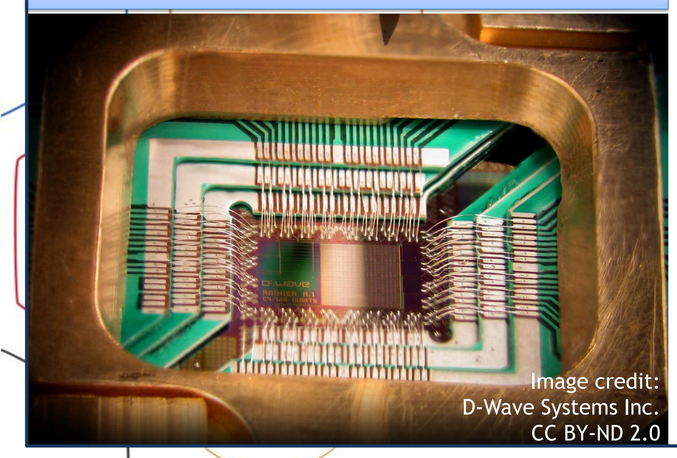
Correlation Electromagnetic Analysis on an FPGA Implementation of CRYSTALS-Kyber

R. Carrera Rodriguez[1] - F. Bruguier[1] - P. Benoit[1] – E. Valea[2]
[1]LIRMM – Université de Montpellier / CNRS, Montpellier, France
[2]Univ. Grenoble Alpes, CEA, List, F-38000 Grenoble, France

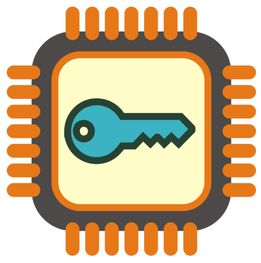
1. Motivation



Shor's algorithm in a quantum computer can break asymmetric cryptosystems such as:

- RSA
- ECC
- Diffie-Hellman
- Elgamal

Alternative ?



Post-Quantum Cryptography

Idea: Use mathematical problems not efficiently solvable by classical and quantum computers

Recent proposed schemes are not side-channel secure at algorithm level

Research needed for securing at implementation level

2. CRYSTALS-Kyber

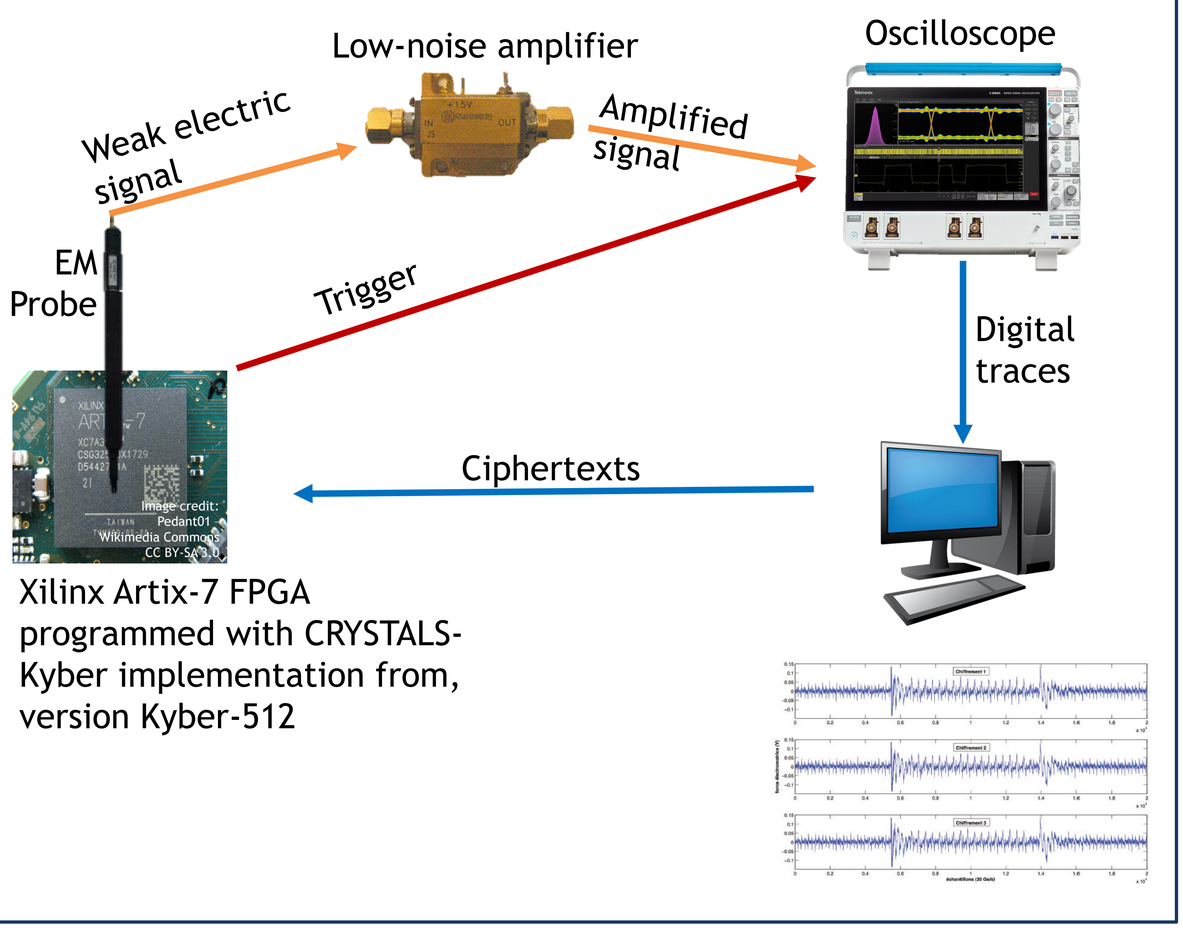
- Chosen by NIST as the standard for key encapsulation mechanisms (KEM)
- Security based on the Module-Learning with errors, belonging itself to Lattice-based cryptography
- Two basic parts:
  - An internal public key encryption system to encrypt the encapsulated key. The decryption routine is shown to the right
  - A Fujisaki-Okamoto transform to obtain a KEM resistant to chosen ciphertext attacks

