Addressing the Challenges of Post-Quantum Crypto in Embedded Systems

European Cyber Week

Rina Zeitoun - rina.zeitoun@idemia.com

IDEMIA - Crypto & Security Labs

November 19 – 20, 2024

Outline

1 › Context

2 › Case Study: ML-KEM

3 › Quantum-Safe Proofs of Concept

4 › Conclusion

Outline

1 ❯ Context

2 ❯ Case Study: ML-KEM

3 ❯ Quantum-Safe Proofs of Concept

4 ❯ Conclusion

IDEMIA Secure Transactions

€1.5 Billion +
In revenues in 2023

900M SIM cards
shipped in 2022

700M payment products
delivered in 2022

400M+ digital tokens
provisioned

210 eSIM platforms
deployed

200+ scientific publications
over 10 years

2400 customers
in 150+ countries

750+ active patent
families

More than
50 nationalities

10,000 employees
including 800+ R&D engineers

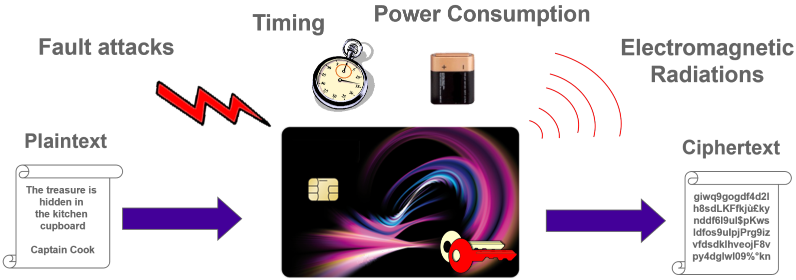
Advanced payment cards | **Mobile payment** | **5G** | **Car connectivity** | **Cloud-based digital connectivity**

Smartcard Constraints

- Need to implement **optimized** code (assembly language) **to fit** algorithms on smartcards.
- Standardized post-quantum algorithms are **not especially designed** for smartcards.
- RAM and performance optimizations are **essential** for post-quantum crypto deployment.

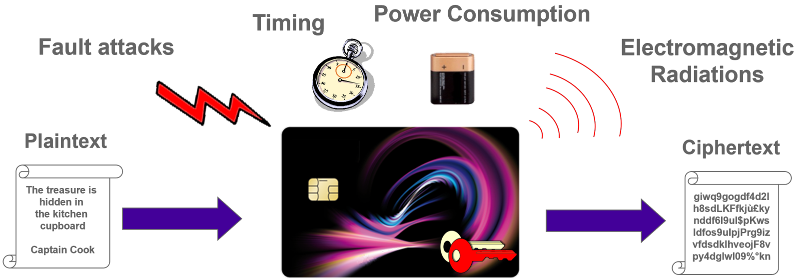
Security Constraints

› Our products are deployed in hostile environments: Attackers have physical access to the device.



Security Constraints

› Our products are deployed in hostile environments: Attackers have physical access to the device.



Security against all physical attacks is mandatory

› Simple/Differential Power/Electromagnetic Analysis, Timing/Template/Fault Attacks, etc.

› **Standardized PQC** algorithms are **only** resistant to **Timing** Attacks.

› **Countermeasures** imply **time and memory** overheads: Need to design **optimized** countermeasures.

