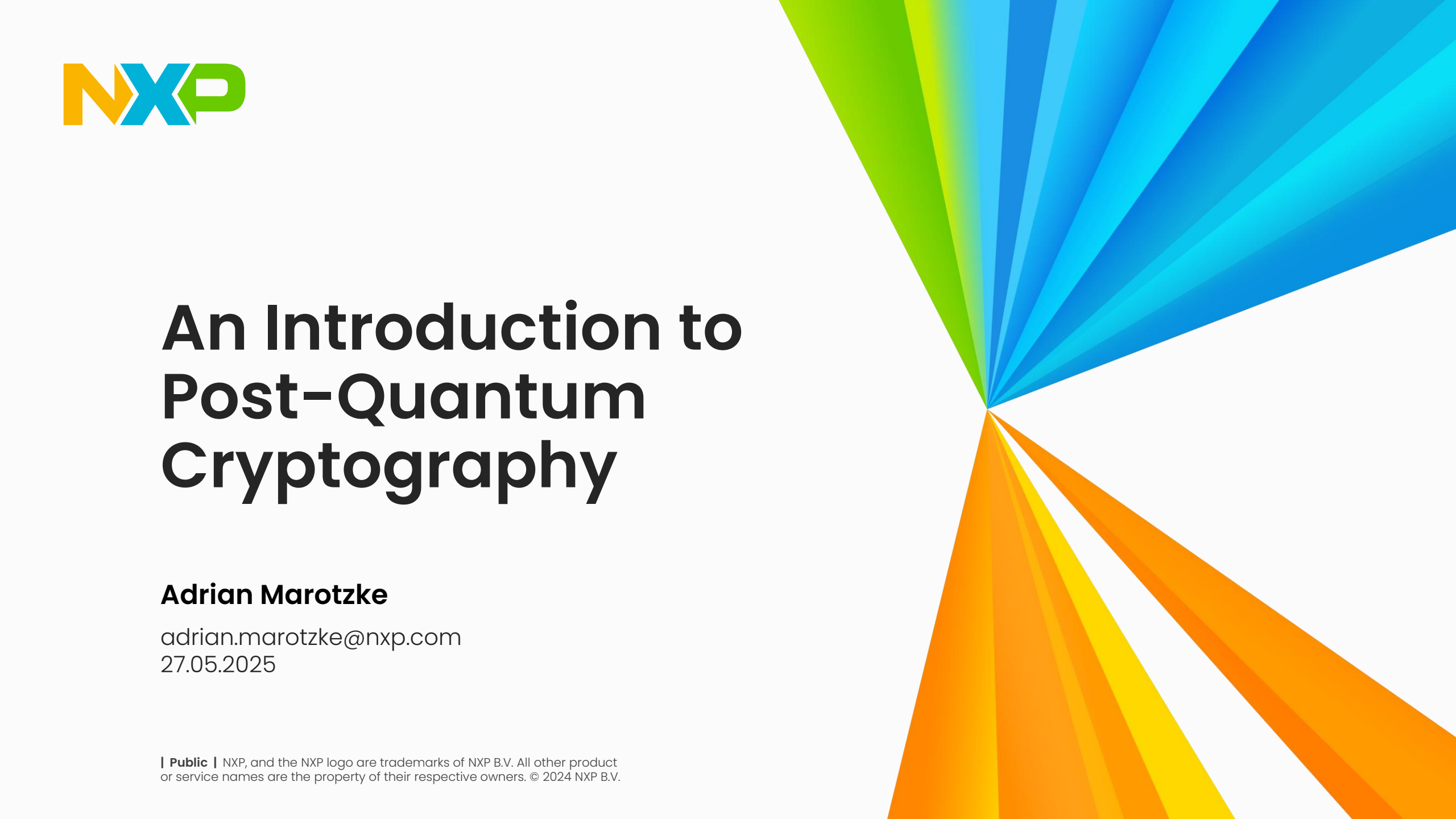


# An Introduction to Post-Quantum Cryptography

**Adrian Marotzke**

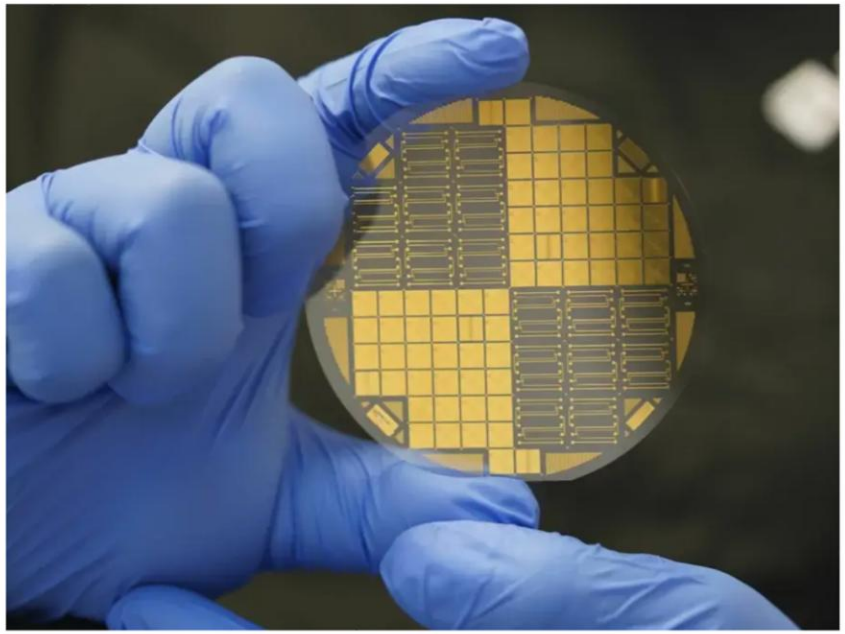
adrian.marotzke@nxp.com
27.05.2025

TUHH | TU HAMBURG | STUDIUM UND LEHRE | FORSCHUNG UND TRANSFER | DEKANATE | INTERNATIONAL | DE

## Startschuss für Hamburg Quantencomputing

**Gemeinschaftsprojekt der Universität Hamburg und TU Hamburg zur Entwicklung zukünftiger Quantencomputer**

01.07.2024



Source: QUDORA Technologies

A project of

QUDORA TECHNOLOGIES

NXP

## XAPHIRO – Prototype trapped-ion quantum computer with at least 50 qubits

## NXP, eleQtron and ParityQC Reveal their First Quantum Computing Demonstrator for the DLR Quantum Computing Initiative

May 30, 2024 2:00 PM CEST (UTC+2) by NXP Semiconductors Press Release

