# Challenges and Pathways in the Migration to Post-Quantum Cryptography

**Maria Isabel González Vasco**

Universidad Carlos III de Madrid

uc3m

European Conference on PQC Migration

# The Stage: A New Cryptographic Epoch

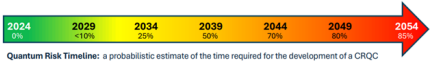
# The Quantum Menace

ARE WE THERE YET??

# The Quantum Menace

ARE WE THERE YET??


- Quantum cryptanalytic techniques advance and will become practical in...

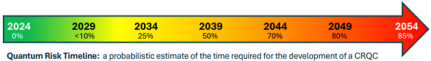



[Figure from *An updated Methodology for Quantum Risk Assessment*, M. Mosca and J. Mulholland, Global Risk Institute, Sept. 2025]

# The Quantum Menace

ARE WE THERE YET??


- Quantum cryptanalytic techniques advance and will become practical in...




[Figure from *An updated Methodology for Quantum Risk Assessment*, M. Mosca and J. Mulholland, Global Risk Institute, Sept. 2025]

- Cryptographically Relevant Quantum Computers may not materialize in the near term but...how about dedicated hardware for cryptanalysis?

# You and whose army?

A fair question: How relevant will quantum algorithms ultimately be in practice?

# You and whose army?

A fair question: How relevant will quantum algorithms ultimately be in practice?

- It remains unclear how to estimate the speed of quantum algorithms in solving different mathematical problems (and thus, fixing concrete long-term parameters for cryptographic primitives is hard).

# You and whose army?

A fair question: How relevant will quantum algorithms ultimately be in practice?

- It remains unclear how to estimate the speed of quantum algorithms in solving different mathematical problems (and thus, fixing concrete long-term parameters for cryptographic primitives is hard).
- It is challenging to characterize or reliably identify problems that are particularly amenable to quantum speed-ups.

# You and whose army?

A fair question: How relevant will quantum algorithms ultimately be in practice?

- It remains unclear how to estimate the speed of quantum algorithms in solving different mathematical problems (and thus, fixing concrete long-term parameters for cryptographic primitives is hard).
- It is challenging to characterize or reliably identify problems that are particularly amenable to quantum speed-ups.

The only proper answer: DO YOU INTEND TO LEARN THIS THE HARD WAY?
—instead, be prepared!

# The Road to Quantum Resistance

# Quantum, Post-Quantum, Future-Quantum & Friends

- What kind of adversarial models make sense?
  - Make your security concerns precise (e.g., HNDL attacks call for transcript-protection mechanisms)
  - Understand quantum adversarial actions (Quantum **BAD GUYS** are not mere factoring oracles)

# Quantum, Post-Quantum, Future-Quantum & Friends

- What kind of adversarial models make sense?
  - Make your security concerns precise (e.g., HNDL attacks call for transcript-protection mechanisms)
  - Understand quantum adversarial actions (Quantum **BAD GUYS** are not mere factoring oracles)
- Establish the grade of cryptographic strength you aim at (oversimplified):
  - Future Quantum: (pre-quantum authentication is just fine, v.g., OK to mix pre-quantum signatures with post-quantum time stamps)
  - Full quantum resistance: use post-quantum tools, mathematically proven secure against quantum adversaries
  - Anything in between? (e.g. QROM and Factoring/Dlog oracles)

# Migration to Quantum resistant tools

Two actions towards understanding what needs to be done (and how... and when!)

# Migration to Quantum resistant tools

Two actions towards understanding what needs to be done (and how... and when!)

- In search for (clear) guidelines
  - Standardization bodies (NIST, ETSI, IETF, ISO/IEC..)
  - National strategic guidelines (In Spain, See CCN-TEC 009, CCN-Stic 221)
  - Cross-national guidelines (EU directives and EC Commission Roadmap recommendations)

# Migration to Quantum resistant tools

Two actions towards understanding what needs to be done (and how... and when!)

