CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

# Research Directions and Emerging Challenges in PQC

**Mélissa Rossi**
Cryptographer @ CryptoExperts

# Research on current standards

# Fundamental research to refine the security of the current standards

**Current PQC standards rely on assumptions whose precise security margins are still being actively investigated.**

- Security reductions between post-quantum problems
  Standard assumptions and variants: which are more secure? By how much?

## Learning With Errors

Solving a linear system with noise

Given the pair $(\mathbf{A} \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = \mathbf{A}\mathbf{s}+\mathbf{e} \in \mathbb{Z}_q^m)$ where

$\mathbf{A}$ is uniform modulo q

$\mathbf{e}$ and $\mathbf{s}$ are drawn according to a distribution $\chi$

Find $\mathbf{s}$

# Fundamental research to refine the security of the current standards

## **Structured** Learning With Errors

Solving a linear system with noise

Given the pair $(\mathbf{A} \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = \mathbf{A}\mathbf{s}+\mathbf{e} \in \mathbb{Z}_q^m)$ where

$\mathbf{A}$ is drawn modulo q with a **cyclic structure by blocks**

$\mathbf{e}$ and $\mathbf{s}$ are drawn according to a distribution $\chi$

Find $\mathbf{s}$

Structured lattice problems are **conjectured as hard** as unstructured lattice problems in the considered regime of parameters.

# Fundamental research to refine the security of the current standards

**Security estimates heavily rely on heuristics, asymptotic models, and extrapolations.**

Even small algorithmic improvements may significantly affect concrete security levels and parameter choices.

**Heuristic Attacks** → **Complexity Refinements** → **Parameter Impact**

**Critical need for tooling**

e.g. *Lattice Estimator*

State-of-the-art attack models

Continuous parameter reevaluation

Concrete security tracking

## Quantum Security Models

Need for tighter security models accounting for quantum attackers, quantum queries, and quantum-accessible oracles.

# Technical Migration Research Issues

# Hybridation

**Hybrid cryptographic mechanisms are recommended by EU regulators to avoid security regressions during PQ transition.**

## Hybrid Key Encapsulation

Many generic constructions already exist

- Additional **communication complexity**
- **Retro-compatibility** constraints
- Exposure to **downgrade attacks**

## Hybrid Signatures

Current solutions remain less satisfactory

- **Limited compatibility** with existing X.509 frameworks
- Difficulty of obtaining strong **formal proofs**
- Complex protocol integration
- Persistent **downgrade attack** risks

**Hybridization is currently the most pragmatic migration path, but introduces significant engineering and security challenges.**

# Simple cases of migration

**Software** products using **elementary cryptographic functions (encryption, signature)** via **open libraries**

Protocol updates + adaptations

D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in TLS 1.3 (draft IETF). *https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.*

C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van-Geest, O. Garcia-Morchon, and V. Smyslov. Multiple Key Exchanges in IKEv2 (IETF). *https://datatracker.ietf.org/doc/html/rfc9370.*

# More complex cases

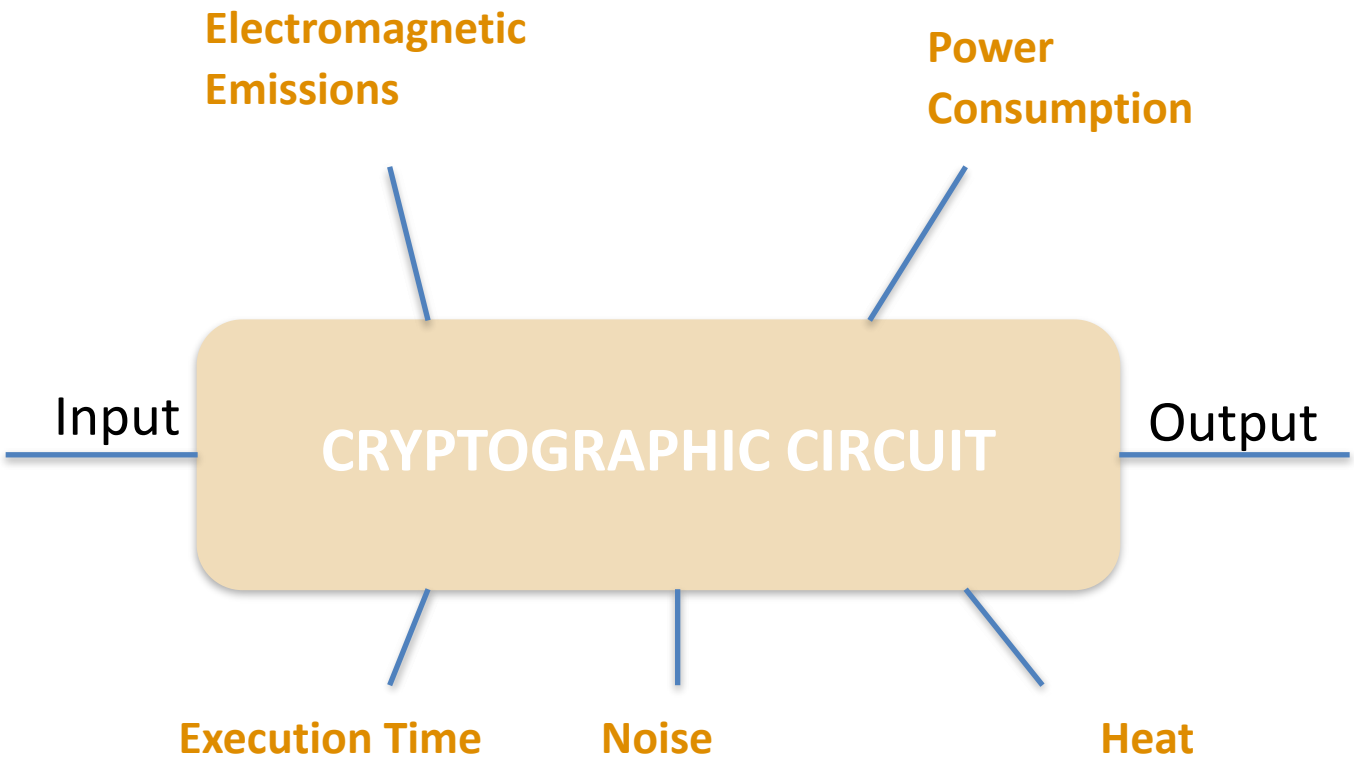
➔ For **hardware products**, the size of the chip may be increased.
➔ Exposure to physical attacks