SHARE

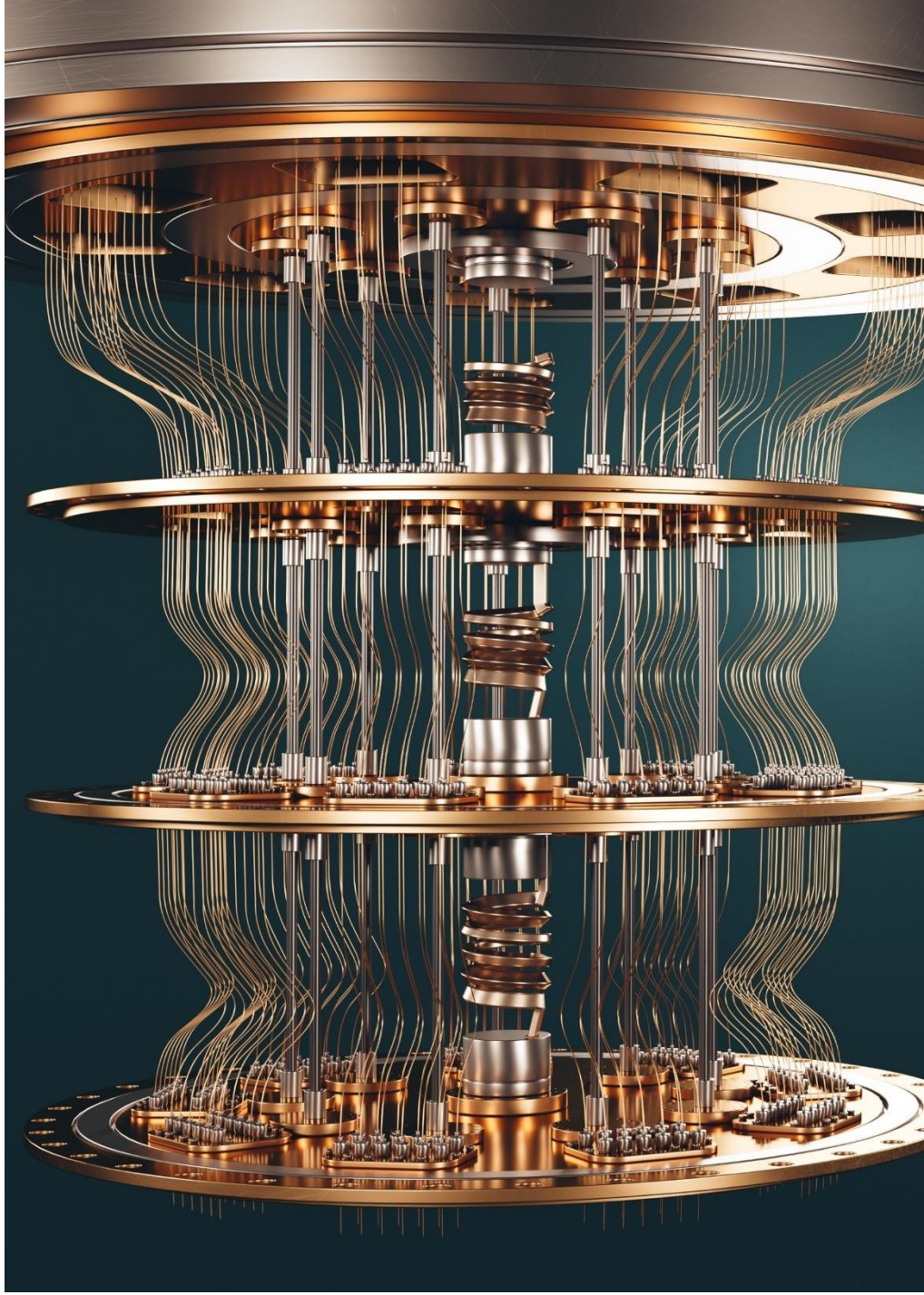
- NXP, eleQtron and ParityQC present the first full-stack, ion-trap based quantum computer demonstrator made entirely in Germany
- It was commissioned by the DLR Quantum Computing Initiative (DLR QCI) to expand the quantum expertise of its partners from research and industry
- DLR will make the demonstrator accessible to industry players and academia to strengthen the quantum ecosystem and boost knowledge around quantum computing




https://intranet.tuhh.de/presse/pressemitteilung_einzeln.php?id=14695
https://www.nxp.com/company/about-nxp/newsroom/NW-NXP-ELEQTRON-AND-PARITYQC-FIRST-QUANTUM
https://qci.dlr.de/en/xaphiro/

