ETSI/IQC Quantum Safe Cryptography Event

The Challenge of Side-Channel Countermeasures on Post-Quantum Crypto

Rina Zeitoun - rina.zeitoun@idemia.com

IDEMIA - Crypto & Security Labs

13 - 15 February, 2023

OUTLINE

1 › Context

2 › Side-channel Attacks on Lattice-based KEM

3 › Masking and Conversions Problematics

4 › The example of Kyber

5 › Conclusion

CONTEXT

IDEMIA: The leader in identity technologies

- Identity (3B ID docs, 5M biometric terminals).
- Payment (800M payment products - 2022).
- Telecoms (900M SIM cards - 2022).

Into the wild

- Our products are deployed in hostile environments.
- Attackers have physical access to the device.
- Must be resistant to side-channel/fault attacks.

☞ Security against side-channel attacks is **mandatory**.

SIDE-CHANNEL ATTACKS

Main Powerful Attacks

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

Into Specifications of Selected NIST PQC Algorithms

- Resistance to Timing Attacks is always addressed.
- All other attacks are mainly **left for research**.

Smartcards: In real life

- Timing attacks are indeed important to consider.
- But **all** other classical side-channel attacks are definitely **real threats**!
- Main powerful attacks should **systematically** be studied in NIST submissions.

OUTLINE

1 › Context

2 › Side-channel Attacks on Lattice-based KEM

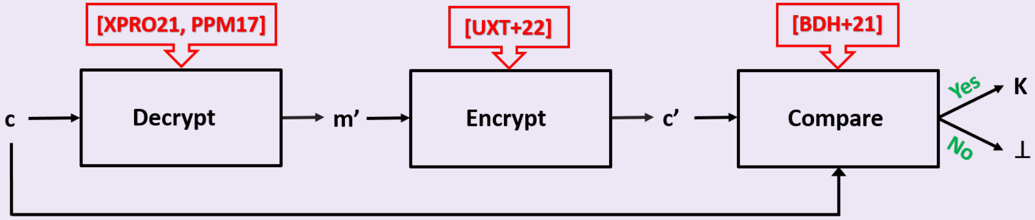
3 › Masking and Conversions Problematics

4 › The example of Kyber

5 › Conclusion

SIDE-CHANNEL ATTACKS ON LATTICE-BASED KEM

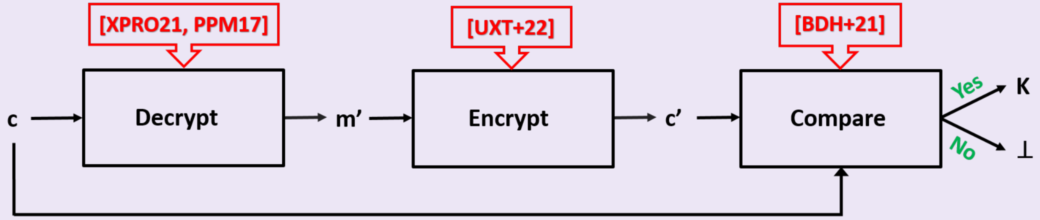
Power/EM Attacks on Decapsulation based on FO Transform



☞ **Whole Decapsulation needs to be protected**

SIDE-CHANNEL ATTACKS ON LATTICE-BASED KEM

Power/EM Attacks on Decapsulation based on FO Transform



☞ **Whole Decapsulation needs to be protected**

Template Attacks on Key Generation

- Template attacks require detailed knowledge of target but can be a real threat!
- Investigated in security certifications (Common Criteria and EMVco).

OUTLINE

1 › Context

2 › Side-channel Attacks on Lattice-based KEM

3 › Masking and Conversions Problematics

4 › The example of Kyber

5 › Conclusion

MASKING COUNTERMEASURE

High-Order Masking Countermeasure

- Each sensitive variable x is shared into n variables: $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$
- Manipulate $x_1, x_2, \ldots, x_n$ independently

MASKING COUNTERMEASURE

High-Order Masking Countermeasure

- Each sensitive variable x is shared into n variables: $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$
- Manipulate $x_1, x_2, \ldots, x_n$ independently

Computing with Boolean Masking

Given $x = x_1 \oplus \cdots \oplus x_n$ and $y = y_1 \oplus \cdots \oplus y_n$, how can we compute $x \oplus y$?

- Compute $x_1 \oplus y_1, \cdots, x_n \oplus y_n$

MASKING COUNTERMEASURE

High-Order Masking Countermeasure

- Each sensitive variable x is shared into n variables: $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$
- Manipulate $x_1, x_2, \ldots, x_n$ independently

Computing with Boolean Masking

Given $x = x_1 \oplus \cdots \oplus x_n$ and $y = y_1 \oplus \cdots \oplus y_n$, how can we compute $x \oplus y$?

