The Quantum Threat
to RSA and Elliptic Curve Cryptography

Markku-Juhani O. Saarinen
<markku-juhani.saarinen@tuni.fi>

09 December 2024

Tampereen yliopisto
Tampere University

COMP.SEC.230 – PQC Engineering

“Introduction to Post-Quantum Cryptography (PQC): Modern cryptographic methods designed to resist attacks with quantum computers.”

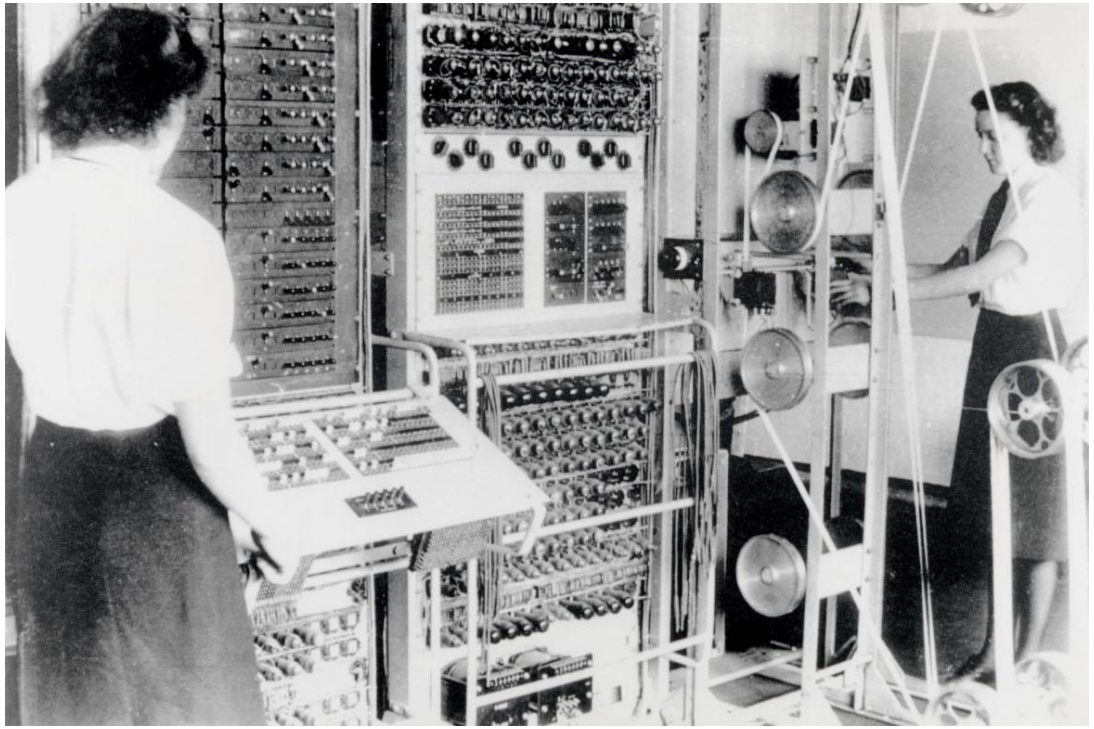
Schedule: 4th teaching period: 03.03.2025 - 25.04.2025 (weeks 10-17).

I’m presenting a part of the first lecture. The desired learning outcomes are:

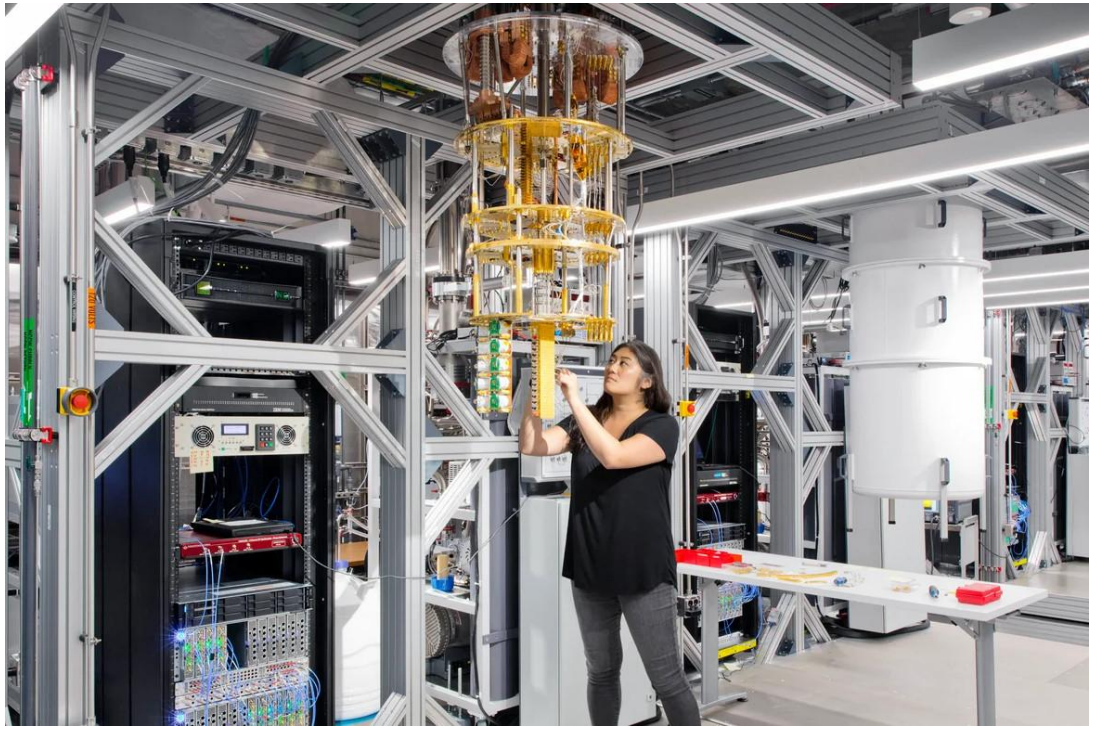
- High-level understanding of what “post-quantum cryptography” is.
- Which older cryptosystems are vulnerable to quantum cryptanalysis?

The rest of the course discusses particular families of PQC algorithms; their cryptanalysis and implementation. This is an advanced-level course for researchers and engineers who want to understand modern cryptography.

Cryptanalysis and Computing



Secret development of the Colossus digital computer during WW2 allowed the British to break the Lorentz cipher and read high-level German army messages.



Sufficiently powerful quantum computers can break RSA and Elliptic Curve cryptography, the foundation of the security of the public Internet and e-commerce.

Quantum Computing & Public Key Cryptography

1970s-: Public key cryptography is invented, allowing private communication in public networks without the need for pre-established secret keys ("shared secrets") between parties.

.. while elsewhere ..