Algorithm 1 KYBER.CPAPKE.Dec()

Require: Secret key $sk \in \mathcal{B}^{12 \cdot k \cdot n/8}$
Require: Ciphertext $c \in \mathcal{B}^{d_u \cdot k \cdot n/8 + d_v \cdot n/8}$
Ensure: Message $m \in \mathcal{B}^{32}$
1: $\mathbf{u} := \text{Decompress}_q(\text{Decode}_{d_u}(c), d_u)$
2: $v := \text{Decompress}_q(\text{Decode}_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$
3: $\hat{\mathbf{s}} := \text{Decode}_{12}(sk)$
4: $m := \text{Encode}_1(Compress_q(v - \text{NTT}^{-1}(\hat{\mathbf{s}}^T \circ \text{NTT}(\mathbf{u})), 1))$
5: ▷ Secret key multiplied with known value. Thus, vulnerable to vertical SCA
6: **return** m

Operation to attack

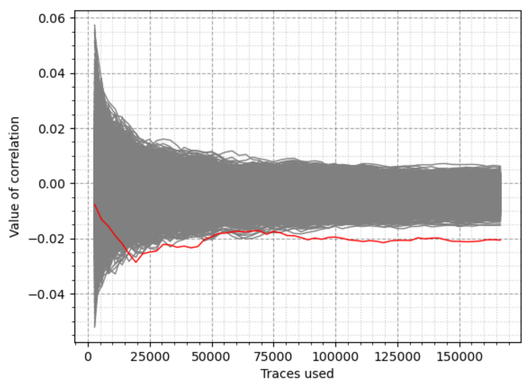
3. Setup



Xilinx Artix-7 FPGA programmed with CRYSTALS-Kyber implementation from, version Kyber-512

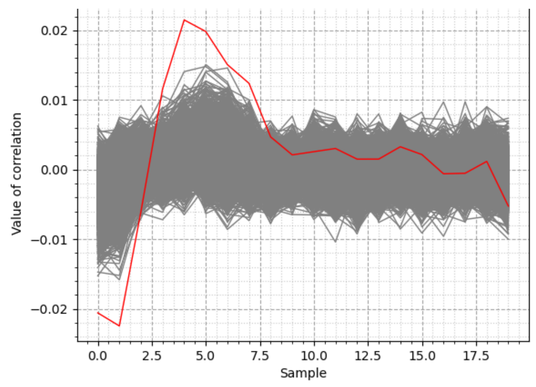
4. Attack and Results

The attack targets the pointwise multiplication in NTT domain in line 4 of Algorithm 1, for Kyber512. Correlation is calculated with a Hamming distance EM-emanation model, $HW(Op \otimes r)$, where Op is the result of the operation and r is the reference value, i.e., the previous value of the register.



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

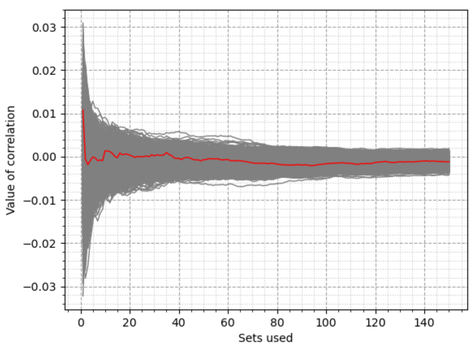
After using all 15 sets of around 11k traces (166620 traces in total), all 512 secret key coefficients are retrieved.



Subkey 0: Correlation values for several samples after using 15 sets of traces. In red, correct key guess

5. Countermeasure

For the device attacked, the first reference value of the Hamming distance model is a multiplication for the NTT of the ciphertext.
For invalidating the model, a random dummy multiplication can be inserted between the end of NTT and the start of PWM. The operands of such multiplication are obtained with a maximal linear-feedback shift register, of degree 24, for obtaining two pseudorandom 12-bit values.



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

Even when using 10x the number of traces, key is not found

This countermeasure is valid for the model and the implementation used. However, it does not prevent attacks using another models, such as Hamming weight. Also, this countermeasure clearly does not protect against higher order attacks.
For better protection, other countermeasures must be used, such as masking and other hiding techniques/

6. Conclusion

A correlation electromagnetic attack on a compact hardware implementation of CRYSTALS-Kyber is presented. It recovers the secret subkeys of the Kyber-512 version with a success rate of 100%. A countermeasure is presented that thwarts the success of this attack, albeit limited against other attacks.
Even though the number of traces used questions the practicality of this attack, this work stresses the need of research for developing side-channel countermeasures for post-quantum algorithms.
Prospects for our work include working on attacks against secured implementations, countermeasures against attacks and efficient implementations of secure PQC.

rafael.carrera-rodriguez@lirmm.fr