# Quantum computers

- Use quantum mechanical effects for computation
- Promise to solve problems not feasible for classical computers
- Shor 1994: Algorithm that computes integer factorization & discrete logarithms in polynomial time on a QC
- Would break RSA and ECC schemes!
- Would break our digital infrastructure ☹



# Shor's & Grover's Algorithm

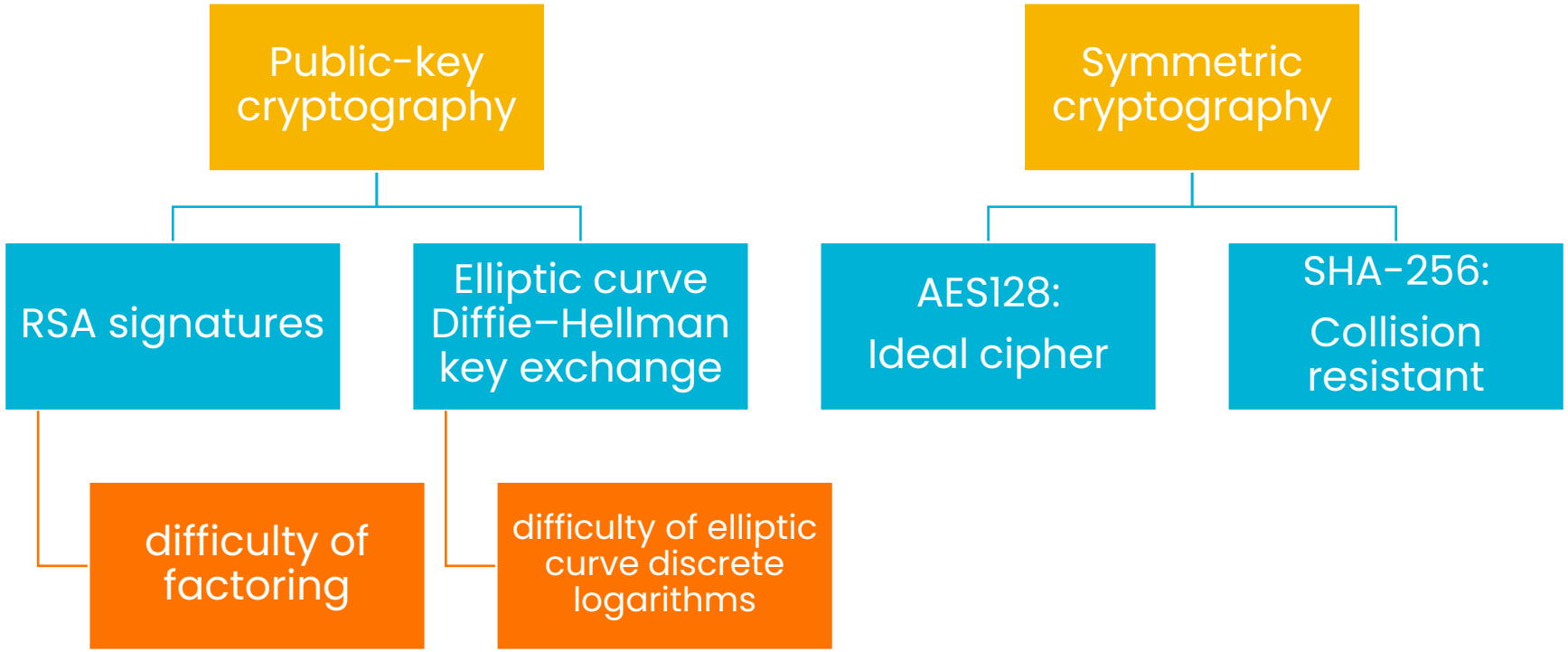
- Shor 1994: Solves factoring & discrete logarithms in polynomial time on a QC
  - ~ 6000 logical ("perfect") qubits
  - ~ 20 million physical qubits (2019) [1]
  - ~ 1 million physical qubits (2025) [2]

- Grover 1996: Unstructured search accelerated by square root
  - Brute force key search can be modeled as unstructured search

[1] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Craig Gidney and Martin Ekerå
[2] How to factor 2048 bit RSA integers with less than a million noisy qubits. Craig Gidney