Outline

1 › Context

2 › Case Study: ML-KEM

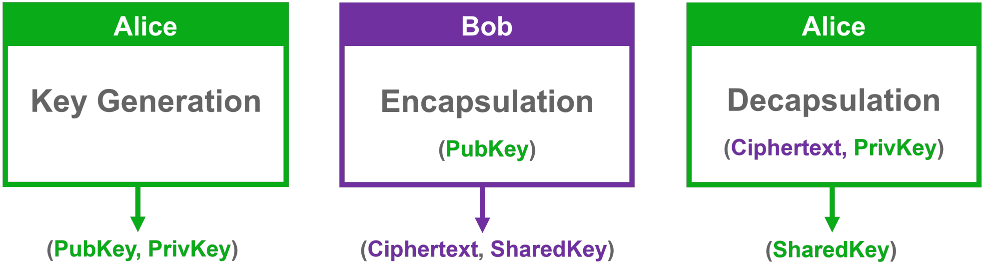
3 › Quantum-Safe Proofs of Concept

4 › Conclusion

New Post-quantum Algorithm ML-KEM

ML-KEM: a Key Encapsulation Mechanism

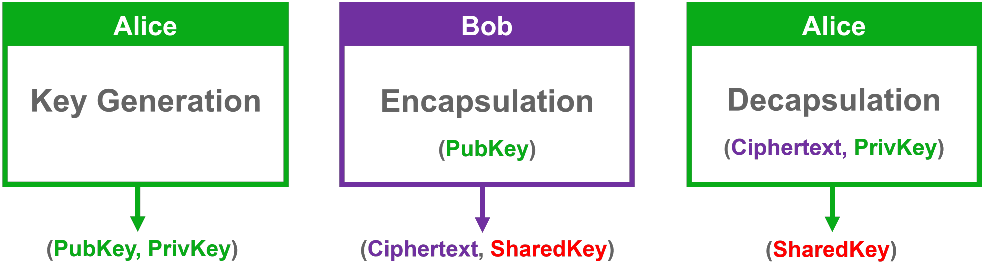
- CRYSTALS-Kyber winner at NIST competition
- NIST standardized ML-KEM as FIPS 203 in August 2024
- ML-KEM replaces RSA, DH and ECDH for key exchange



New Post-quantum Algorithm ML-KEM

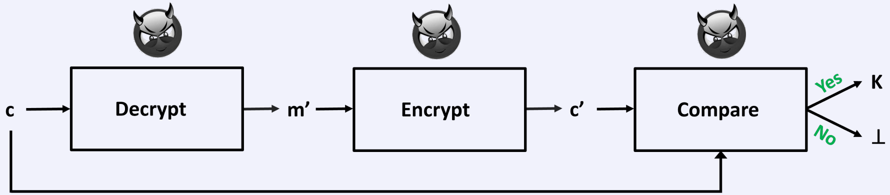
ML-KEM: a Key Encapsulation Mechanism

- CRYSTALS-Kyber winner at NIST competition
- NIST standardized ML-KEM as FIPS 203 in August 2024
- ML-KEM replaces RSA, DH and ECDH for key exchange



Side-channel Attacks on ML-KEM

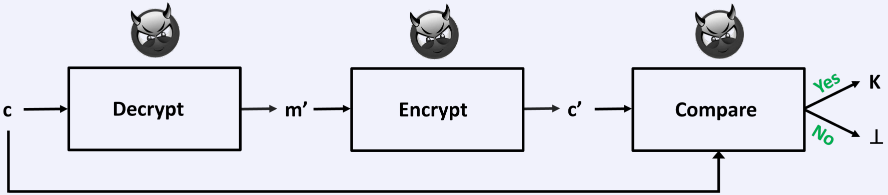
Power/EM Attacks on Decapsulation based on FO Transform



- **Whole Decapsulation needs to be protected**

Side-channel Attacks on ML-KEM

Power/EM Attacks on Decapsulation based on FO Transform



- **Whole Decapsulation needs to be protected**

Side-Channel Attacks on Key Generation

- Investigated in security certifications (Common Criteria and EMVco).

Masking Countermeasure

First-Order Masking Countermeasure

- Each sensitive variable x is shared into 2 variables: $x = x_1 \oplus x_2$
- Manipulate x_1 and x_2 independently

Masking Countermeasure

First-Order Masking Countermeasure

- Each sensitive variable x is shared into 2 variables: $x = x_1 \oplus x_2$
- Manipulate x_1 and x_2 independently

Boolean: securely compute $x \oplus y$?

Given:

- $x = x_1 \oplus x_2$
- $y = y_1 \oplus y_2$

Compute:

- $x_1 \oplus y_1$
- $x_2 \oplus y_2$

Masking Countermeasure

First-Order Masking Countermeasure

- Each sensitive variable x is shared into 2 variables: $x = x_1 \oplus x_2$
- Manipulate x_1 and x_2 independently

Boolean: securely compute $x \oplus y$?

Given:

- $x = x_1 \oplus x_2$
- $y = y_1 \oplus y_2$

Compute:

- $x_1 \oplus y_1$
- $x_2 \oplus y_2$

Arithmetic: securely compute $x + y$?

Generate arithmetic sharing:

- $x = x_1 + x_2 \mod 2^k$
- $y = y_1 + y_2 \mod 2^k$

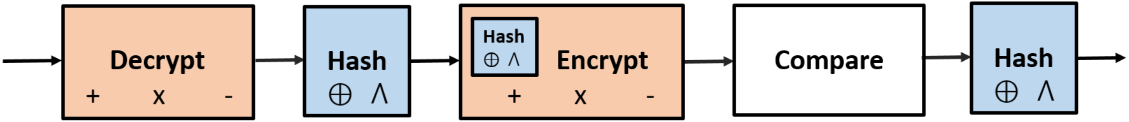
Compute:

- $x_1 + y_1 \mod 2^k$
- $x_2 + y_2 \mod 2^k$

Arithmetic and Boolean Masking

Masks Conversions

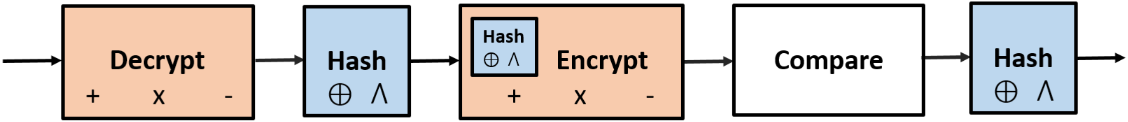
- Need to convert between arithmetic and Boolean masking.
- Efficient classical masks conversions exist.