- In search for (clear) guidelines
  - Standardization bodies (NIST, ETSI, IETF, ISO/IEC..)
  - National strategic guidelines (In Spain, See CCN-TEC 009, CCN-Stic 221)
  - Cross-national guidelines (EU directives and EC Commission Roadmap recommendations)
- In-house analysis (know yourself)
  - Cryptographic inventories
  - Rethink your (current & future!) needs

# The Rough Patches: Theoretical, Technical and Practical Limitations

# Theory matters

Security models may look overly abstract or distant from real life (they are not!). It is crucial to understand adversarial goals and capabilities (and how that translates into parameter choices)

# Theory matters

Security models may look overly abstract or distant from real life (they are not!). It is crucial to understand adversarial goals and capabilities (and how that translates into parameter choices)

Example: Hybrids done wrong [Bindel, N. et al. *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange.* PQCrypto 2019]

**PLAIN XOR-COMBINER IS INSECURE**

*If given $KEM_1, KEM_2$ we build a KEM so that $Encaps(pk_1||pk_2)$ outputs $(c_1||c_2, k_1 \oplus k_2)$, then a Decaps oracle trivially breaks the security of the scheme — just query it for $(c_1||c_{whatever})$ and $(c_{something}||c_2)$ for known $k_{whatever}$ and $k_{something}$!!*

# Theory matters

Security models may look overly abstract or distant from real life (they are not!). It is crucial to understand adversarial goals and capabilities (and how that translates into parameter choices)

Example: Hybrids done wrong [Bindel, N. et al. *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange.* PQCrypto 2019]

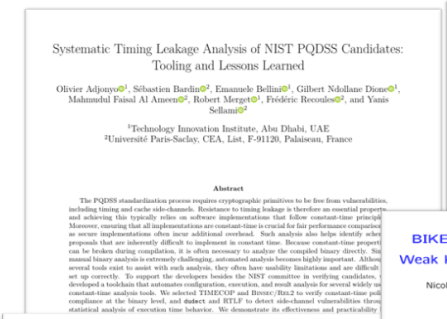
**PLAIN XOR-COMBINER IS INSECURE**

*If given $KEM_1, KEM_2$ we build a KEM so that $Encaps(pk_1||pk_2)$ outputs $(c_1||c_2, k_1 \oplus k_2)$, then a Decaps oracle trivially breaks the security of the scheme — just query it for $(c_1||c_{whatever})$ and $(c_{something}||c_2)$ for known $k_{whatever}$ and $k_{something}$!!*

Side note: Hybrids involving QKD are even more involved... see our NATO SPS project

https://www.quantum-safe-cryptography.science/

# Theory is tidy–practice is not.



Systematic Timing Leakage Analysis of NIST PQDSS Candidates: Tooling and Lessons Learned

Olivier Adjonyo[1], Sébastien Bardin[2], Emanuele Bellini[1], Gilbert Ndollane Dione[1], Mahmudul Faisal Al Ameen[2], Robert Merget[1], Frédéric Recoules[2], and Yanis Sellami[2]

[1]Technology Innovation Institute, Abu Dhabi, UAE
[2]Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France

Abstract

The PQDSS standardisation process requires cryptographic primitives to be free from vulnerabilities, including timing and cache side-channels. Resistance to timing leakage is therefore an essential property and achieving this typically relies on software implementations that follow constant-time principles. Moreover, ensuring that all implementations are constant-time is crucial for fair performance comparisons as secure implementations often incur additional overhead. Such analysis also helps identify schemes proposals that are inherently difficult to implement in constant time. Because constant-time properties can be broken during compilation, it is often necessary to analyze the compiled binary directly. Since manual binary analysis is extremely challenging, automated analysis becomes highly important. Although several tools exist to assist with such analysis, they often have usability limitations and are difficult to set up correctly. To support the developers besides the NIST committee in verifying candidates, we developed a toolchain that automates configuration, execution, and result analysis for several widely used constant-time analysis tools. We selected TIMECOP and BINSEC/REL2 to verify constant-time policy compliance at the binary level, and dudect and RTLF to detect side-channel vulnerabilities through statistical analysis of execution time behavior. We demonstrate its effectiveness and practicability

Journal of Cryptographic Engineering (2023) 13:443–460
https://doi.org/10.1007/s13389-023-00315-3

REGULAR PAPER

A side-channel attack on a masked and shuffled software implementation of Saber

Kalle Ngo[1] · Elena Dubrova[1] · Thomas Johansson[2]

Received: 12 June 2022 / Accepted: 28 February 2023 / Published online: 25 April 2023
© The Author(s) 2023