# Contemporary cryptography

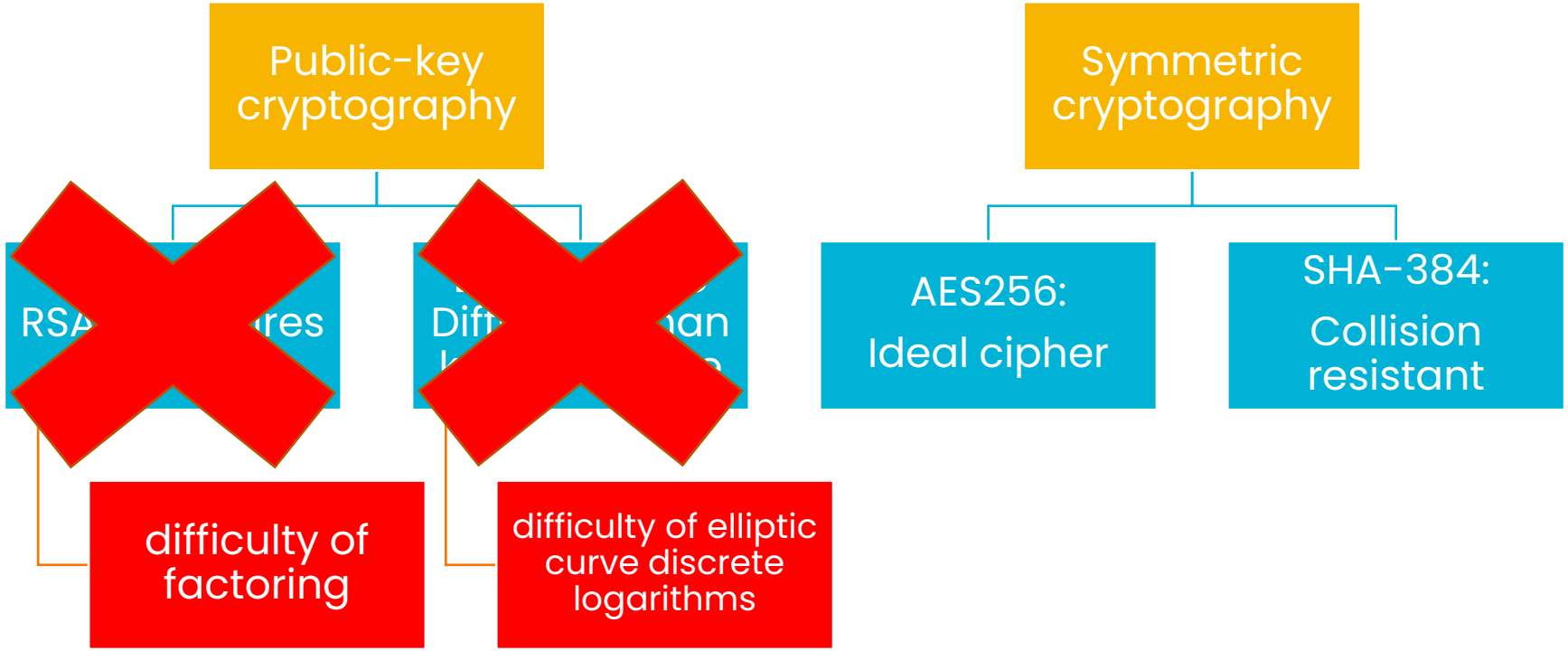
## TLS-ECDHE-RSA-AES128-GCM-SHA256



# Contemporary cryptography

## TLS-~~ECDHE-RSA~~-AES256-GCM-SHA384

"Double" the key sizes



# So when is it going to be here ?

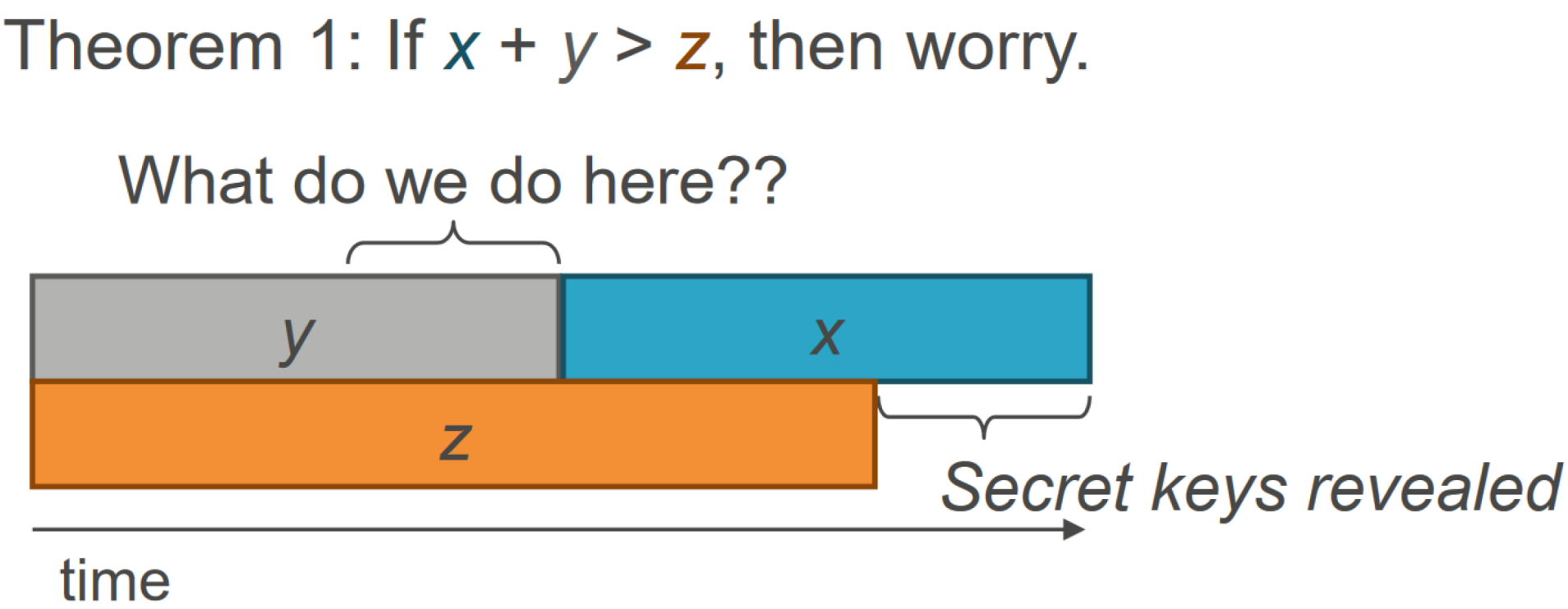
"I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031."

