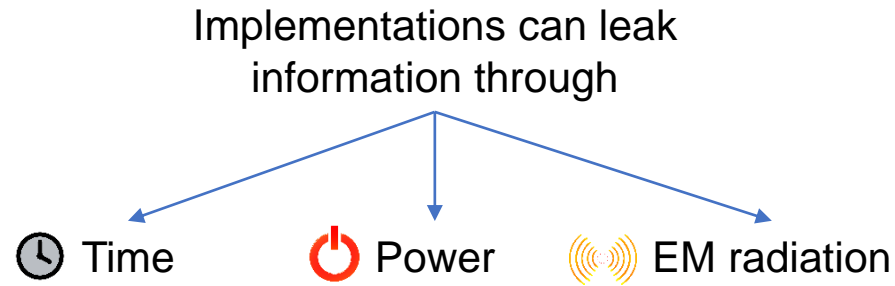
Also written as $L(\mathbf{B}) = \{\mathbf{B}\mathbf{x}, \mathbf{x} \in \mathbb{Z}^n\}$, $\mathbf{B} \in \mathbb{R}^{n \times n}$

This structure can define some problems where cryptosystems can be based on:

- Shortest Vector Problem (SVP)
- Closest Vector Problem (CVP)



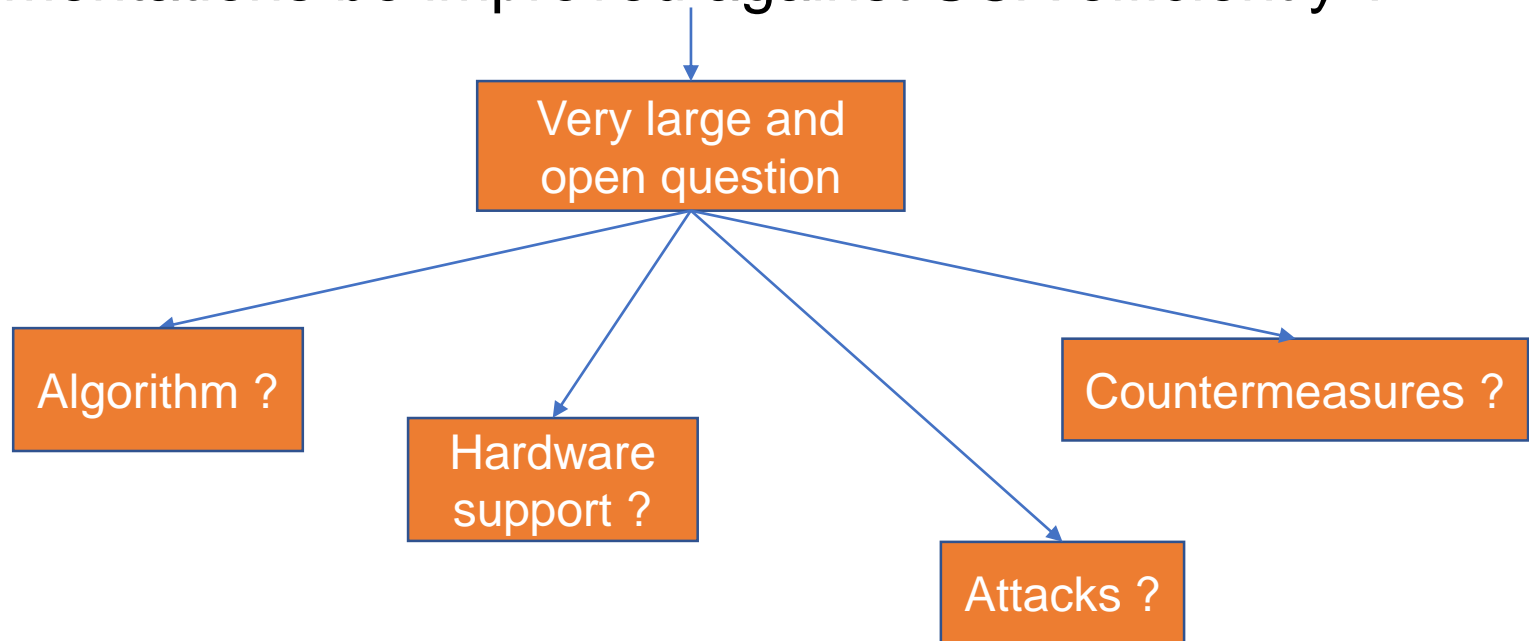
Side-Channel Analysis