➔ When cryptography is implemented in a **proprietary manner,** increased vigilance is required in the implementation of post-quantum algorithms and hybridization mechanisms.
If one departs from standard designs, security proofs are required.

➔ For advanced cryptographic functions, some equivalents are still at the research stage (electronic voting, blockchain, attribute-based encryption, etc.).
Security proofs are required.

# Implementation security issues

# Side-channel attacks



# Relevant Scenarios and Impact of Leakage

## Practical Targets

- IoT devices and sensors
- Smart cards and SIM cards
- Secure elements and TPMs
- Hardware wallets
- Embedded cryptographic accelerators

**Leakage**

Noisy physical information produced during computation

**Intermediate Variables**

Leakage depends on secret-related internal states

**Statistical Exploitation**

Signal processing and statistical analysis

**Cryptanalytic Attack**

Recovery of secret information

**Leakage does not directly reveal the secret key. The challenge is to exploit noisy observations statistically related to secret-dependent computations.**

**Examples of attacks:**

A Not So Discrete Sampler: Power Analysis Attacks on HAWK Signature Scheme *https://eprint.iacr.org/2022/057.pdf*

The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon *https://eprint.iacr.org/2024/1248.pdf*

# Post-Quantum Assumptions in the Presence of Leakage

Post-quantum algorithms must be revisited in the **presence of physical leakage.**

## Permeability of PQ Assumptions

- Leakage may **weaken hardness** assumptions in practice

## Designing with Leakage in Mind

- Avoid repeated manipulation of highly sensitive variables
- Limit reuse of secret-dependent intermediate states
- Carefully evaluate optimized arithmetic routines
- Integrate side-channel resistance early in the design phase

**Ongoing tooling effort: evaluating PQ hardness under realistic leakage assumptions.**

# Algorithmic countermeasures

**Implementation security can be improved directly at the algorithmic level.**

## Main Protection Strategy: Masking

- Reduce exploitable correlations in physical leakage
- But increase the randomness and complexity

## Research Challenges

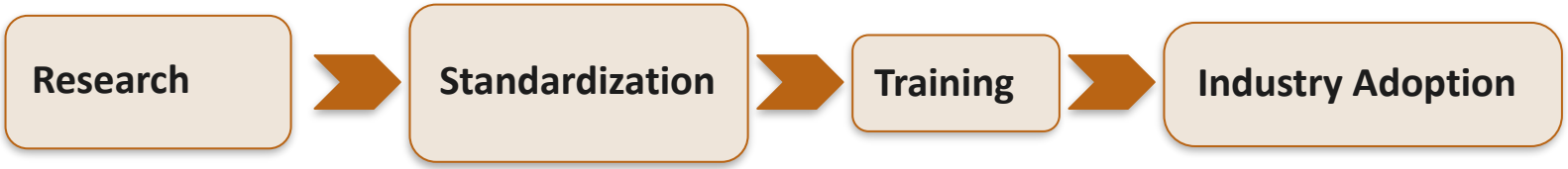
- Achieving both efficiency and strong physical security
- Balancing performance, memory footprint, and randomness costs
- Security often constrained by standardized algorithmic structures
- Current standards create a practical glass ceiling for protections

**Emerging alternatives such as Raccoon, Plover, and Polka aim to revisit design choices with implementation security as a primary objective.**

# The need for broad understanding

# Dissemination

The transition to post-quantum cryptography requires a **broad and operational understanding across the cybersecurity ecosystem.**




## Existing Dissemination Initiatives on PQC

ANSSI *resources* on PQC, *MOOC*
ANSSI *training programs* for eligible audiences
CryptoExperts *short training* sessions

## Why It Matters

Migration cannot rely solely on cryptographic experts
Consulting is good but deep understanding is better

# Thank you for attending this workshop

Stay tuned with the PQCSA project