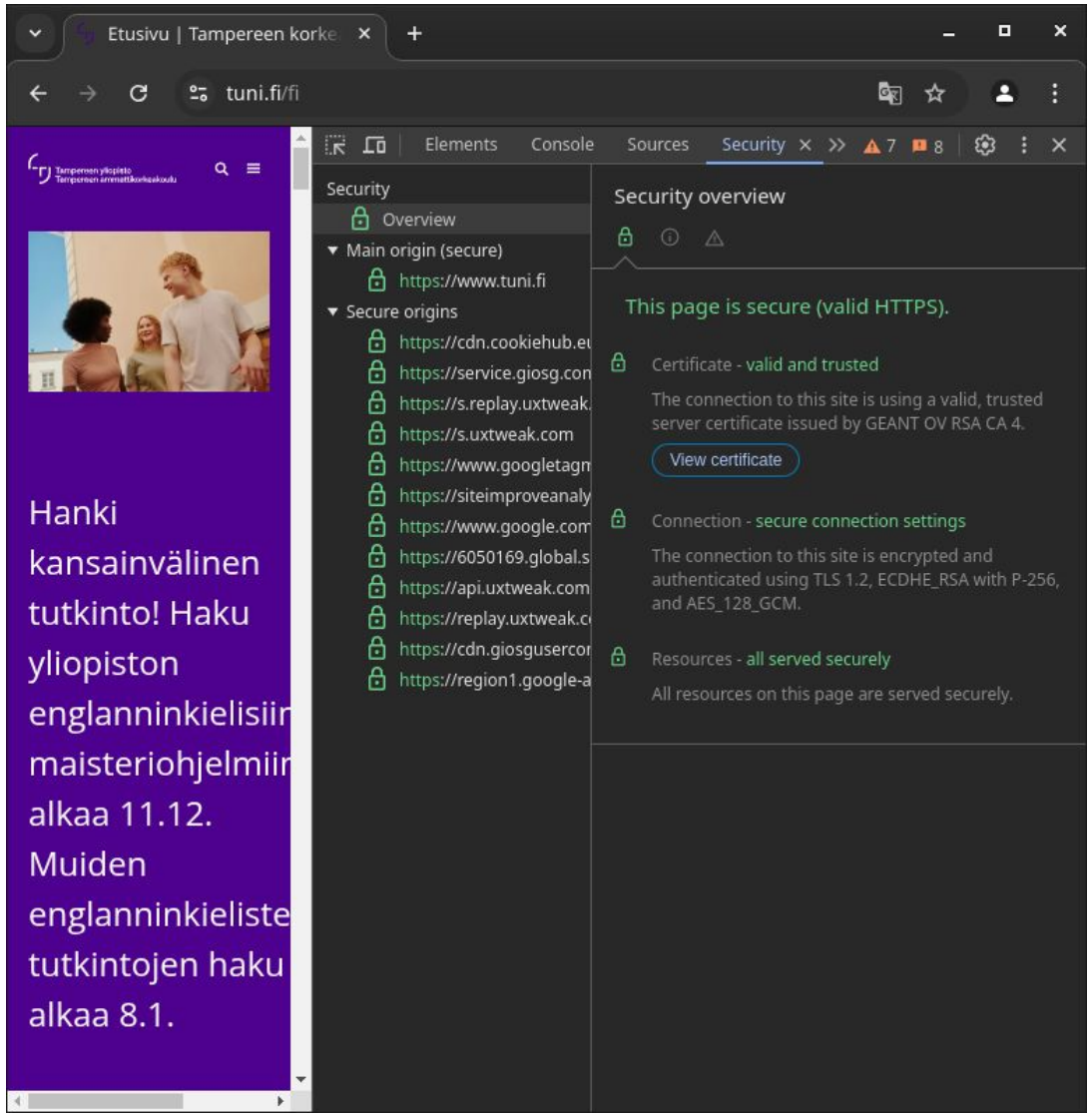
1980s-: First suggestions (Benioff, Feynman) to build "non-digital" quantum computers that use quantum states and other phenomena directly. Initially proposed just for quantum simulation.

