Exploring Fault Attacks Resistance and Possible Countermeasures for Lattice Based Cryptography

Francesco Regazzoni

Post Quantum Cryptography - Why

- Quantum Computer will exist/exists
- Shor's Algorithm could be used to break ECC and RSA in polynomial time
- Advances in classical cryptography

Post Quantum Cryptography - When

- Long term security!

Post Quantum Cryptography - What

Crypto systems that are executed **on classical computers** but for which no fast quantum algorithms are know are referred as **post quantum**.

Post Quantum Cryptography - A Bit More What

- Hardness of problems
- Quantum Physics

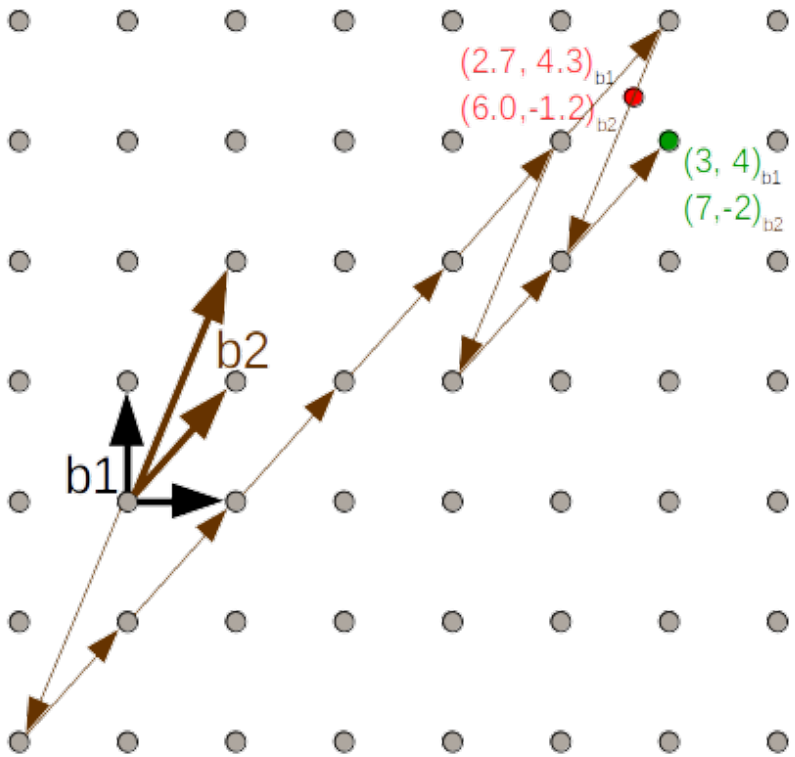
Post Quantum Cryptography - A Bit More What

- Hardness of problems
- Quantum Physics

- Hash Based
- Code Based
- ...
- Lattice Based

Lattice-based cryptography

- A lattice L is a discrete set of points in the space $\mathbb{R}^n$ with periodic structure. Foundations problems are Shortest Vector Problem and Closes Vector Problem



Lattice-based schemes

- Bliss, Bliss-B (Signature scheme)
- NTRU (Encryption scheme)
- New Hope (Key exchange protocol)
- R-LWE (Encryption scheme)

Learning With Errors (LWE)

Find $s \in Z_Q^N$, given $A = \begin{bmatrix} \vdots & & \vdots \\ a_1 & \dots & a_m \\ \vdots & & \vdots \end{bmatrix}$; $b^t = s^t A + e$

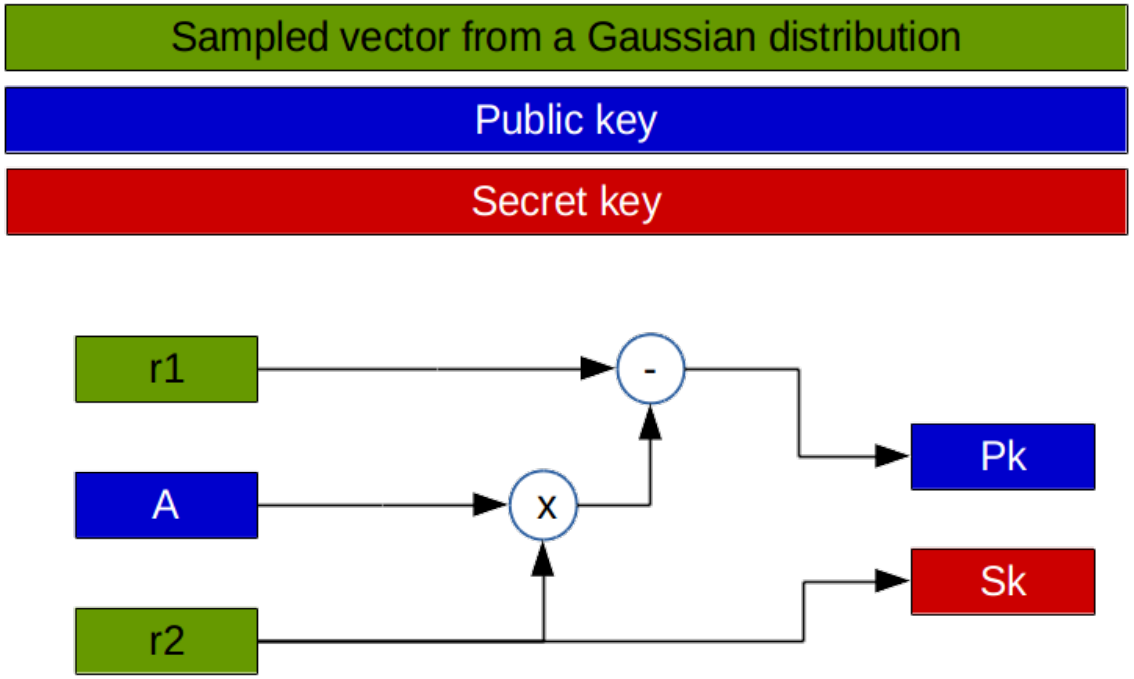
Ring Learning With Errors (R-LWE)

