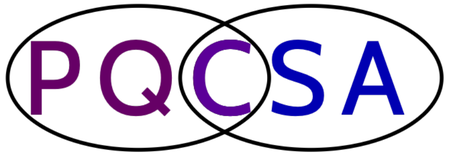
Welcome to

PQCSA Workshop

Privacy in the Post-Quantum Era: Challenges and Migration Strategies

May 19, 2026, Brussels, Belgium



Opening remarks

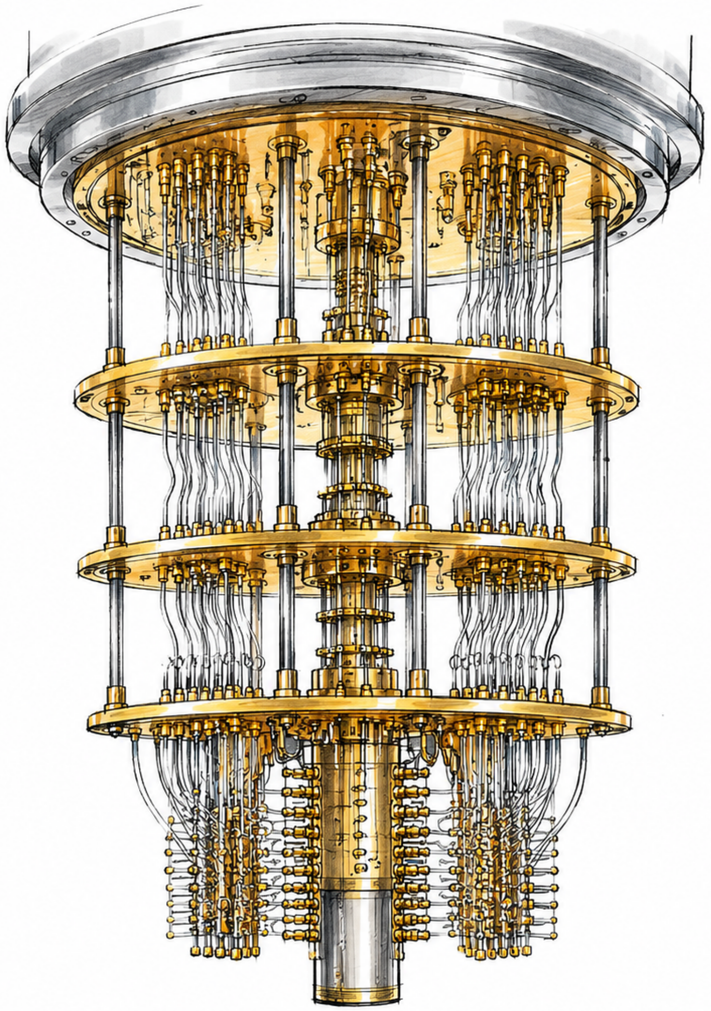
1. Context: quantum threat / post-quantum transition
2. PQCSA project
3. Today’s program

Context

Today’s security of internet, banking, mobile, identity, … relies on public key cryptography: RSA, ECC, Diffie-Helman

A large scale quantum computer would break these cryptosystems

Post-quantum cryptography (PQC) replaces these cryptosystems by quantum-resistant alternatives



Main threats

Encryption

Harvest now, decrypt later

Adversaries collect encrypted traffic today
They wait for a CRQC to decrypt it later

🗓️ Already happening!

⚠️ Long-lived sensitive data at risk:
health records · state secrets
financial data · personal data / PII