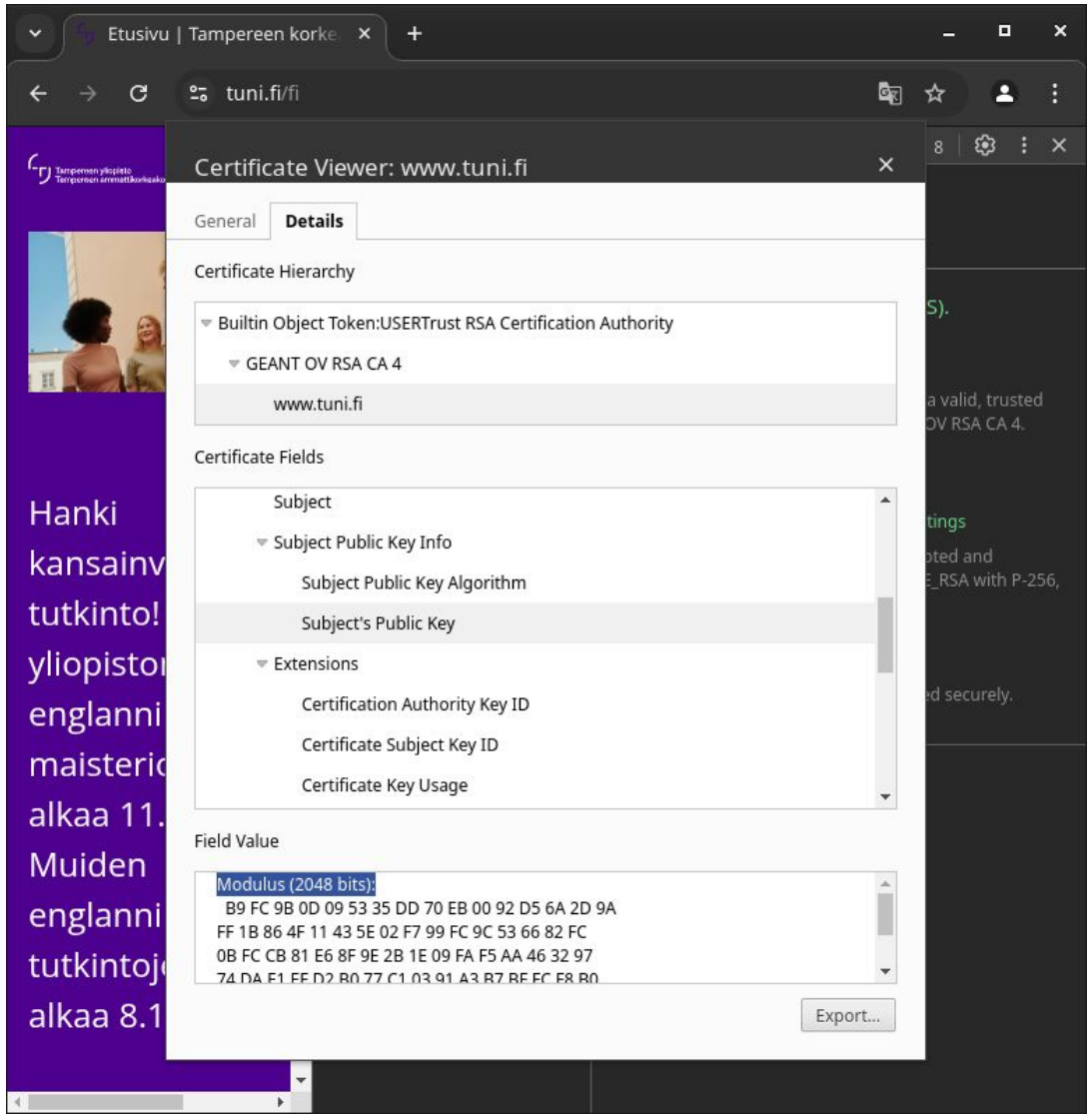
1994: Peter Shor shows that factoring (RSA) and Discrete Logarithm / Elliptic Curve problems can be solved if a large quantum computer is built (in polynomial time - basically regardless of key size.)

.. quantum computing research continues, while at the same time ..

1990s-2000s: Public internet and mobile communication revolution; digital technologies become embedded in society, commerce, government. Digital identity (e.g., web site certificates) and online privacy / confidentiality (e.g., TLS) are entirely dependent on the security of public key cryptography.

Typical in 2024: P-256 ECDH, RSA-2024





Traditional vs. Quantum Circuit Models

TRADITIONAL COMPUTER

Binary bit has state 0 or 1.

Digital gates: Operations on bits.
"Size": Hard-wired as a physical circuit.

Gates are active simultaneously.
Each cycle maps a computer state (registers, flip flops) to a new one.

Complexity: Steps, or cycles * gates.

QUANTUM COMPUTER

Qubit: $\alpha|0\rangle+\beta|1\rangle$ Superposition.
"Size": A hardware component.

Quantum gates: Individual operation steps on qubits. Must be reversible.

Measurement: Irreversible operation resulting in a classical bit at the end.

Complexity: Gates / "circuit depth."

Traditional Complexity Estimates

ECDH P-256 and **X25519:** Breaking an n-bit **Elliptic Curve Diffie-Hellman** key exchange requires solving the Elliptic Curve Discrete Logarithm (ECDL) problem. Classical ECDL: Exponential $\mathbf{O(2^{n/2})}$ computational steps, i.e. $\mathbf{\sim 2^{128}}$ in this case.

RSA-2048: Factoring a 2048-bit modulus allows one to forge RSA authentication signatures and certificates (malicious updates, man-in-the-middle attack, etc.)

The best known classical algorithms were *subexponential* but *superpolynomial*. General Number Field Sieve (GNFS): $\mathbf{\sim 2^{112}}$ for RSA-2048, $\mathbf{\sim 2^{128}}$ for RSA-3072.

"Moore's Law" – doubling of transistor density every ~2 years (since 1965.)