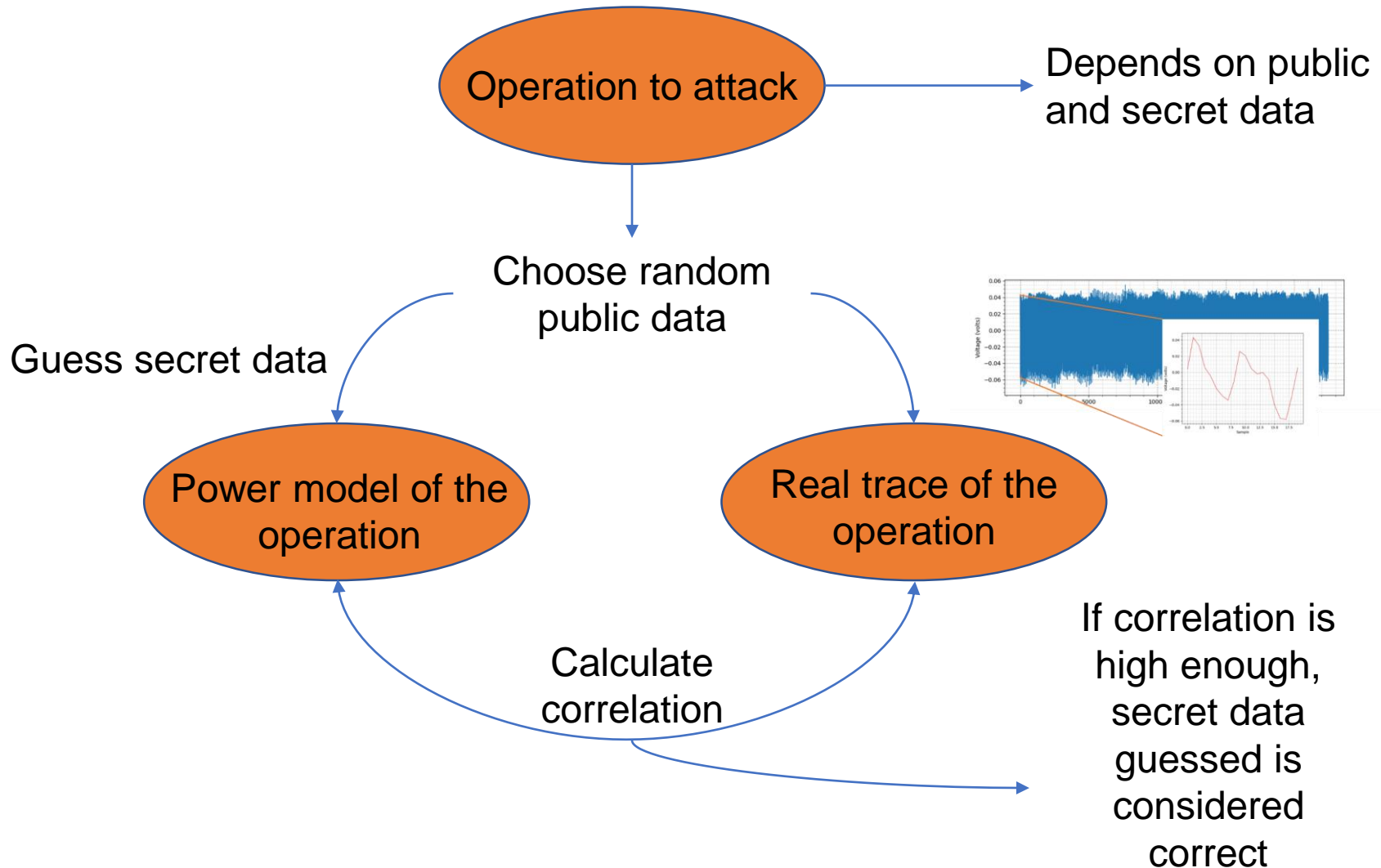
Countermeasures are needed

Thesis Problem

- The development of lattice-based cryptography implementations is being accelerated today.
 - Most of the algorithms are not inherently secure against SCA
- Question : How can the security of lattice-based cryptography implementations be improved against SCA efficiently ?