Signatures / PKI

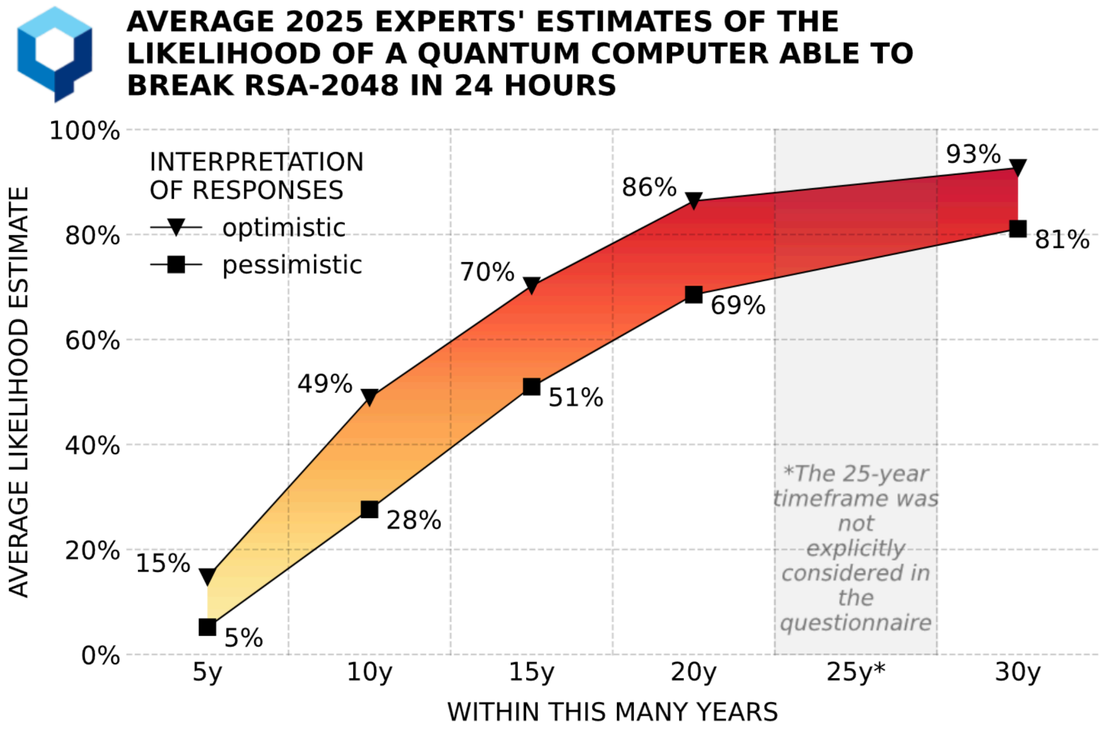
CRQC can forge signatures, impersonate PKI certificates, steal cryptocurrencies, …

🗓️ Future threat

⚠️ But migration takes years:
root CAs · HSMs · firmware
code signing · ID documents

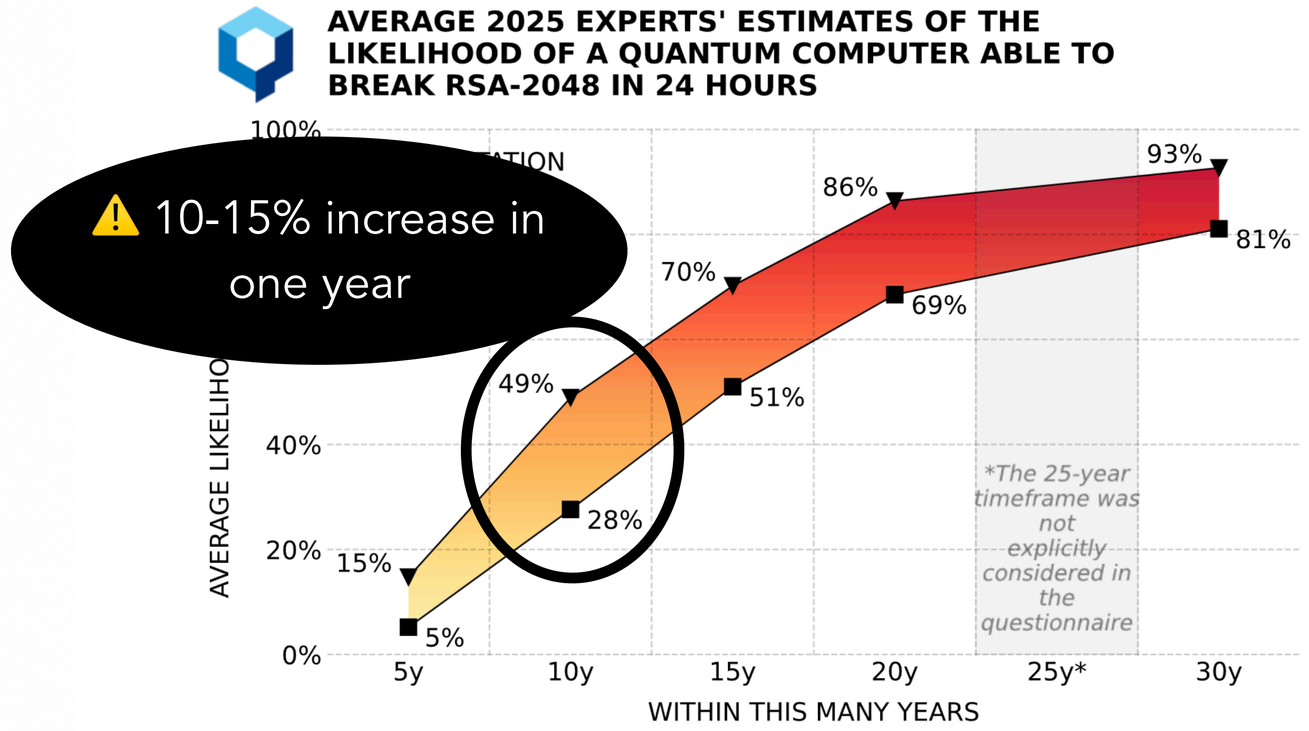
When?

When?