Some QC numbers – Steady progress suffices

[Gidney & Ekerå 2019] design for Shor's on **RSA-n** with superconducting QC:

n (3 + 0.002 lg n)	*Logical / abstract qubits (**2n** is also possible)*
logical qubits × $2(d + 1)^2$	*Physical qubits; d = code dist. = 27 for n=2048*
$\mathbf{n^2}$ (500 + lg n)	*Toffoli gates ("arithmetic ops")*
$\mathbf{n^3}$ (0.3 + 0.0005 lg n)	*Measurement depth ("time")*

[Häner et al., 2020] estimate **8n** + 10.2 lg n logical qubits for an n-bit elliptic curve. Breaking Elliptic Curves appears easier at similar classical security level.

For quantum threat to materialize, exponential improvement **is not required**.

[Gidney, Ekerå, 2019] https://arxiv.org/abs/1905.09749 [Häner et al., 2020] https://arxiv.org/abs/2001.09580

Limitations of Quantum Computing

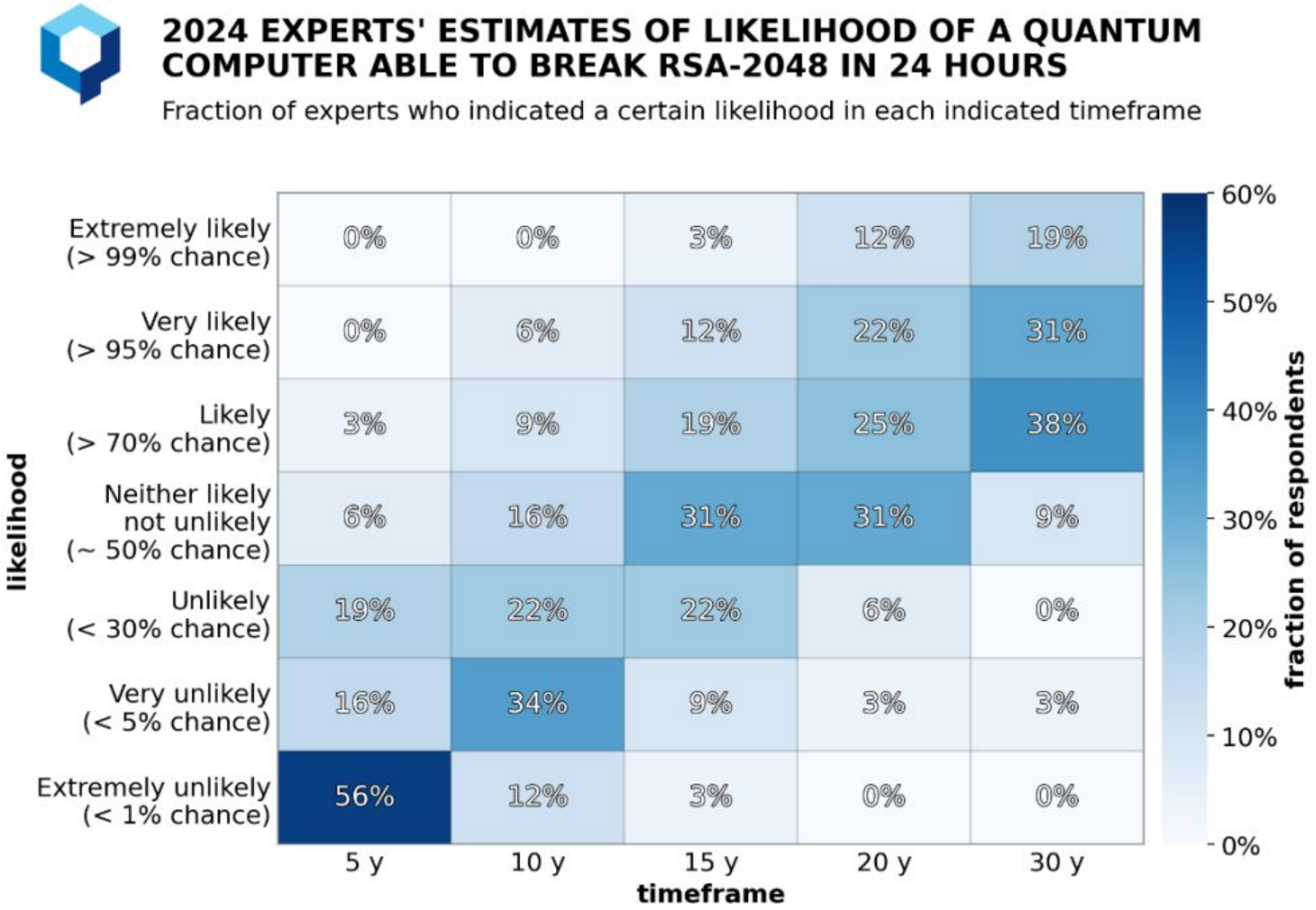
- Shor's 1994 (factoring and discrete logarithm) algorithm was one of the earliest found – but still one of only a handful of truly effective quantum algorithms.