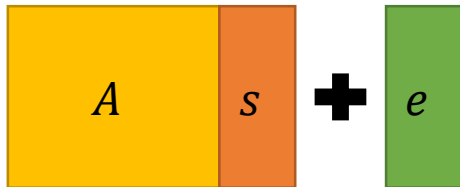


Correlation Power Analysis [BCO04]



Polynomial multiplication in CRYSTALS-Kyber

Kyber based on variant of
LWE called Module Learning
with Errors


$$A \cdot s + e$$

Basic elements are
polynomials in the ring

$$R_{3329} = \mathbb{Z}_{3329}[X]/(X^{256} + 1)$$

- $A \in R_q^{k \times k}$
- $s, e \in R_q^k$

- Schoolbook polynomial multiplication is expensive: $O(n^2)$
- Designers chose the Number Theoretic Transform (NTT) to accelerate it to $O(n \log n)$

After transformation, pointwise multiplication is done by:

$$\begin{aligned}\hat{h}_{2i} &= \hat{f}_{2i}\hat{g}_{2i} + \hat{f}_{2i+1}\hat{g}_{2i+1} \cdot \zeta^{2br_7(i)+1} \\ \hat{h}_{2i+1} &= \hat{f}_{2i}\hat{g}_{2i+1} + \hat{f}_{2i+1}\hat{g}_{2i}\end{aligned}$$

Direct multiplication between secret
key and ciphertext in decryption
routine

Related works on CPA on Kyber's polynomial multiplication

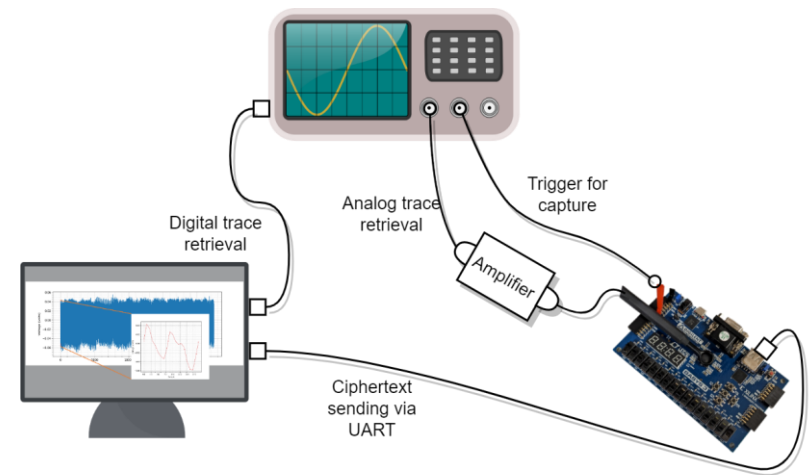
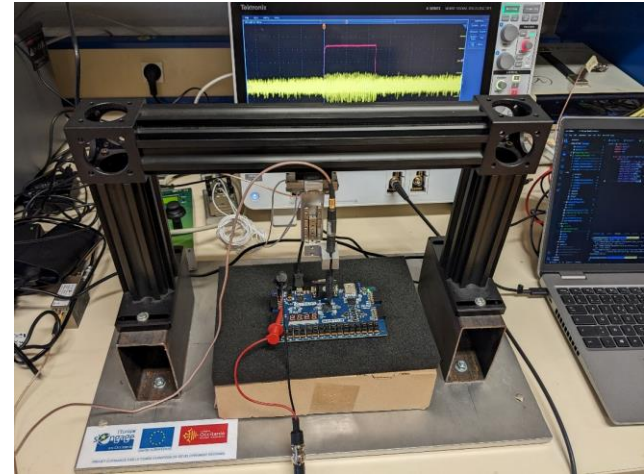
	Works	# Traces
Software attacks	[KLdG21][MBBM+22] on ARM Cortex M4 implementations	200
Hardware attacks	None until our work	?

Goal

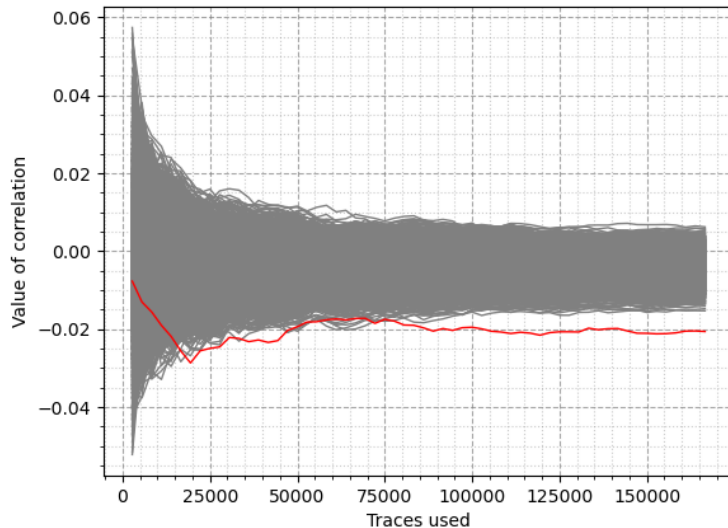
- Perform for the first time a CPA on a hardware implementation of CRYSTALS-Kyber and report requirements on difficulty
- Evaluate difference in difficulty w.r.t. the reported attacks on software