Quantum Threat Timeline Report 2025

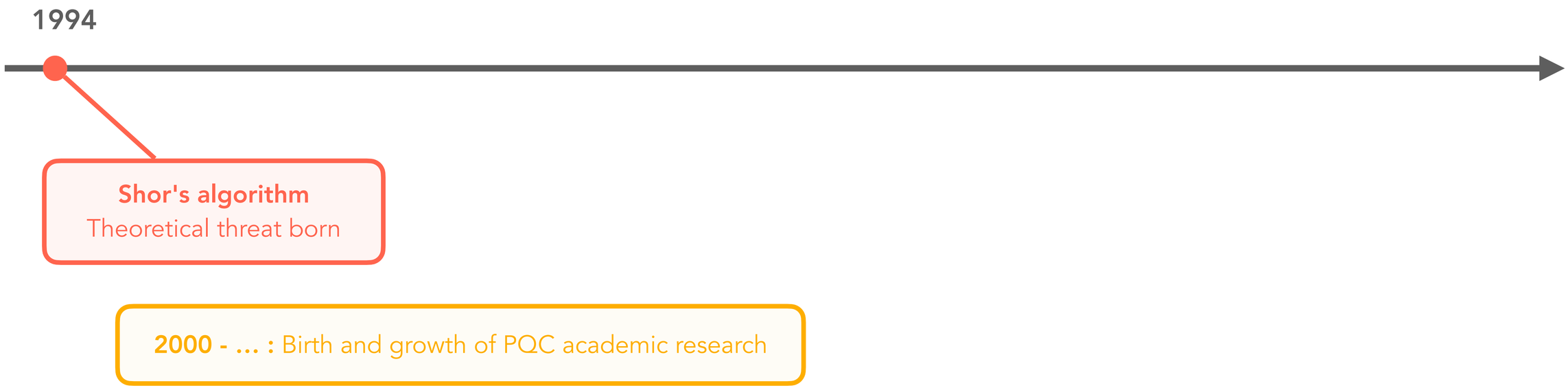
When?