Arithmetic and Boolean Masking

Masks Conversions

- Need to convert between arithmetic and Boolean masking.
- Efficient classical masks conversions exist.



Difference with previous schemes

- **Classical schemes:** k-bit Boolean $\Leftrightarrow$ arithmetic modulo 2^k; usually $k = 32$
- **ML-KEM:** k-bit Boolean $\Leftrightarrow$ arithmetic modulo q; **arbitrary** k, q

Many new problematics to secure ML-KEM

Arbitrary Masks Conversions

- Generic conversions suitable for ML-KEM exist.
- Downside: Can be too costly in practice.

Many new problematics to secure ML-KEM

Arbitrary Masks Conversions

- Generic conversions suitable for ML-KEM exist.
- Downside: Can be too costly in practice.

Other problematics to secure ML-KEM (prime $q = 3329$)

- Encryption function: $\lfloor q/2 \rceil \cdot m$
- Centered Binomial Distribution: $HW(x) - HW(y)$
- Decryption function: $\lceil (2/q) \cdot x \rfloor \bmod 2$
- $\text{Compress}_{q,d}(x)$ function: $\lceil (2^d/q) \cdot x \rfloor \bmod 2^d$
- Polynomials comparison: $X \;\; =? \;\; Y$

Many new problematics to secure ML-KEM

Arbitrary Masks Conversions

- Generic conversions suitable for ML-KEM exist.
- Downside: Can be too costly in practice.

Other problematics to secure ML-KEM (prime $q = 3329$)

- Encryption function: $\lfloor q/2 \rceil \cdot m$
- Centered Binomial Distribution: $HW(x) - HW(y)$
- Decryption function: $\lceil (2/q) \cdot x \rfloor \bmod 2$
- $\text{Compress}_{q,d}(x)$ function: $\lceil (2^d/q) \cdot x \rfloor \bmod 2^d$
- Polynomials comparison: $X \; =? \; Y$

☞ **Need specific solution for each problem**

ML-KEM Encryption (prime $q = 3329$)

Encryption Problematic (First order): Securely compute $\lfloor q/2 \rceil \cdot m$

- We have $m = m_1 \oplus m_2$ where m_1, m_2 are 1-bit long.
- Compute $y_1 + y_2 \bmod q = 1665 \cdot (m_1 \oplus m_2)$.

ML-KEM Encryption (prime $q = 3329$)

Encryption Problematic (First order): Securely compute $\lfloor q/2 \rceil \cdot m$

- We have $m = m_1 \oplus m_2$ where m_1, m_2 are 1-bit long.
- Compute $y_1 + y_2 \bmod q = 1665 \cdot (m_1 \oplus m_2)$.

Encryption Solution

Convert 1-bit **Boolean** sharing m_1, m_2 into **arithmetic** modulo q

- Use generic solution
- Use [1] with better efficiency (CHES 2022)

[1] *High-order Table-based Conversion Algorithms and Masking Lattice-based Encryption.* Coron, Gérard, Montoya, Zeitoun, CHES'22.

ML-KEM Encryption (prime $q = 3329$)

Encryption Problematic (First order): Securely compute $\lfloor q/2 \rceil \cdot m$

- We have $m = m_1 \oplus m_2$ where m_1, m_2 are 1-bit long.
- Compute $y_1 + y_2 \bmod q = 1665 \cdot (m_1 \oplus m_2)$.

Encryption Solution

Convert 1-bit **Boolean** sharing m_1, m_2 into **arithmetic** modulo q

- Use generic solution
- Use [1] with better efficiency (CHES 2022)

Centered Binomial Distribution (CBD):

- Similar problematic and solution to securely compute $e = HW(x) - HW(y)$ in CBD.

ML-KEM Encryption (prime $q = 3329$)

Encryption Problematic (First order): Securely compute $\lfloor q/2 \rceil \cdot m$

- We have $m = m_1 \oplus m_2$ where m_1, m_2 are 1-bit long.
- Compute $y_1 + y_2 \bmod q = 1665 \cdot (m_1 \oplus m_2)$.