Setup

- Board: Digilent Basys-3 with Xilinx Artix-7 FPGA programmed with Kyber at its lowest security parameters
- Tektronix MSO64 oscilloscope, 1.25 GS/s (20 samples per clock cycle)
- EM probe Langer RF-U 5-2.
- Amplifier Femto HSA-X-2-40



Experimental results



Subkey 0: Maximum correlation in trace, according to number of traces sets used. In red, correct guess

- After using 15 sets of around 11k traces (166620 traces in total), all 512 secret key coefficients are retrieved.
- Time with Intel Core i7-11850H :
- Trace capturing: 6 hours and 45 minutes
- Analysis part: 2 hours and 45 minute

Countermeasure

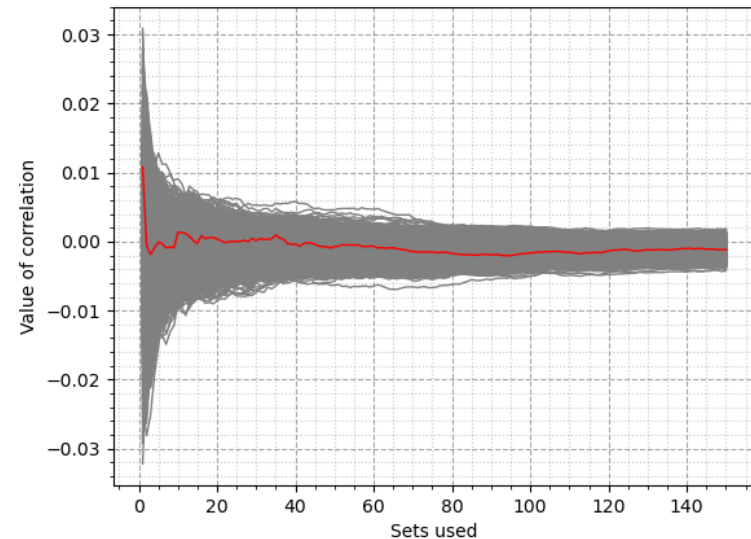
- Random and dummy multiplications are introduced before actual multiplications to invalidate the power model used. Only necessary before first multiplications.
- A linear-feedback shift register is used to generate the inputs to the multipliers
- The countermeasure has an overhead of 3.80% LUTs, 6.65% flip-flops and 2-4 clock cycles

Results of attack with countermeasure

The attack is not successful anymore, even with 10x the number of traces (1.6 million)

Limitations:

- Not valid against other possible models
- With a small modification in the model used for the first multiplications, the attack should still be possible with an increase complexity of $\approx 2^{12}$



Highest correlation of all samples for each key guess in function of the number of sets of traces used for the subkey 0 after countermeasure. In red, correct key guess.

Conclusion

- This work shows that such an attack is possible on hardware and stresses the need for countermeasures even in low power and compact hardware implementations
- A low-cost countermeasure is presented against the proposed attack as a building block to increase security of the implementation.
- It also shows in practice the difference in difficulty between attacks on software and hardware