— Michele Mosca, November 2015
https://eprint.iacr.org/2015/1075

It is difficult to make predictions, especially about the future. (Danish proverb)

Michele Mosca. Cybersecurity in a Quantum World: Will we be ready? https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

# We have to be ready: Store now, decrypt later attack




- z is the time until a CRQC becomes reality
- y is the time to migrate to PQC
- x is the time that sensitive information must remain secret

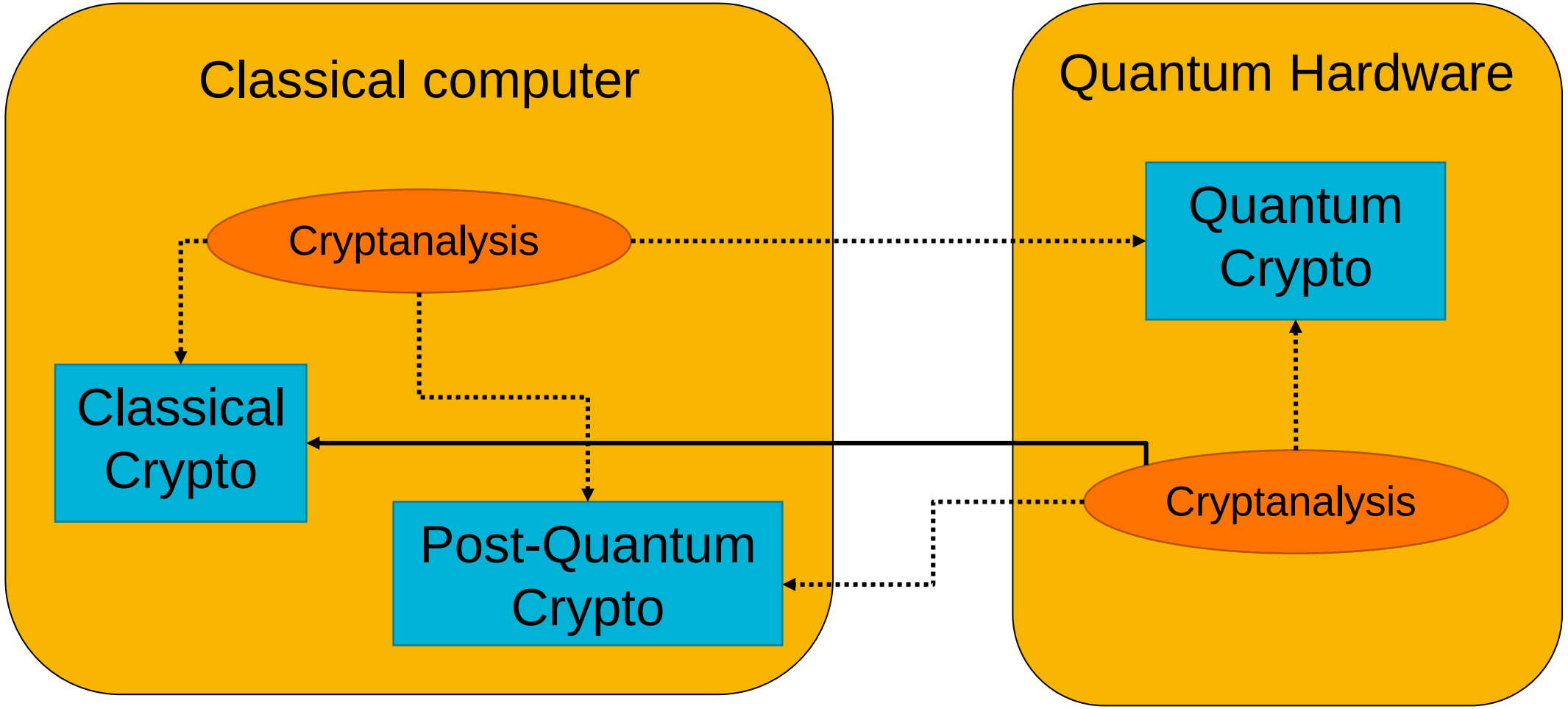
Michele Mosca. Cybersecurity in a Quantum World: Will we be ready? https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