- Simpler annealing-based or "variational" quantum computers (e.g., d-Wave) cannot be used to implement Shor's algorithm – no real threat to cryptography.

- General (secret key) search can be sped up using **Grover's algorithm**, but it has **$O(2^{n/2})$** exponential complexity and very large overheads.

- Attacks on AES-128 or SHA-256 do not seem presently feasible with quantum computers; current standard symmetric cryptography is considered safe.

GCHQ's 2024 estimates: https://csrc.nist.gov/Presentations/2024/practical-cost-of-grover-for-aes-key-recovery



https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

PQC Development Timeline

Late 2000s: ``Post-Quantum Cryptograpy'' is born: hash-based, code-based, lattice-based, and multivariate families had been identified as potential replacements to RSA and ECC by 2009.

2015: U.S. National Security Agency (NSA) CNSS Advisory Memorandum 02-15. Indicates a long-term requirement for quantum-resistant cryptography standards. Standardization is initiated.

2016: National Institute for Standards and Technology (NIST) starts an open, international standardization and evaluation process for PQC algorithms (digital signature and key establishment.)

82 submissions by 30 Nov 2017 deadline. First selections after three evaluation rounds in July 2022.

2024: Ratified specs (FIPS 203, FIPS 204, FIPS 205) in August 2024. Standards immediately in effect.

https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

Main Replacements: NIST PQC Standards

KEY ESTABLISHMENT

DIGITAL SIGNATURES

Kyber: FIPS 203 ML-KEM (2024)

Primary PQC **key establishment** algorithm to replace Diffie-Hellman (ECDH) key exchange and RSA public-key encryption. Lattice-based.

Some of **{ HQC, BIKE**, **Classic McEliece }** (2025?)

Being evaluated in "Round 4." Code-based key establishment algorithms. Longer public keys.

Hybrid schemes: One still needs to support traditional Elliptic Curve and RSA methods.

Dilithium: FIPS 204 ML-DSA (2024)

Primary "general-purpose" PQC **signature algorithm** to replace ECDSA, RSA signatures. Lattice-based.

XMSS and **LMS**: NIST SP 800-208 (2020)

SPHINCS+: FIPS 205 SLH-DSA (2024)

Hash-based signatures; Firmware signing.

Falcon: FIPS 206 FN-DSA (2025). Lattice-based.

Signature "On-Ramp" Algorithms (2026?)

“It’s the law” (well, in United States it is)