Number Theoretic Transform

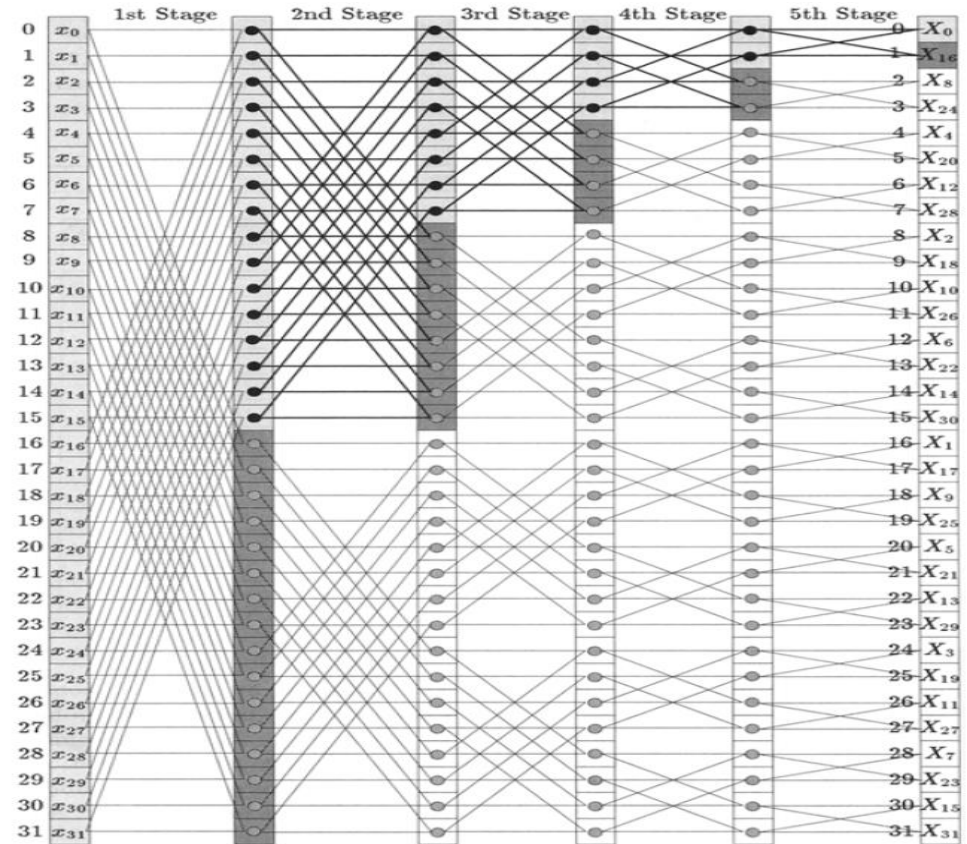
- One of Kyber basic operations is polynomial multiplication
- Accelerated by Number Theoretic Transform (NTT) that is a Fast Fourier Transform over the ring of integers \mathbb{Z}_q , $O(n \log n)$

$$X_j = \sum_{i=0}^{255} x_i \zeta^{i*j} \text{ mod } q$$

- Its efficient implementation is paramount in CRYSTALS-Kyber

Side Channel Attacks on NTT

- NTT is a highly regular algorithm
- In 2017, an attack combining algorithm information + side-channel information was published, requiring only one attack trace, called SASCA (Soft-Analytical Side-Channel Attack) [PPM17]

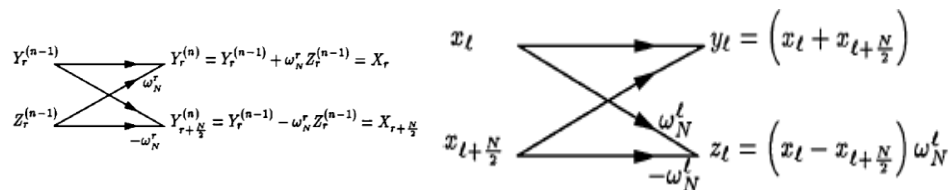


$$\begin{array}{l}
 \begin{array}{c}
 Y_r^{(n-1)} \\
 Z_r^{(n-1)}
 \end{array}
 \begin{array}{c}
 \nearrow \omega_N^r \\
 \searrow -\omega_N^r
 \end{array}
 \begin{array}{l}
 Y_r^{(n)} = Y_r^{(n-1)} + \omega_N^r Z_r^{(n-1)} = X_r \\
 Y_{r+\frac{N}{2}}^{(n)} = Y_r^{(n-1)} - \omega_N^r Z_r^{(n-1)} = X_{r+\frac{N}{2}}
 \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 x_t \\
 x_{t+\frac{N}{2}}
 \end{array}
 \begin{array}{c}
 \nearrow \omega_N^t \\
 \searrow -\omega_N^t
 \end{array}
 \begin{array}{l}
 y_t = \left(x_t + x_{t+\frac{N}{2}} \right) \omega_N^t \\
 z_t = \left(x_t - x_{t+\frac{N}{2}} \right) \omega_N^t
 \end{array}
 \end{array}$$