# Post-quantum / quantum-safe cryptography

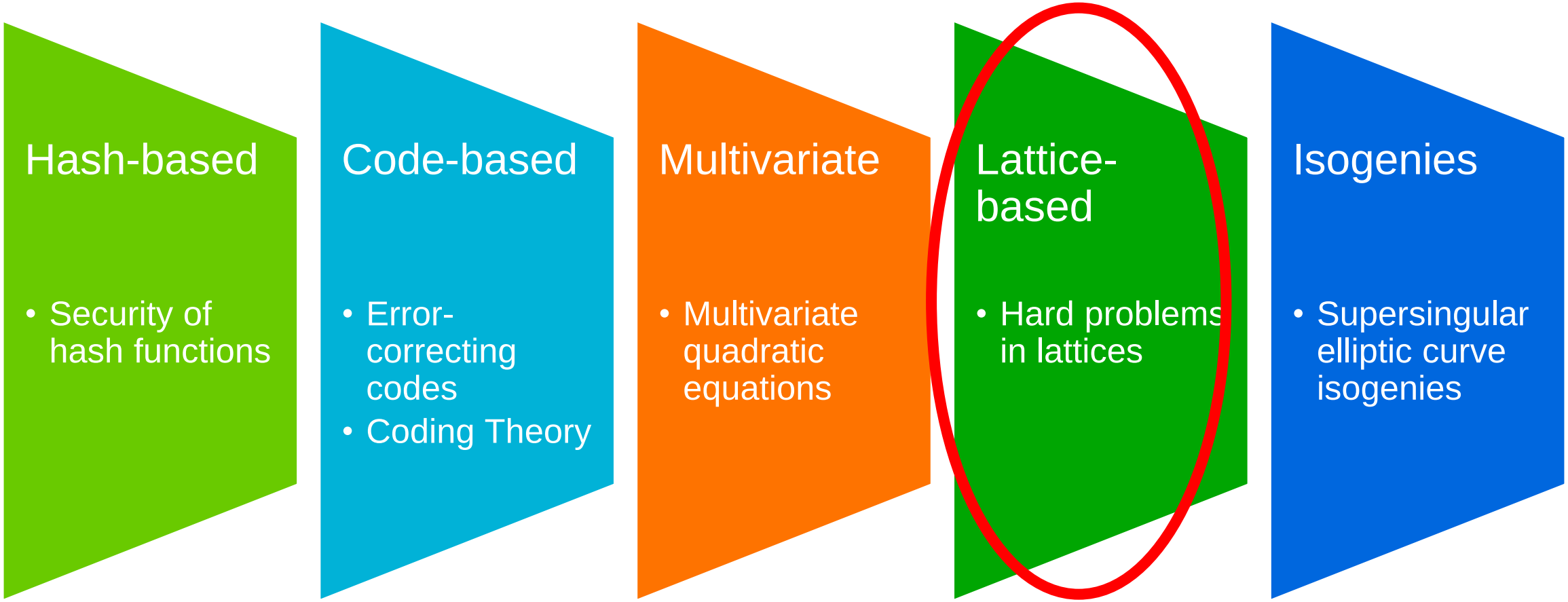
- Post-quantum cryptography emerged ~ 2006
- Academic research have since proposed many schemes designed to withstand a quantum computer
  - No known exponential quantum speedup

- Governments & standardization bodies are active since ~ 2015

# Post-quantum versus quantum crypto

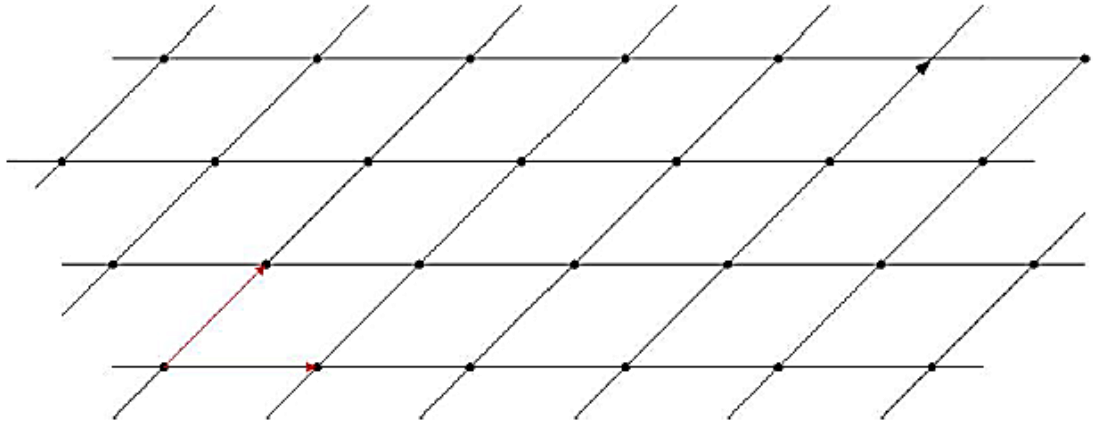


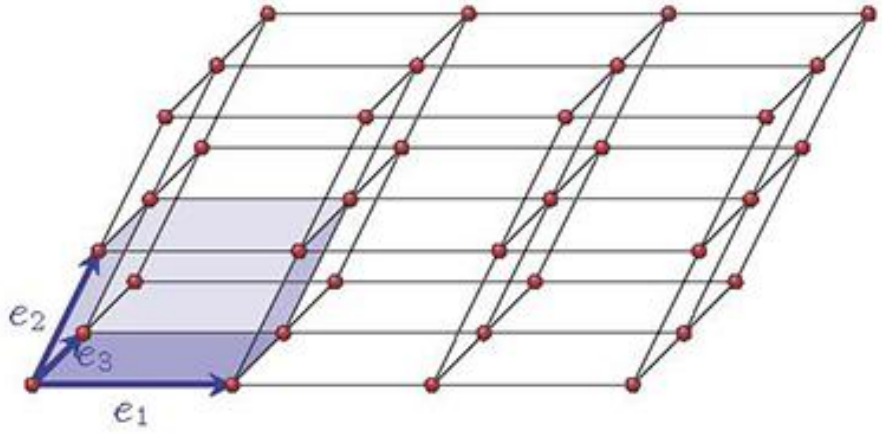
# Post-quantum / quantum-safe cryptography