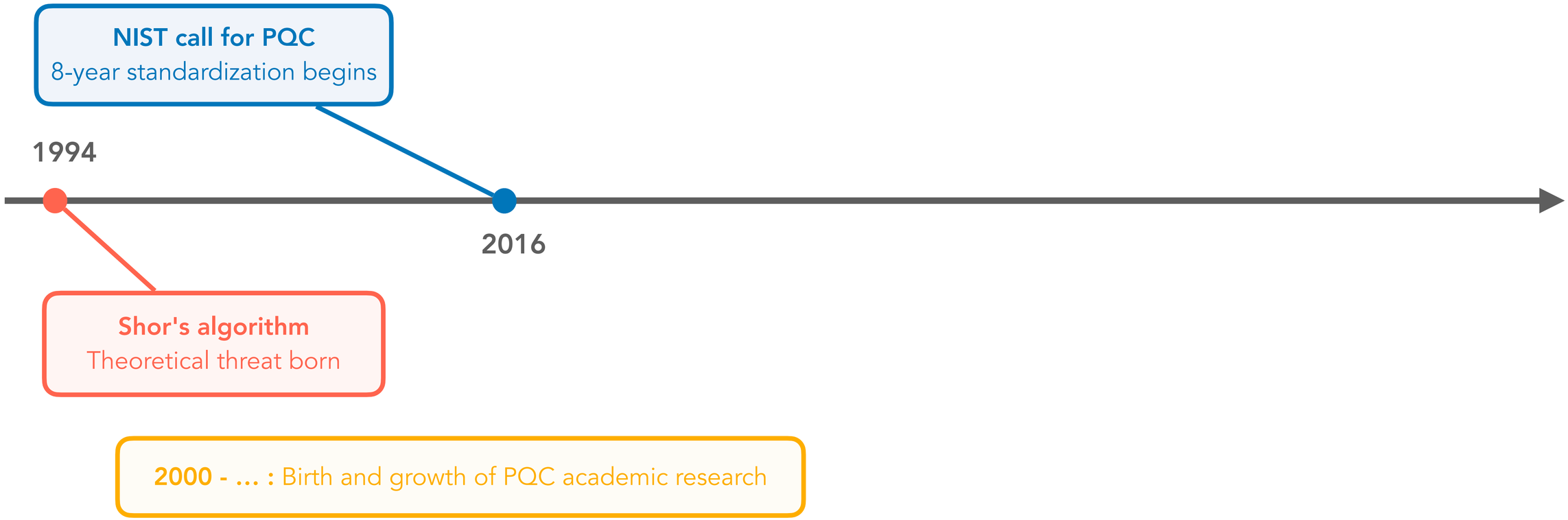
Quantum Threat Timeline Report 2025

A short history

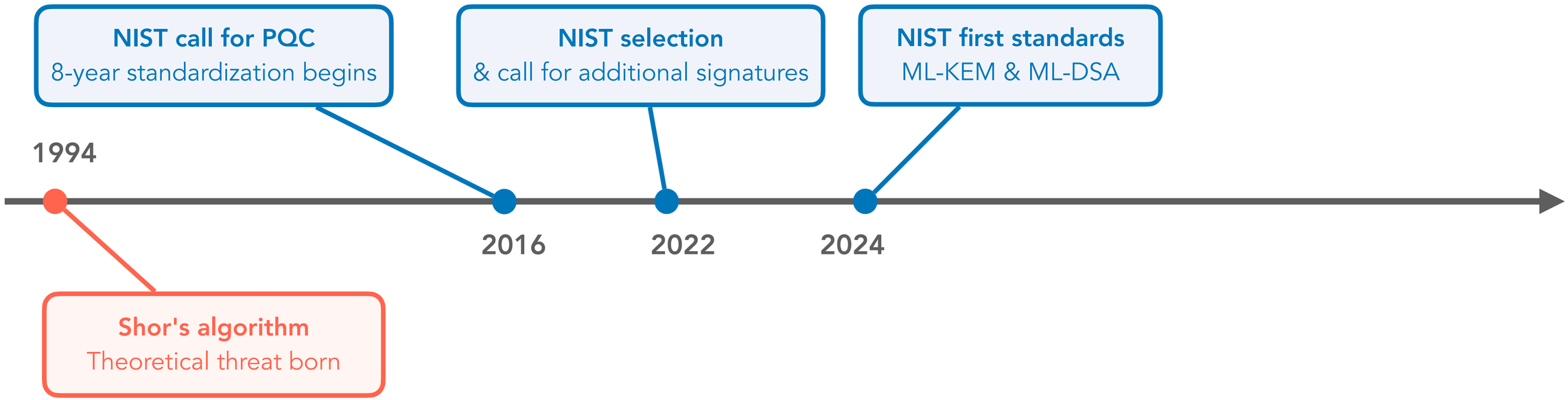
A short history



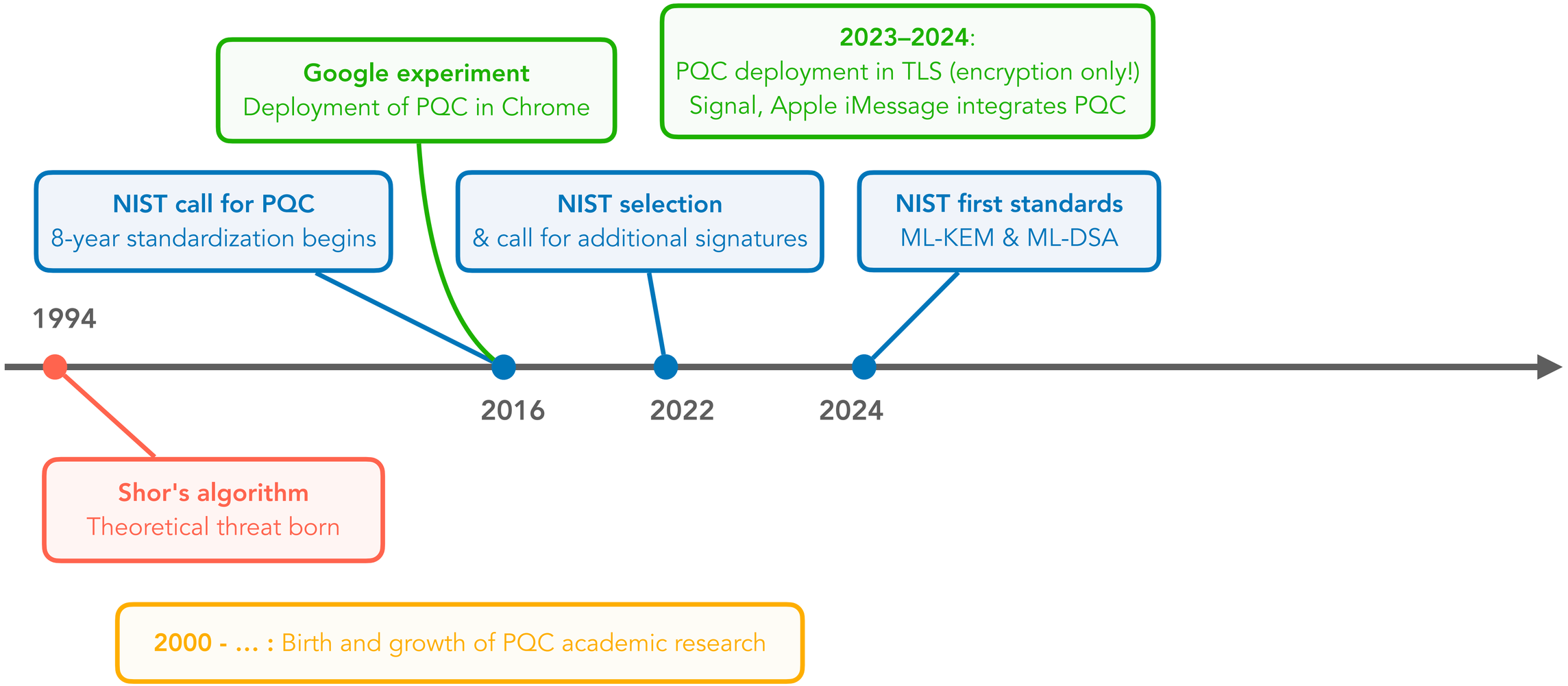
A short history



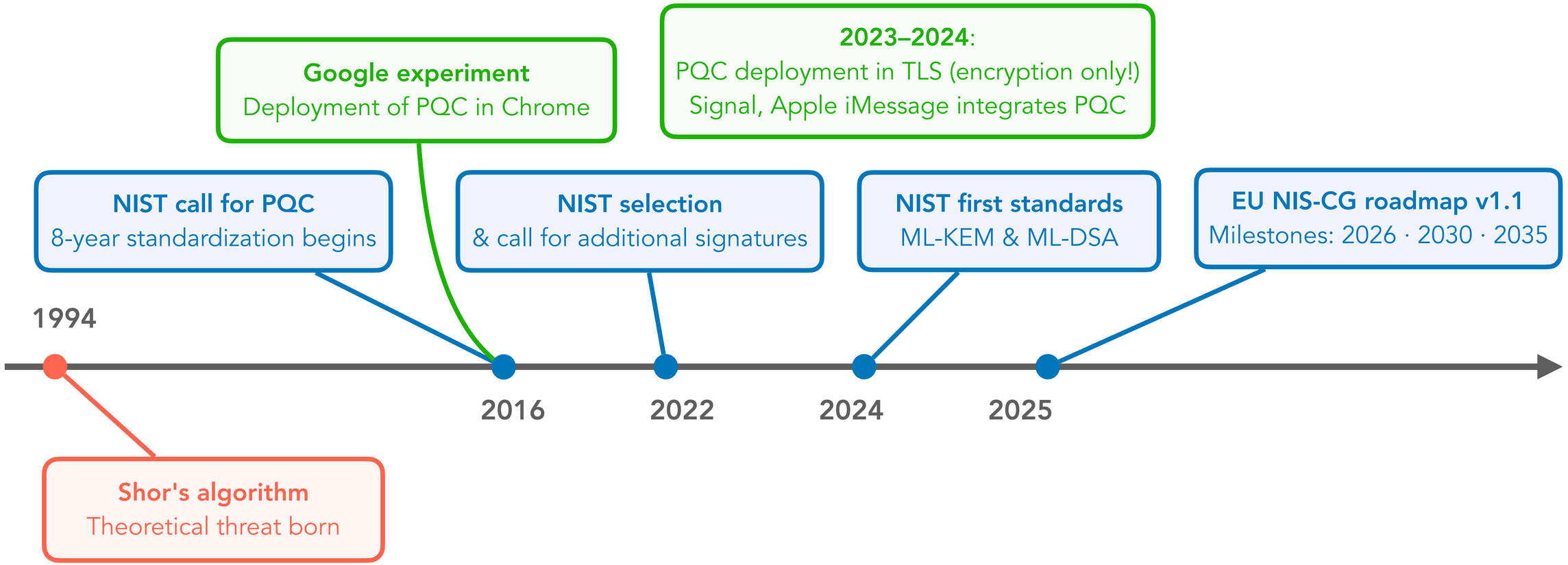
A short history



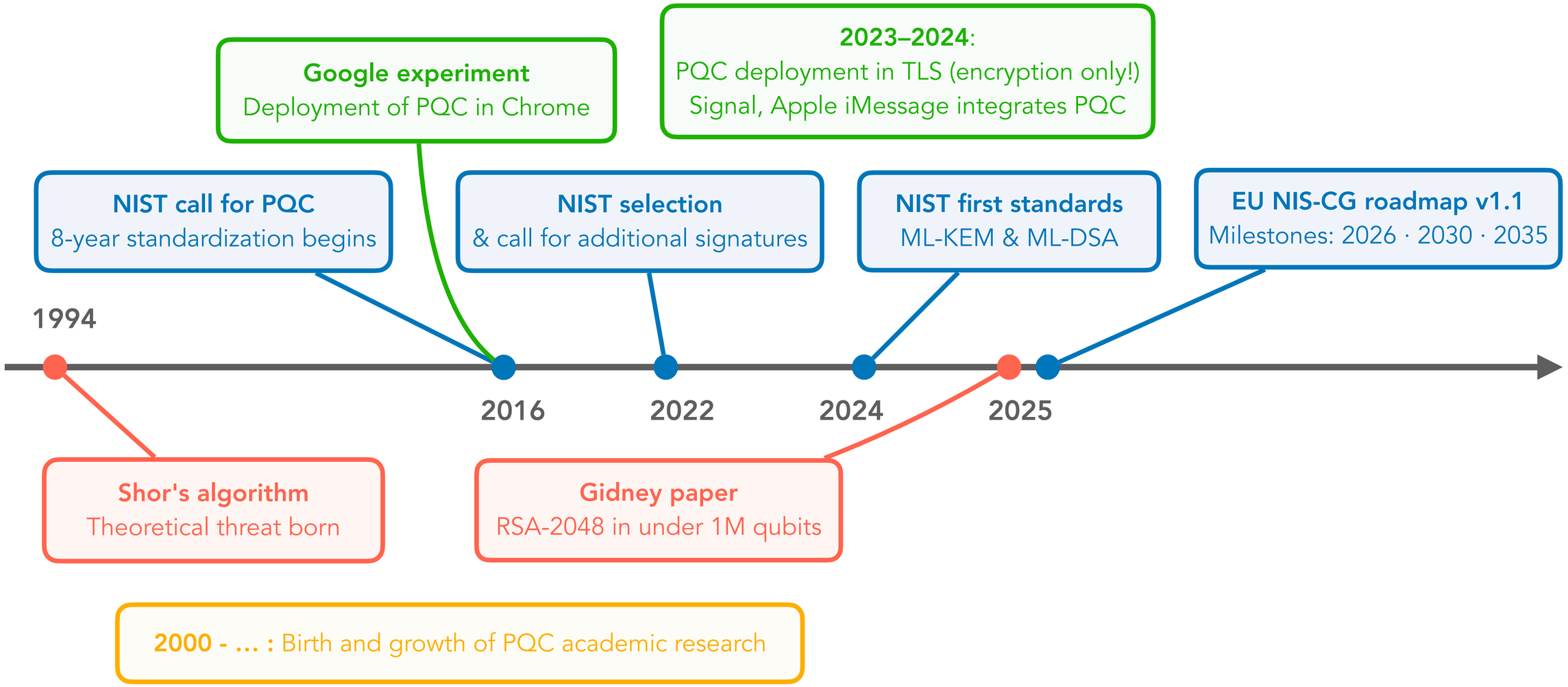
A short history



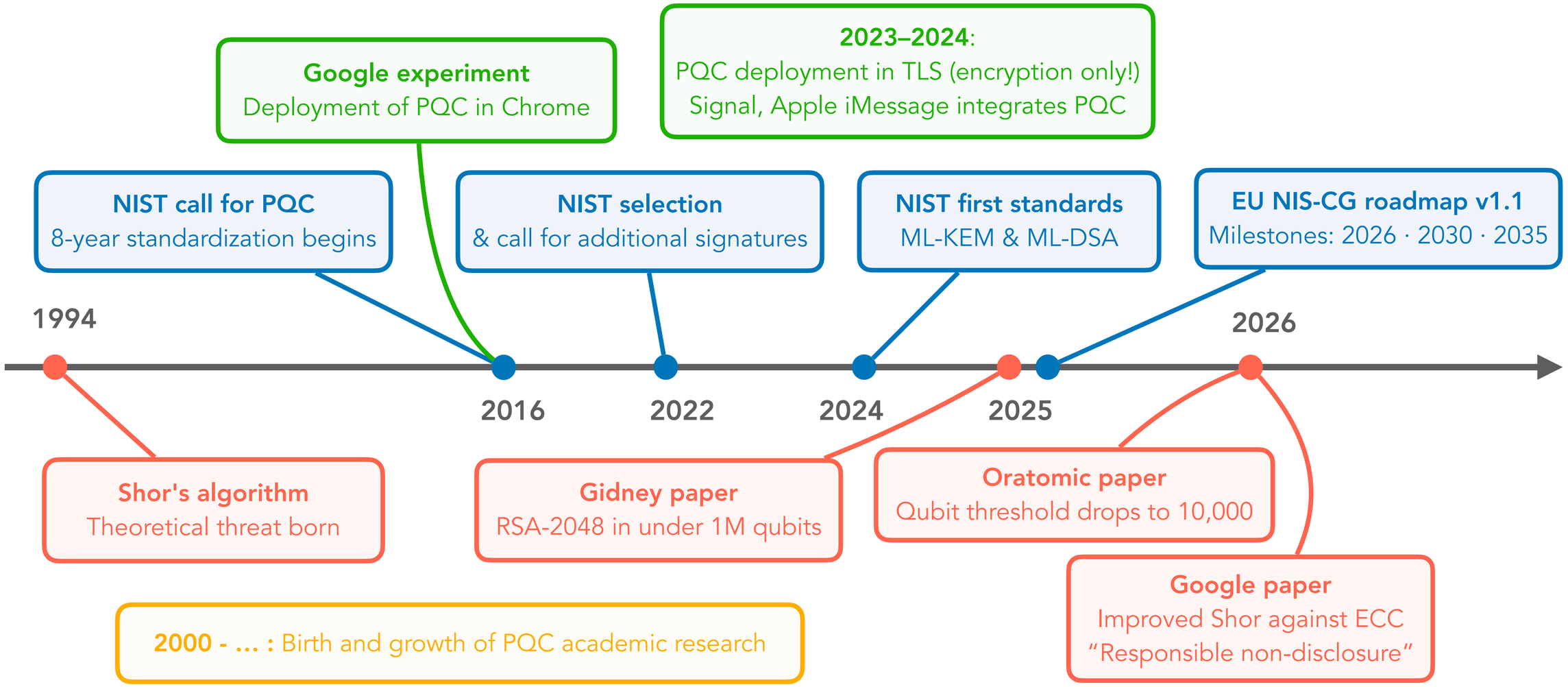
A short history



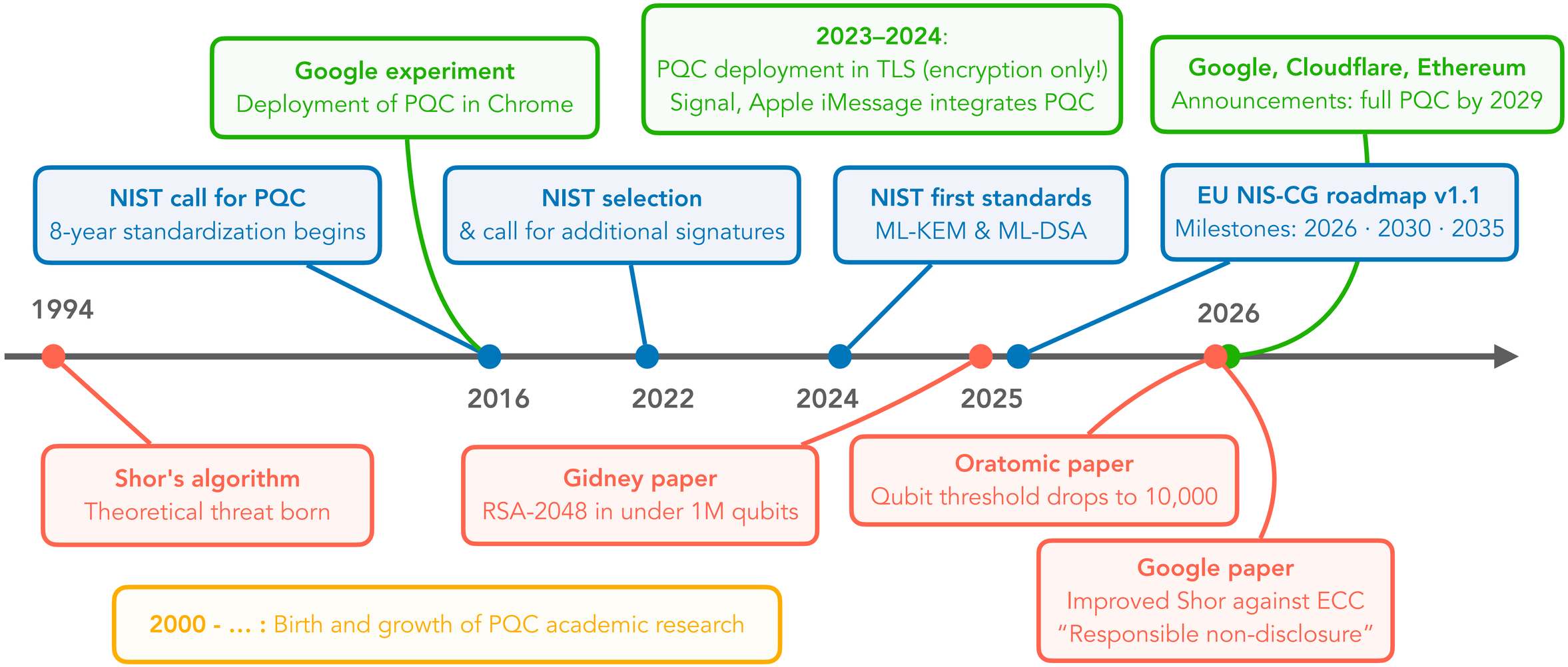
A short history



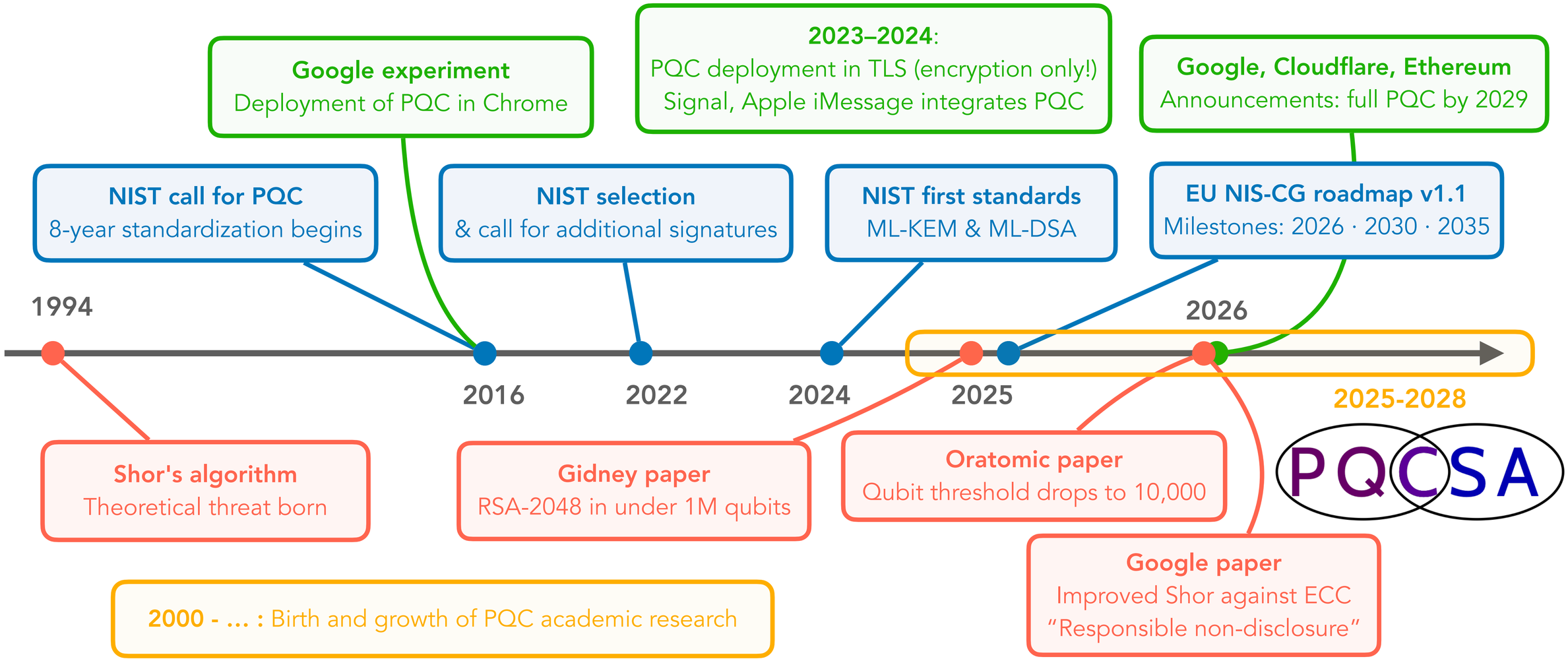
A short history