Encryption Solution

Convert 1-bit **Boolean** sharing m_1, m_2 into **arithmetic** modulo q

- Use generic solution
- Use [1] with better efficiency (CHES 2022)

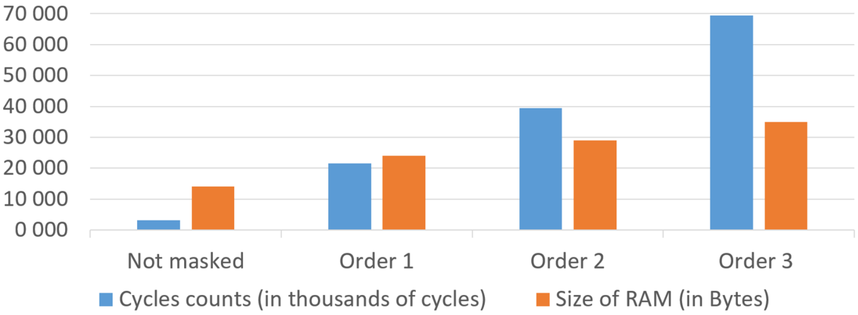
Centered Binomial Distribution (CBD):

- Similar problematic and solution to securely compute $e = HW(x) - HW(y)$ in CBD.

Other problematics and solutions in [1] and [2] (references on next slide)

Fully masked implementation of ML-KEM [1], [2]

ML-KEM-768 Decapsulation on ARM Cortex-M3 for given security order:



- For security order $t > 3$, required RAM too large for ARM Cortex-M3 target device.
- In practice: acceptable on smartcards (security order 1 and 2).

[1] *High-order Table-based Conversion Algorithms and Masking Lattice-based Encryption.* Coron, Gérard, Montoya, Zeitoun, CHES'22.
[2] *High-order Polynomial Comparison and Masking Lattice-based Encryption.* Coron, Gérard, Montoya, Zeitoun, CHES'23.

Outline

1 › Context

2 › Case Study: ML-KEM

3 › **Quantum-Safe Proofs of Concept**

4 › Conclusion

Quantum-Safe Proofs of Concept

Payment Transaction

- Quantum-safe EMV transaction
- Quantum-safe offline CBDC solution
- P2P payment migration (national scheme)

5G

- Quantum-safe IMSI encryption
- Quantum-safe Profile Download for eUICC
- Quantum-safe crypto-agility for eUICC

Identity

- Quantum-safe Passport Reading
- Quantum-safe version of Personal Identity Verification (PIV) card
- Quantum-safe FIDO WG

Critical Devices

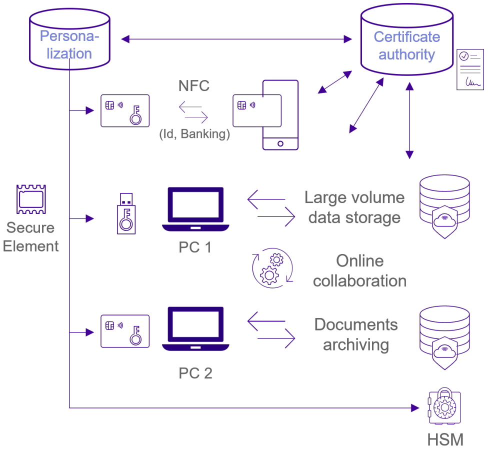
- Quantum-safe TLS secured by SIM for critical devices
- Crypto-agility for critical devices

Data Protection

- HYPERFORM: research program for end-to-end data encryption
  - workstation / data at rest / data in transfer / collaborative space quantum-safe encryption

Project HYPERFORM: data protection

- Major R&D program in Europe on Quantum-safe data protection
- Funded by France 2030 Research Program
- 3 years research program (2023 - 2026)
- 8 French partners
- A reference platform implemented in practice
- Including Secure Element, Cloud and PC
- Implement hybrid crypto and crypto-agility



Outline

1 ❭ Context

2 ❭ Case Study: ML-KEM

3 ❭ Quantum-Safe Proofs of Concept

4 ❭ Conclusion

Conclusion

Smartcards:

- Embedded systems: optimizations are essential for PQC deployment.
- Many practical physical attacks published on ML-KEM.
- Real need to secure implementations against all SCA and FA.

Countermeasures:

- New challenges to secure ML-KEM against SCA.
- Solutions are not trivial and can imply non-negligible overhead.

In practice:

- IDEMIA has implemented several quantum-safe Proofs of Concepts.

Going Forward:

- Research and implementations on going (*e.g.* with project HYPERFORM).
- Upcoming large-scale deployment of quantum-safe products.

Thank you for your attention!

rina.zeitoun@idemia.com

IDEMIA GROUP

www.idemia.com