Related works on countermeasures

Countermeasures are focused on breaking the regularity of the algorithm

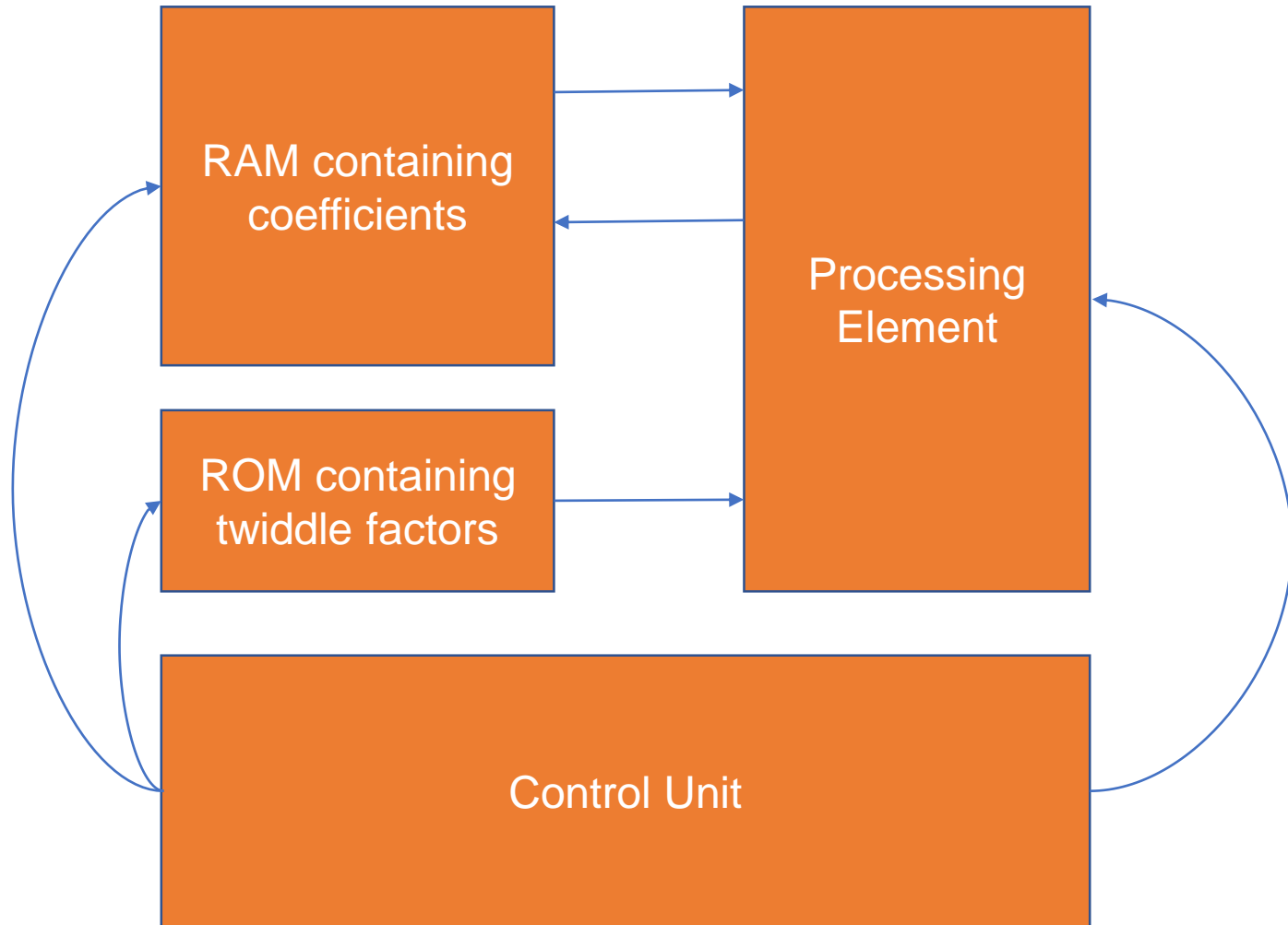
- Shuffling: Randomize order of operations within an execution [ZBT19][RPBC20]
 - Two hardware implementations [ZBT19][CMJ22]
 - Shuffling may not be enough [HSST22]
- Masking: Randomize twiddle factor in a butterfly operation of the NTT [RPBC20]
 - Requires extra multiplications (up to 4 for certain butterfly operations)
 - No hardware implementation so far