- We moved from standard lattices to lattices in a ring
- The matrix A becomes a vector
- Key size is reduced
- Performance is improved

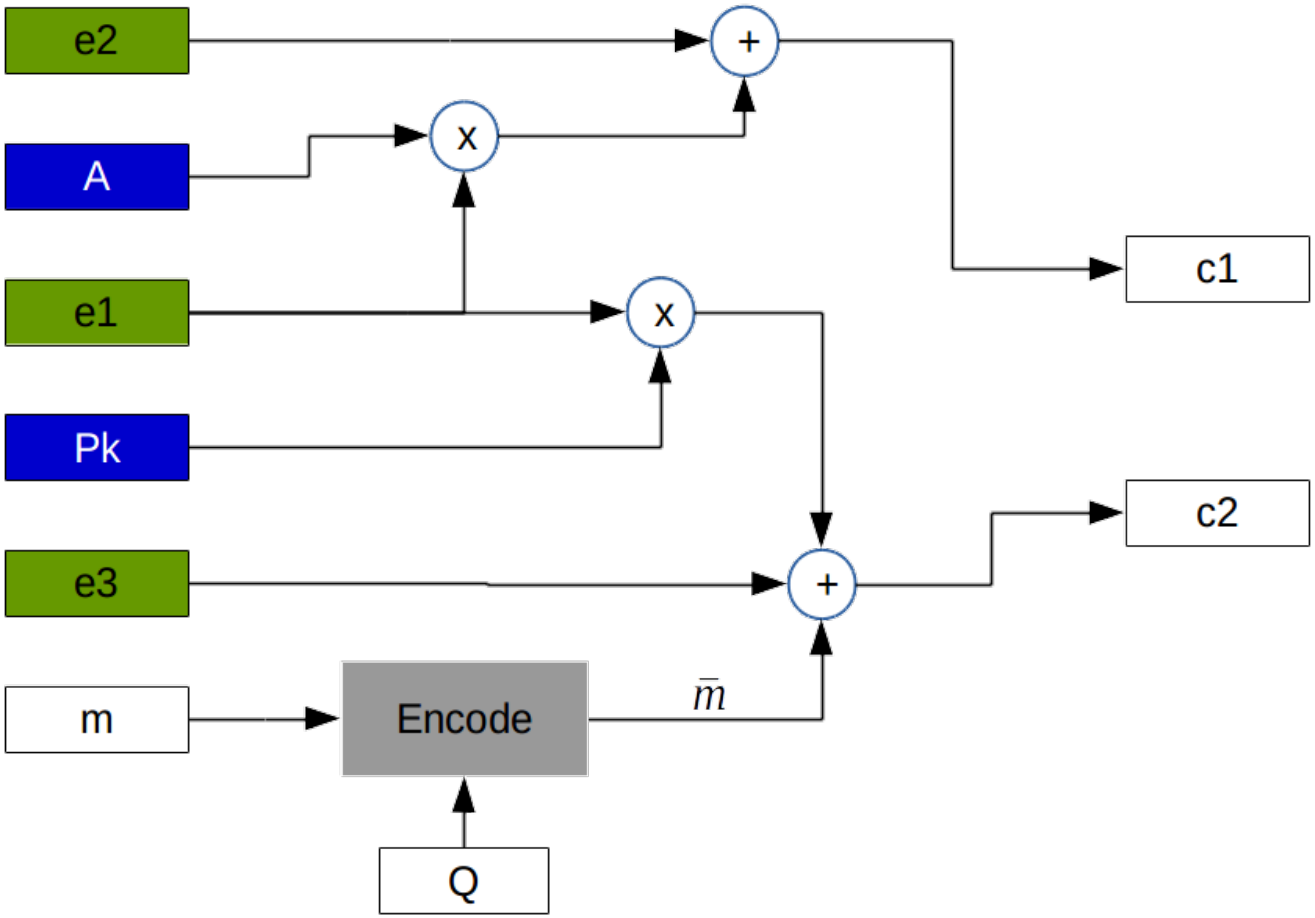
R-LWE

- RLWE is a cryptosystem based on the Learning With Errors problem on Ring
- It is parameterized by the length N, an integer Q and a distribution with variance σ