# Lattice-based crypto

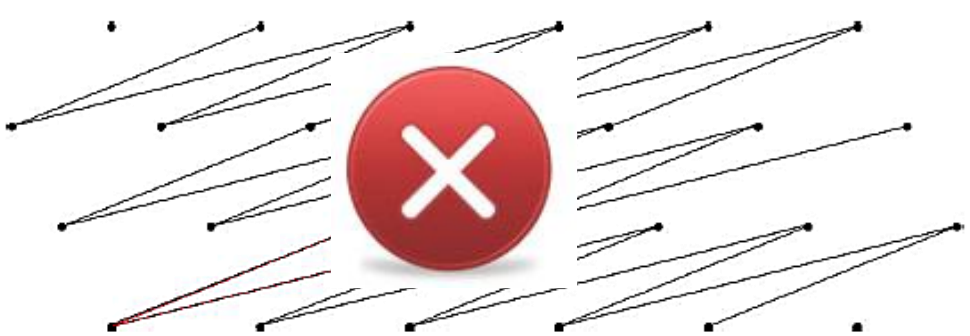
- Integer multiples of independent (basis) objects





# Lattice-based crypto

- Mathematicians have their own notion of beautiful or „good“ and „bad“



- Public key is a „bad“ basis for the lattice
- Secret key is a „good“ basis for the lattice
- For high dimensions, there is no way to go from a bad to a good one

- Core problems: Shortest Vector Problem, Closest Vector Problem

# Lattice-based crypto

**The Good:**

- Lattice-based systems can be fast and small
- Can achieve reasonable key sizes ~ 1 KB
- Re-use of arithmetic co-pros used for RSA/ECC

**The Bad:**

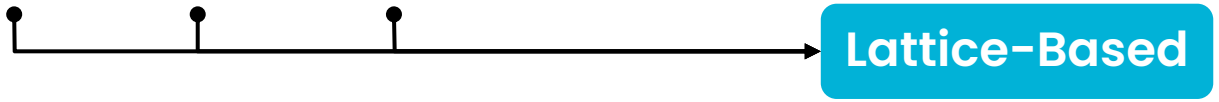
- Relatively new (~ 10 to 20 years), is security well enough understood?
- Secure implementations?
  - Side-channel attacks

**The summary:**

- Lattice algorithms Kyber, Dilithium are standardized
- Already being deployed
- Hardware is available

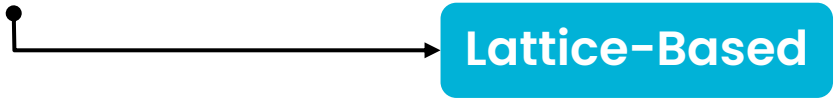
# NIST, BSI & Standardization

- 2016 Call for proposals for PQC by NIST
  - 69 submissions
  - 2022: First four winners: Kyber, Dilithium, Falcon, Sphincs+




- Standards published in 2024
- Currently plan to deprecate RSA by 2030

- BSI currently recommends the use of the NIST algorithms, in addition to:
  - Classic McEliece
  - FrodoKEM