A short history



A short history



PQCSA

- Coordination and Support Action, funded by the EU, 2025 → 2028
- Goals:
  - Coordinate the EU ecosystem to reach consensus on PQC algorithms, protocols & migration roadmaps
  - Dissemination, training, building awareness on PQC and the need for migration
- Partners: Eindhoven U.T. (coordinator), Bundesdruckerei, CryptoExperts, K.U. Leuven, T.C. Dublin

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

bdr.

Trinity College Dublin
The University of Dublin

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

KU LEUVEN

PQCSA

- Organisation of 23 events over 4 years (this is the 6th)
- Publication of reports, surveys, migration roadmaps, training materials
- So far:
  - *Survey of PQC algorithms*
  - *Survey of PQC protocols*
  - *Report on hot topics and open problems in PQC*
- For further information

https://pqcsa.eu/

Bluesky

LinkedIn

Today’s program

Morning:

- 🎤 **Dahmun Goudarzi** from **Alice et Bob** about

  Advancement in cryptographically relevant quantum computers

- ☕ *Coffee break 10:30 → 11:00*

- 🎤 **Bernardo Lopes Goncalves** and **Fabiana Da Pieve** from **European Commission**
  - *Status of PQC activities at the Commission*
  - *The evolving EU policy digital landscape*

- 🎤 **Laima Jančiūtė** (independent researcher) about

  Governance aspects of the PQC transition

- 🥙 Lunch break 12:30 → 13:30

Today’s program

Afternoon:

- 🎤 **Reyhane Attarian** from **Sopra Steria** about

  Architectural framework for PQC vulnerability management

- 🎤 **Matthieu Lequesne** from **CNIL (French Data Protection Authority)** about

  Migration to quantum-safe cryptography: perspective from CNIL

- ☕ Coffee break 15:00 → 15:30

- 🎤 **Christiane Peters** from **Google** about

  PQC migration at Google

- 🎤 **Bas Westerbaan** from **Cloudflare** about

  The road ahead to a fully post-quantum Internet

- 🎤 **Mélissa Rossi** from **CryptoExperts** about

  Research directions and emerging challenges in PQC

Your friendly hosts

Heloise

Mélissa

Matthieu