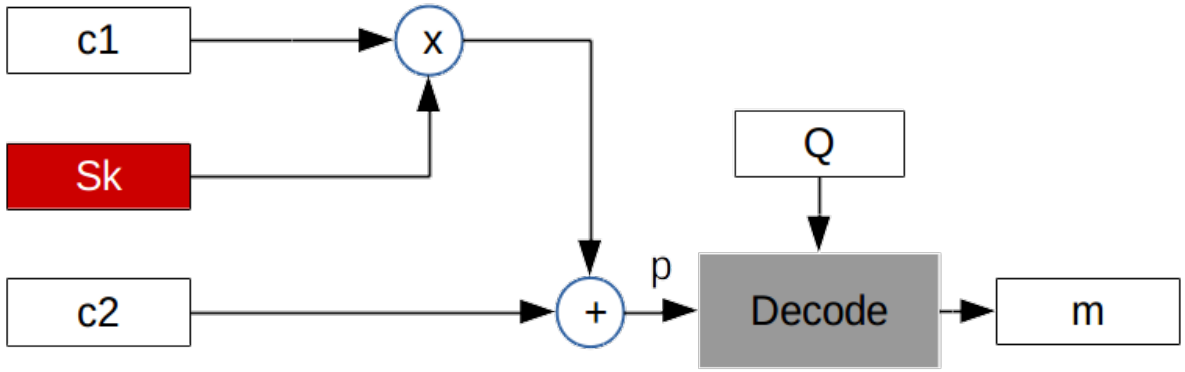
Key generation



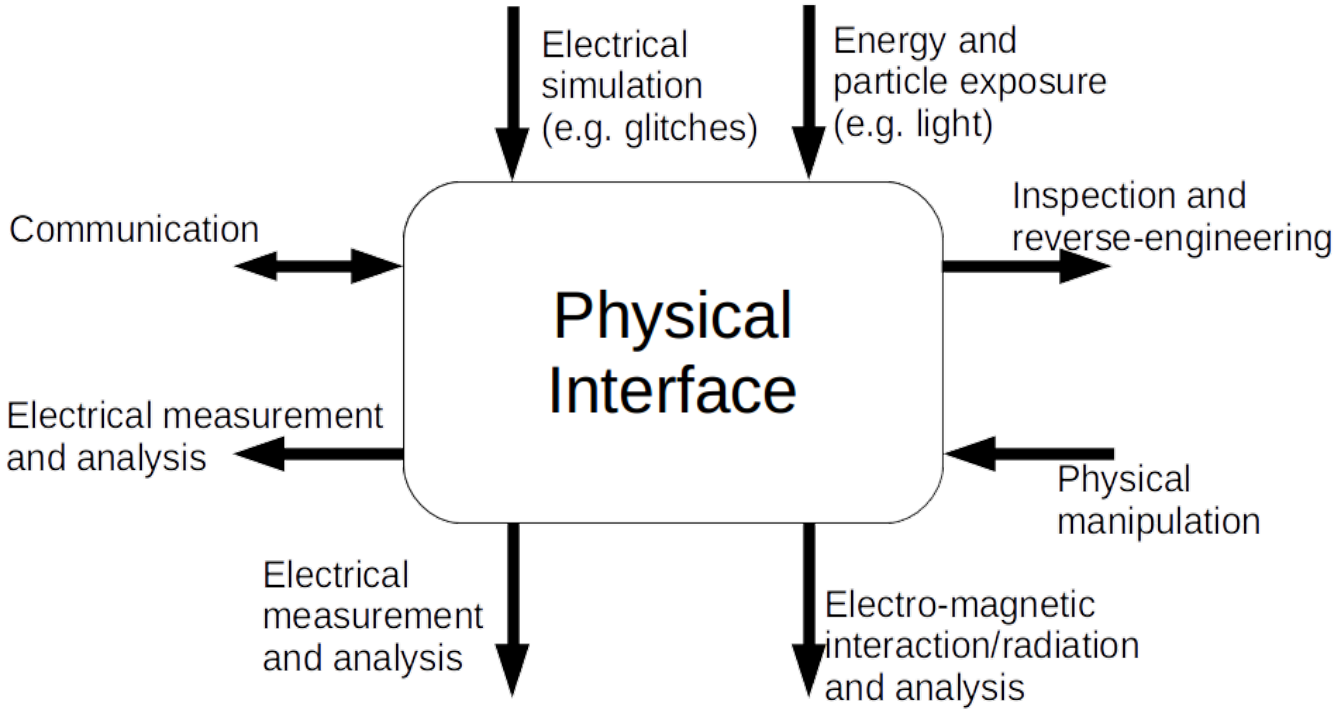
Encryption



Decryption



Physical attacks



- Timing analysis
- Power analysis
- Fault attacks

NIST requires side channel resistance

- "Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks"