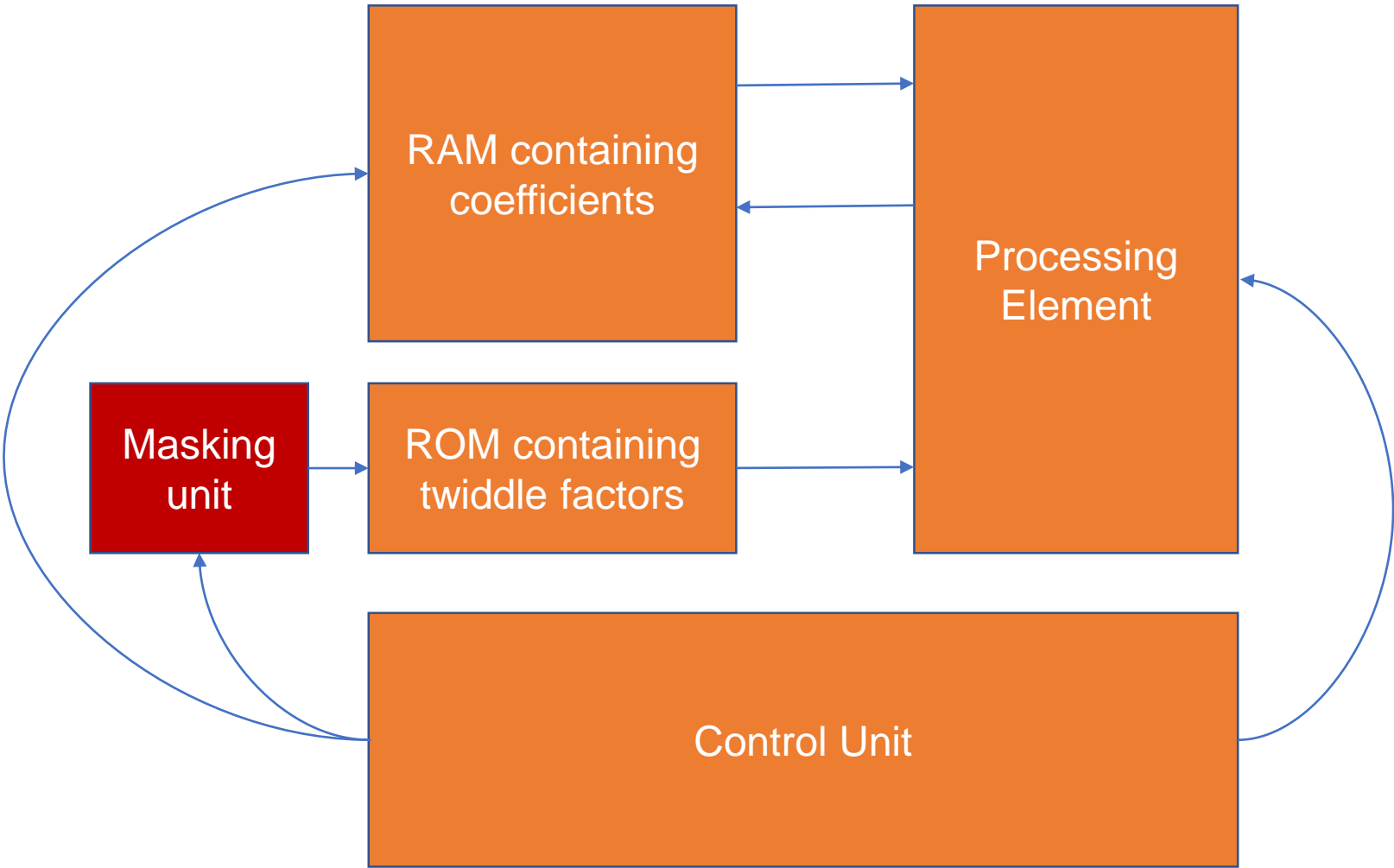
Goal

- Explore an efficient implementation of an NTT with the masking [RPBC20] countermeasure
- Make a security analysis of this countermeasure
- Reuse hardware for polynomial multiplication
 - Use [RPBC20] countermeasure to also protect against CPA for this operation [Saa17]
- Offer configurable security at runtime, as a tradeoff with performance, by allowing the user to change the number of masks in a round at runtime