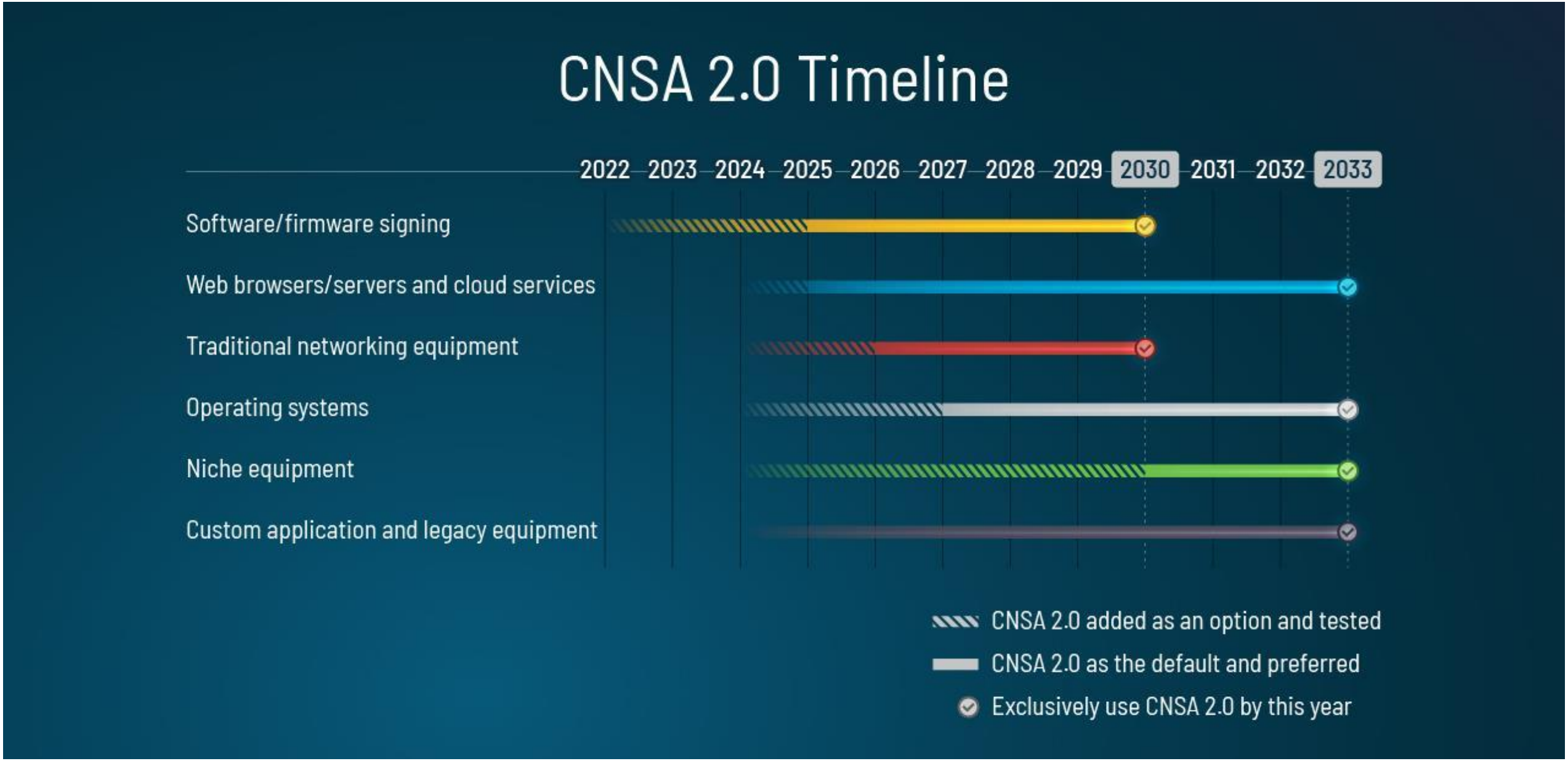
NSM-8 (Jan 2022): *“On Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems”*

NSM-10 (May 2022): *“On Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”*

HR 7535 (Dec 2022): *“Quantum Computing Cybersecurity Preparedness Act”*

<u>These PQC-related National Security Memorandums and the Public Law:</u>

- Mandates transition to Post-Quantum Cryptography in government IT.
- Assigns inventory, reporting responsibilities, sets timelines, etc.
- Outside Government’s own IT systems and some critical sectors, the use post-quantum cryptography (like most information security) is of course not enforced, apart from self-regulation and “business best practices” in many industries.



https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

NIST IR 8547 (Draft, November 2024)