- Compute $x_1 \oplus y_1, \cdots, x_n \oplus y_n$

Arithmetic Masking Countermeasure

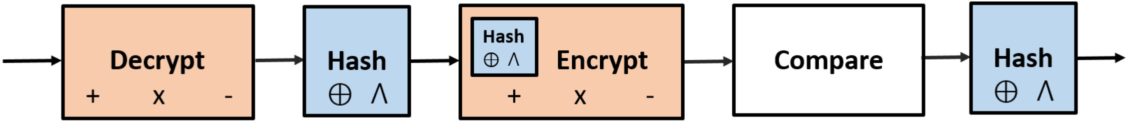
Generate arithmetic sharings s.t. $x = x_1 + \cdots + x_n \mod 2^k$ and $y = y_1 + \cdots + y_n \mod 2^k$

- Compute $x_1 + y_1 \mod 2^k, \cdots, x_n + y_n \mod 2^k$

ARITHMETIC AND BOOLEAN MASKING

Masks Conversions

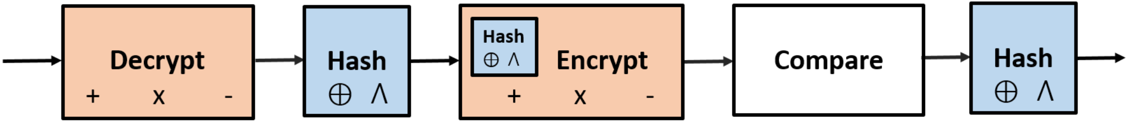
- Need to convert between arithmetic and Boolean masking.
- Efficient classical masks conversions exist ([Gou01],[CGV14],[CGTV15],[BCZ18], etc.)



ARITHMETIC AND BOOLEAN MASKING

Masks Conversions

- Need to convert between arithmetic and Boolean masking.
- Efficient classical masks conversions exist ([Gou01],[CGV14],[CGTV15],[BCZ18], etc.)



Difference with previous schemes

- **Symmetric schemes:** k-bit Boolean $\Leftrightarrow$ arithmetic modulo 2^k; usually $k = 32$
- **Post-Quantum schemes:** k-bit Boolean $\Leftrightarrow$ arithmetic modulo q; **arbitrary** k, q

NEW PROBLEMATICS WITH POST-QUANTUM CRYPTO

Arbitrary Masks Conversions

- Generic conversions suitable for PQ schemes exist ([BBE+18]: generalization of [CGTV15])
- Downside: Can be too costly in practice

NEW PROBLEMATICS WITH POST-QUANTUM CRYPTO

Arbitrary Masks Conversions

- Generic conversions suitable for PQ schemes exist ([BBE+18]: generalization of [CGTV15])
- Downside: Can be too costly in practice

Other Problematics

- Secure polynomials comparison (Kyber, Dilithium)
- Secure computation of compression: $\lceil (2^d/q) \cdot x \rfloor \bmod 2^d$ (Kyber)
- Secure generation of a random in a given interval (Dilithium)
- Secure Euclidean division (NTRU, Dilithium)
- etc.

NEW PROBLEMATICS WITH POST-QUANTUM CRYPTO

Arbitrary Masks Conversions

- Generic conversions suitable for PQ schemes exist ([BBE+18]: generalization of [CGTV15])
- Downside: Can be too costly in practice

Other Problematics

- Secure polynomials comparison (Kyber, Dilithium)
- Secure computation of compression: $\lceil (2^d/q) \cdot x \rfloor \bmod 2^d$ (Kyber)
- Secure generation of a random in a given interval (Dilithium)
- Secure Euclidean division (NTRU, Dilithium)
- etc.

☞ **Need specific solution for each problem**

OUTLINE

1 › Context

2 › Side-channel Attacks on Lattice-based KEM

3 › Masking and Conversions Problematics

4 › **The example of Kyber**

5 › Conclusion

KYBER MASKING PROBLEMATICS AND SOLUTIONS

Many problematics to secure Kyber (prime $q = 3329$)

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

KYBER MASKING PROBLEMATICS AND SOLUTIONS

Many problematics to secure Kyber (prime $q = 3329$)

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

Encryption Problematic: Securely compute $\lfloor q/2 \rceil \cdot m$

- We have $m = m_1 \oplus \cdots \oplus m_n$ where m_i are 1-bit long.
- Compute $y_1 + \cdots + y_n \bmod q = 1665 \cdot (m_1 \oplus \cdots \oplus m_n)$.