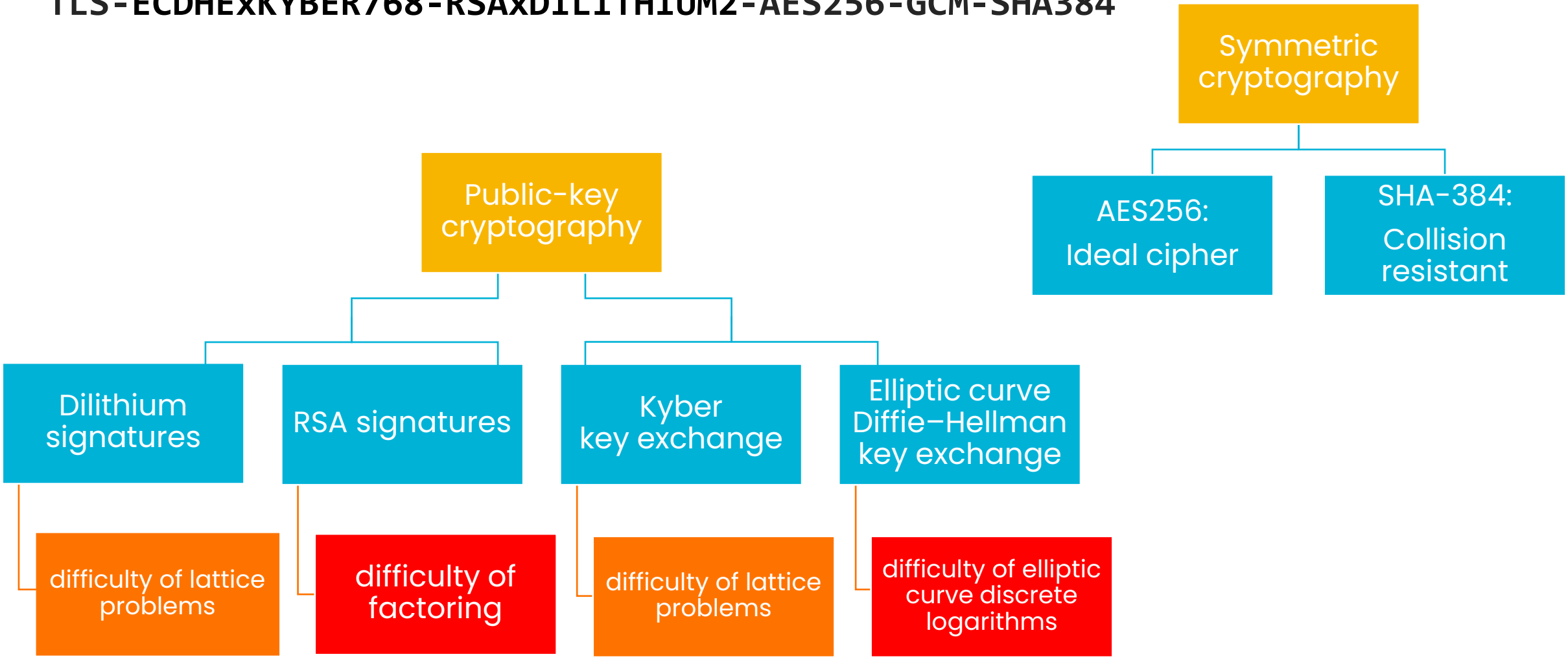
# Hybrid Crypto

- PQC algorithms are relatively new
- Always use in combination with classic crypto
- Guarantees pre-quantum security vs total security break

- Example: Total break of 3rd round algorithm Rainbow and 4th round cipher SIKE
  - Broken on a laptop in a few minutes

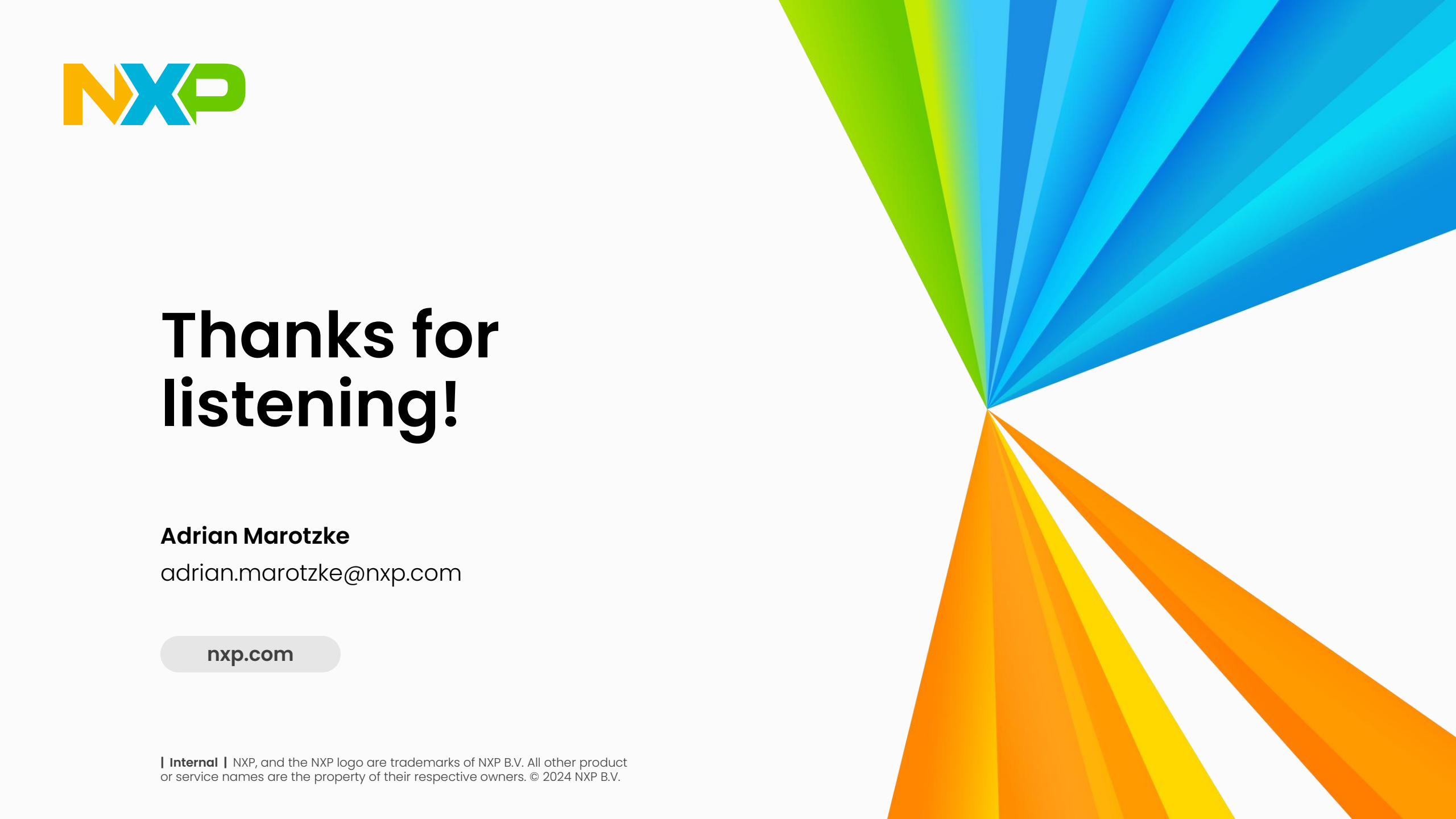
# Future cryptography

## TLS-ECDHExKYBER768-RSAxDILITHIUM2-AES256-GCM-SHA384



# NXP & PQC

- NXP has been (and is) very active in PQC research & standardization
- PQC-cable products with hardware support such as i.MX95, i.MX94 and S32K5
- More info on www.nxp.com/pqc and pqc@nxp.com



# Thanks for listening!

**Adrian Marotzke**
adrian.marotzke@nxp.com

nxp.com

nxp.com