[1] http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf

Fault Attacks

- Maliciously inject an error into a device computing a cryptographic operations
- Exploit the faulty behavior to gather information about the secret key

Way of Injecting Faults

- Low cost techniques for under-powering the chip
- Highly expensive and highly precise faults injected using dedicated laser equipment

- Target data or control
- Target bit, byte, or word

Considered Faults

- Zeroing
- Skipping
- Randomization

Attacks on Key Generation

Can Affect

- The secret key (sk)
- The public key (pk)

Can be Injected

- During loop control (skip of the loop)
- Modifying a value.

Attacks on Key Generation

Possible intermediate results

- $pk = ar_2, sk = r_2 - r_1$ is a vector of zeros, it is easy to compute r_2 from pk. This attack can be achieved skipping the r_1 generation with a single fault or tampering with the output of the TRNG.
- $pk = r_1, sk = 0^n$ – Obtained by skipping the sampling of r_2. The secret key consists of zeros, the scheme can be easily broken.
- $pk = r_1, sk = r_2$ – Achieved by skipping the subtraction loop during the generation of pk, requires the injection of a single fault. Produce an incorrect result, not exploitable

Attacks on Key Generation

Faults on coefficients

- *A subset of the coefficients of* r_1 *or* r_2 *are* 0 – Security reduced proportionally to the amount of coefficient set to a known value
- *A subset of the coefficients of* r_1 *or* r_2 *are random* – Drastically increases the error probability during the decryption, not exploitable

Attacks on Encryption

Attacks on the encryption can recover encrypted messages but not the secret key

Attacks on Encryption

Possible intermediate results

- $c_1 = ae_1, c_2 = pe_1 + e_3 + enc(m)$ – The error vector e_2 zeroed. The message can be recovered by computing e_1 from c_1. With e_1, we recover $e_3 + enc(m)$ thus the message m because e_3 (it consists of small Gaussian distributed coefficients and $enc(m)$ is either 0 or $\frac{q-1}{2}$). Need a single fault that skips the addition of e_2
- $c_1 = ae_1 + e_2, c_2 = e_3 + enc(m)$ – Similar to the first case. Requires to zero either pk or e_1 or to skip the insertion of pke_1 to c_2
- $c_1 = e_2, c_2 = pe_1 + e_3 + enc(m)$ – The message can not be recovered
- $c_1 = random, c_2 = pe_1 + e_3 + enc(m)$ – Generalization of the previous one
- $c_1 = ae_1 + e_2, c_2 = pe_1 + e_3$ or $c_1 = ae_1 + e_2, c_2 = random$ – The message is not part of the ciphertext, it can obviously not be recovered from the ciphertext.

Attacks on Encryption

Faults on coefficients

- *A subset coefficients* e_1, e_2, *or* e_3 *are* 0 – Security reduced proportionally to the amount of coefficient set to a known value
- *A subset of the coefficients of* e_1, e_2, *or* e_3 *are random* – Drastically increases the error probability during the decryption, not exploitable

Attacks on Decryption

- Attacking the decryption phase allow the adversary to recover the secret key

Attacks on Decryption

Zeroing the key

- Playing with the counter of loops, it is possible to control the amount of coefficients used for decryption
- The number of coefficients can be reduced till allow a brute force attack (more than one ciphertext can be need)
- Carefully select the type of fault and the amount of ciphertext needed

Attacks on Decryption

Zeroing the plaintext

- Skipping the part of the loop counter of the multiplication, allow to calculate the intermediate vectors before the mapping
- From these, observing the mapping, we recover the secret key
- Matlab simulation repeated 1000 times
- (On average) secret key recovered using approx 267 ciphertext, (parameters n = 192, q = 4093)

Possible Countermeasures

- Loop skipping faults or faulting of a loop counter: redundant loop counters
- Check the value of all coefficients before using them (trivial)
- Some attacks are equivalent to Chose Ciphertext attacks, counteracting CCA2 would complicate also fault attacks

Conclusions

- Physical Attacks are critical, also for post-quantum cryptography
- We have experience in physical security, but we need to adapt it
- Initial exploration of possible effects of fault attacks on R-LWE

Questions?

Thank you for your attention!

mail: regazzoni@alari.ch