General architecture of an NTT implementation

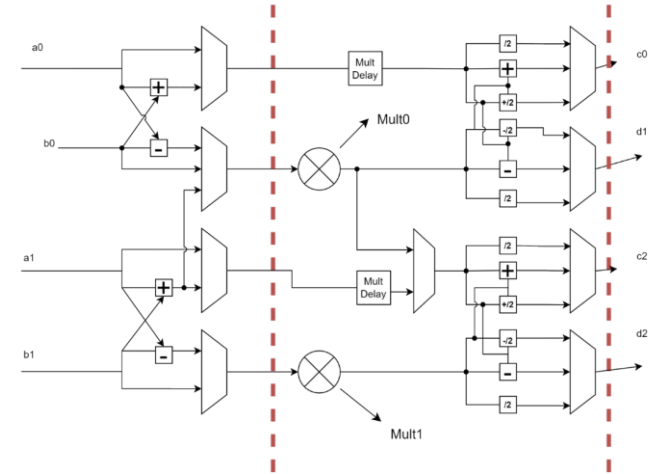


Modified architecture for an NTT implementation



Main features of NTT protected accelerator

- Reconfigurable Processing Element:
 - 4 non-protected butterfly ops
 - 2 or 1 protected butterfly ops
 - Point-wise multiplication
- 8 banks of memory to avoid memory collisions and dependency issues
- Masking unit to randomize twiddle factors
- Control unit to configure all routing and functional elements



Utilization results and SOTA with unprotected implementations

- Considering synthesis for an Artix-7 FPGA:

LUTs	FFs	BRAM	DSPs	Freq (MHz)	ATP (for unprotected NTT)
3909	1422	6	4	158	7.90

- Some unprotected implementations from the SOTA:

Ref	LUTs	FFs	BRAM	DSPs	Freq (MHz)	ATP
[LTHW22]	1170	1164	2	4	303	1.81
[BAM21]	801	717	2	4	222	2.22
[YMOS21]	2543	792	9	4	182	4.25

Conclusions and perspective

- The masking countermeasure of [RPBC20] can be efficiently implemented in hardware
- This module is in process of integration in a SOC made by CEA, as a proof of concept of hardware-software codesign for accelerating PQC algorithms
- Security analysis (mathematical and practical through t-tests) in progress

MIC Days - July 6th, 2023

Thanks ! Questions?

Rafael Carrera Rodriguez

rafael.carrera-rodriguez@lirmm.fr



References (1)

- [ABD+21] R. Avanzi *et al.*, ‘CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation’. 2021.
- [BCO04] E. Brier, C. Clavier, and F. Olivier, ‘Correlation Power Analysis with a Leakage Model’, 2004
- [KLdG21] A. Karlov and N. Linard de Guertechin, ‘Power analysis attack on Kyber’. 2021
- [MBBM+22] C. Mujdei, A. Beckers, J. M. Bermudo Mera, A. Karmakar, L. Wouters, and I. Verbauwhede, ‘Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication’. 2022.
- [JWN+22] Y. Ji, R. Wang, K. Ngo, E. Dubrova, and L. Backlund, ‘A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber’. 2022.
- [PPM17] R. Primas, P. Pessl, and S. Mangard, ‘Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption, 2017.
- [PP19] P. Pessl and R. Primas, ‘More Practical Single-Trace Attacks on the Number Theoretic Transform’, 2019.
- [HHP+21] M. Hamburg *et al.*, ‘Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber’, 2021.
- [HSST22] J. Hermelink, S. Streit, E. Strieder, and K. Thieme, ‘Adapting Belief Propagation to Counter Shuffling of NTTs’. 2022.

References (2)

- [ZBT19] T. Zijlstra, K. Bigou, and A. Tisserand, ‘FPGA Implementation and Comparison of Protections Against SCAs for RLWE’, 2019.
- [RPBC20] P. Ravi, R. Poussier, S. Bhasin, and A. Chattopadhyay, ‘On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT’, 2020.
- [CMJ22] Z. Chen, Y. Ma, and J. Jing, ‘Low-Cost Shuffling Countermeasures against Side-Channel Attacks for NTT-based Post-Quantum Cryptography’, 2022.
- [Saa17] M.-J. O. Saarinen, ‘Arithmetic coding and blinding countermeasures for lattice signatures’, 2017.
- [LTHW22] M. Li, J. Tian, X. Hu, and Z. Wang, ‘Reconfigurable and High-Efficiency Polynomial Multiplication Accelerator for CRYSTALS-Kyber’, 2022.
- [BAM21] M. Bisheh-Niasar, R. Azarderakhsh, and M. Mozaffari-Kermani, ‘High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography’, 2021.
- [YMOS21] F. Yaman, A. C. Mert, E. Ozturk, and E. Savas, ‘A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme’, 2021.