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

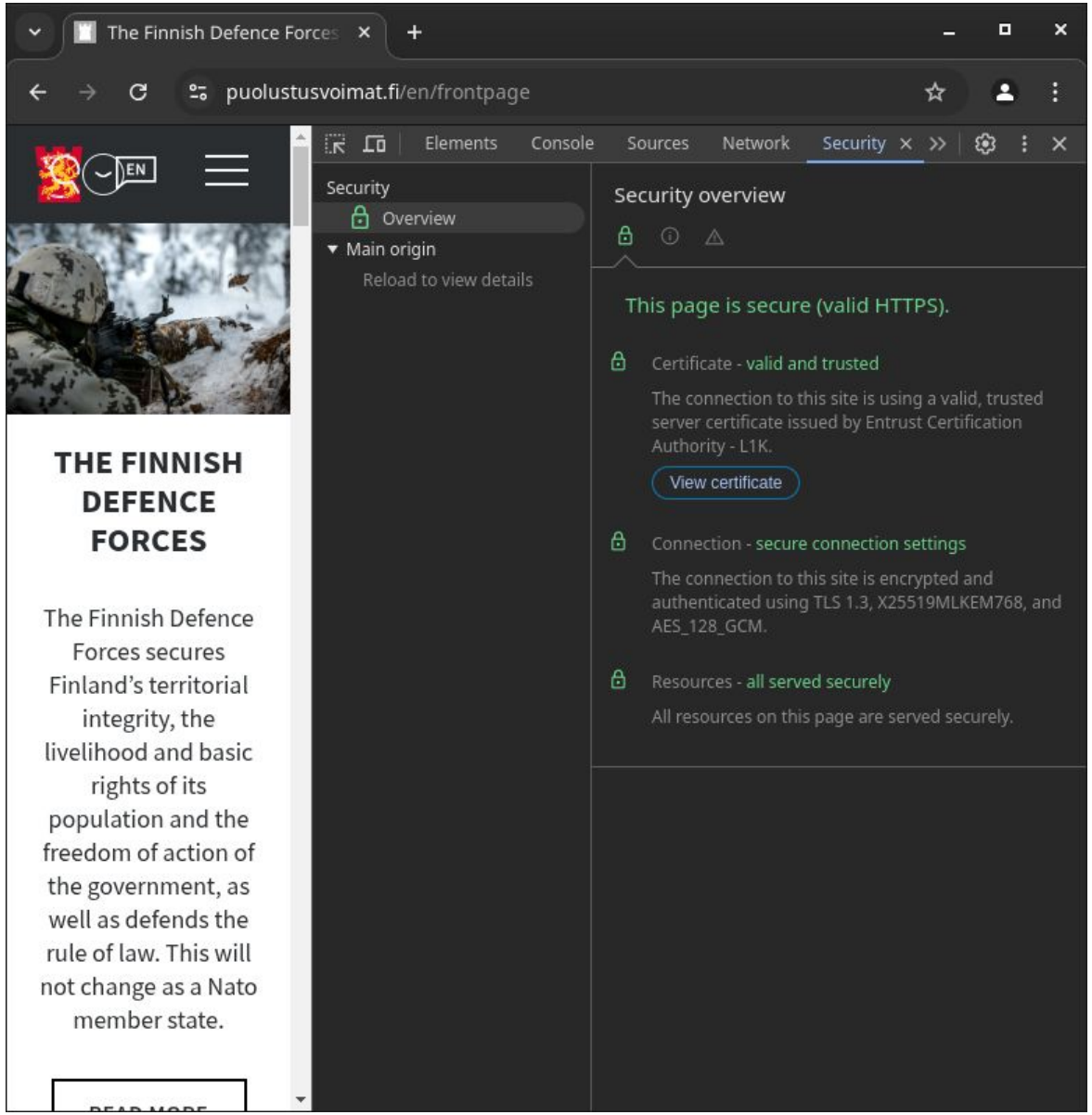
https://doi.org/10.6028/NIST.IR.8547.ipd

Transition is Ongoing

Some prominent service providers such as **google** and **cloudflare** already support the X25519 + MLKEM768 *hybrid key establishment* in TLS 1.3.

In a hybrid scheme the adversary has to break both the traditional and post-quantum scheme to succeed.

Signatures can also be hybridized.



PQC: Recap of the Basics

- **RSA** and **Elliptic Curve** - based cryptosystems **are vulnerable** to an attack with **Quantum Shor's** algorithm, which is very effective (runs in polynomial time.)

- **Post-Quantum Cryptography** (PQC) a.k.a. Quantum-Resistant Cryptography considers cryptographic algorithms that are *secure against attacks with Quantum Computers*.

- **PQC Algorithms** run in traditional computers. They can be used to replace vulnerable cryptography in existing applications. They are based on newer mathematical designs.

- Due to perceived long-term risks, PQC is now required and modernization is ongoing.