KYBER MASKING PROBLEMATICS AND SOLUTIONS

Many problematics to secure Kyber (prime $q = 3329$)

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

Encryption Problematic: Securely compute $\lfloor q/2 \rceil \cdot m$

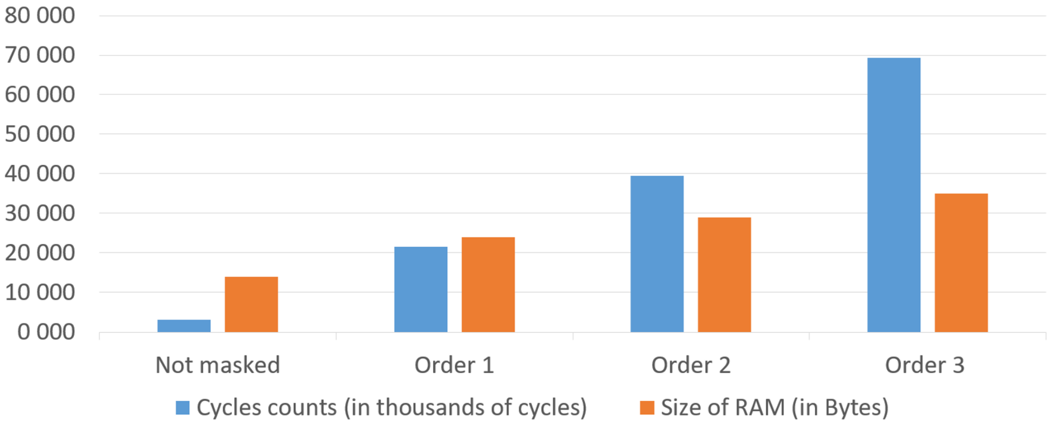
- We have $m = m_1 \oplus \cdots \oplus m_n$ where m_i are 1-bit long.
- Compute $y_1 + \cdots + y_n \bmod q = 1665 \cdot (m_1 \oplus \cdots \oplus m_n)$.

Solution: Convert 1-bit Boolean sharing $m_1, \cdots, m_n$ **into arithmetic modulo** q

- [BBE+18]: complexity $\mathcal{O}(n^2 \cdot \log\log q)$.
- [SPOG19] or [CGMZ21a]: complexity $\mathcal{O}(n^2)$.

FULLY MASKED IMPLEMENTATION OF KYBER [CGMZ21A/B]

Kyber768 Decapsulation on ARM Cortex-M3 for given security order:



- For security order $t > 3$, required RAM too large for ARM Cortex-M3 target device.

OUTLINE

1 〉 Context

2 〉 Side-channel Attacks on Lattice-based KEM

3 〉 Masking and Conversions Problematics

4 〉 The example of Kyber

5 〉 **Conclusion**

CONCLUSION

Smartcards:

- Real need to secure implementations against all SCA.

Standard specifications:

- Resistance against timing attacks studied in standardized PQ algorithms.
- Other Side-Channel Attacks (Power/EM DPA, templates, fault) mainly left for research.

Attacks in practice:

- Many practical Side-Channel Attacks published.

Countermeasures:

- New challenges for PQ crypto countermeasures.
- Not trivial and imply large overhead (can be unacceptable for many products).

Going Forward:

- Encourage designers to study classical SCA at an early stage ("Masking friendly" PQ crypto).

BIBLIOGRAPHY

- [Gou01] *A Sound Method for Switching between Boolean and Arithmetic Masking.* Goubin, CHES'01.
- [CGV14] *Secure Conversion Between Boolean and Arithmetic Masking of Any Order.* Coron, Grobschadl, Vadnala, CHES'14.
- [CGTV15] *Conversion from Arithmetic to Boolean Masking with Logarithmic Complexity.* Coron, Grobschadl, Tibouchi, Vadnala, FSE'15.
- [BCZ18] *Improved High-Order Conversion From Boolean to Arithmetic.* Bettale, Coron, Zeitoun, CHES'18.
- [BBE+18] *Masking the GLP Lattice-Based Signature Scheme at Any Order.* Barthe, Belaïd, Espitau, Fouque, Grégoire, Rossi, Tibouchi, EUROCRYPT'18.
- [SPOG19] *Efficiently Masking Binomial Sampling at Arbitrary Orders for Lattice-Based Crypto.* Schneider, Paglialonga, Oder, Güneysu, PKC'19.
- [CGMZ21a] *High-order Table-based Conversion Alg. and Masking Lattice-based Encryption.* Coron, Gérard, Montoya, Zeitoun, CHES'22.
- [CGMZ21b] *High-order Polynomial Comparison and Masking Lattice-based Encryption.* Coron, Gérard, Montoya, Zeitoun, CHES'23.
- [PPM17] *Single-trace side-channel attacks on masked lattice-based encryption.* Primas, Pessl, Mangard, CHES'17.
- [XPRO21] *Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of Kyber.* Xu, Pemberton, Roy, Oswald, IEEE'21.
- [BDH+21] *Attacking and defending masked polynomial comparison for lattice-based cryptography.* Bhasin, D'Anvers, Heinz, Poppelmann, Beirendonck, CHES'21.
- [UXT+22] *Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs.* Ueno, Xagawa, Tanaka, Ito, Takahashi, Homma, CHES'22.

Thank you for your attention!

rina.zeitoun@idemia.com

IDEMIA

Join us on

www.idemia.com