BIKE Decoding Failure Weak Keys & Error Floors

Nicolas Sendrier, Inria, France

NIST PQC Seminars, September 27, 2024



Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results

PRASANNA RAVI, School of Computer Science and Engineering, Nanyang Technological University, Singapore
ANUPAM CHATTOPADHYAY, Temasek Labs, Nanyang Technological University, Singapore
JAN PIETER D'ANVERS, imec-COSIC, KU Leuven, Belgium
ANUBHAB BAKSI, Temasek Labs, Nanyang Technological University, Singapore

stematic study of Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA) chemes, with main focus on Kyber Key Encapsulation Mechanism (KEM) and which are leading candidates in the NIST standardization process for Post-C). Throu existing at multaneo for both riding defi res within s work, w -based ch well-kno oller and ARM Cortex-A53 processor. Our perfor ncur reasonable performance overhea our work argues for usage of custom schemes, either in a standalone manne CCS Concepts: • Security and privac

Additional Key Words and Phrases: Lat
Kyber, Dilithium



Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

**Abstract.** This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

# In a nutshell...

If you are designing PQC implementations, worry about:

- Constant-time discipline (timing and cache)– REMEMBER KYBERSLASH

# In a nutshell...

If you are designing PQC implementations, worry about:

- Constant-time discipline (timing and cache)– REMEMBER KYBERSLASH
- Side-channel hardening and testing (power/EM, deep-learning SCA).

# In a nutshell...

If you are designing PQC implementations, worry about:

- Constant-time discipline (timing and cache)– **REMEMBER KYBERSLASH**
- Side-channel hardening and testing (power/EM, deep-learning SCA).
- Key-space pathologies (weak keys, bad parameter choices)—**REMEMBER BIKE**

# In a nutshell...

If you are designing PQC implementations, worry about:

- Constant-time discipline (timing and cache)– **REMEMBER KYBERSLASH**
- Side-channel hardening and testing (power/EM, deep-learning SCA).
- Key-space pathologies (weak keys, bad parameter choices)—**REMEMBER BIKE**
- Crypto-agility and deprecation plans in case an algorithm is broken —**REMEMBER RAINBOW**.

# In a nutshell...

If you are designing PQC implementations, worry about:

- Constant-time discipline (timing and cache)– **REMEMBER KYBERSLASH**
- Side-channel hardening and testing (power/EM, deep-learning SCA).
- Key-space pathologies (weak keys, bad parameter choices)—**REMEMBER BIKE**
- Crypto-agility and deprecation plans in case an algorithm is broken —**REMEMBER RAINBOW**.
- Protocol integration costs — **TLS**(larger keys and ciphertext may blow up handshake size, certificate chains get heavier–). Even if the algorithm is secure and the implementation is SC resistant, protocol and infrastructure issues can make deployment fragile or inefficient.

# Lessons Learned: Keys to a Quantum-Secure Future

# Take home

- Decide on the quantum resistance level you want (or can afford) to pursue.

# Take home

- Decide on the quantum resistance level you want (or can afford) to pursue.
- Read the standards, drafts, and white papers and make sure you truly understand how they map to your needs.

# Take home

- Decide on the quantum resistance level you want (or can afford) to pursue.
- Read the standards, drafts, and white papers and make sure you truly understand how they map to your needs.
- Talk to the experts: the theorists who design the schemes and the engineers who know how to implement and integrate PQC in the real world. Even better: hire them!

# Take home

- Decide on the quantum resistance level you want (or can afford) to pursue.
- Read the standards, drafts, and white papers and make sure you truly understand how they map to your needs.
- Talk to the experts: the theorists who design the schemes and the engineers who know how to implement and integrate PQC in the real world. Even better: hire them!
- Never forget: even the strongest cryptographic designs can crumble under sloppy implementation or careless integration.

# Take home

- Decide on the quantum resistance level you want (or can afford) to pursue.
- Read the standards, drafts, and white papers and make sure you truly understand how they map to your needs.
- Talk to the experts: the theorists who design the schemes and the engineers who know how to implement and integrate PQC in the real world. Even better: hire them!
- Never forget: even the strongest cryptographic designs can crumble under sloppy implementation or careless integration.
- And remember: nothing stays stable for as long as it used to—that might even be a good thing!

# Challenges and Pathways in the Migration to Post-Quantum Cryptography

**Maria Isabel González Vasco**

Universidad Carlos III de Madrid

uc3m

European Conference on PQC Migration