Norwegian University of Science and Technology

Quantum Computers and Digital Security

Tjerand Silde - NTNU

Introduction

Associate Professor in Cryptology

Department of Information Security and Communication Technology at NTNU

Leading the NTNU Applied Crypto Lab

Quantum safe cryptography and privacy

Part-time position in PONE Biometrics

NTNU Applied Cryptology Lab

Cryptography Courses at NTNU

- TTM4135 Applied Cryptography and Network Security

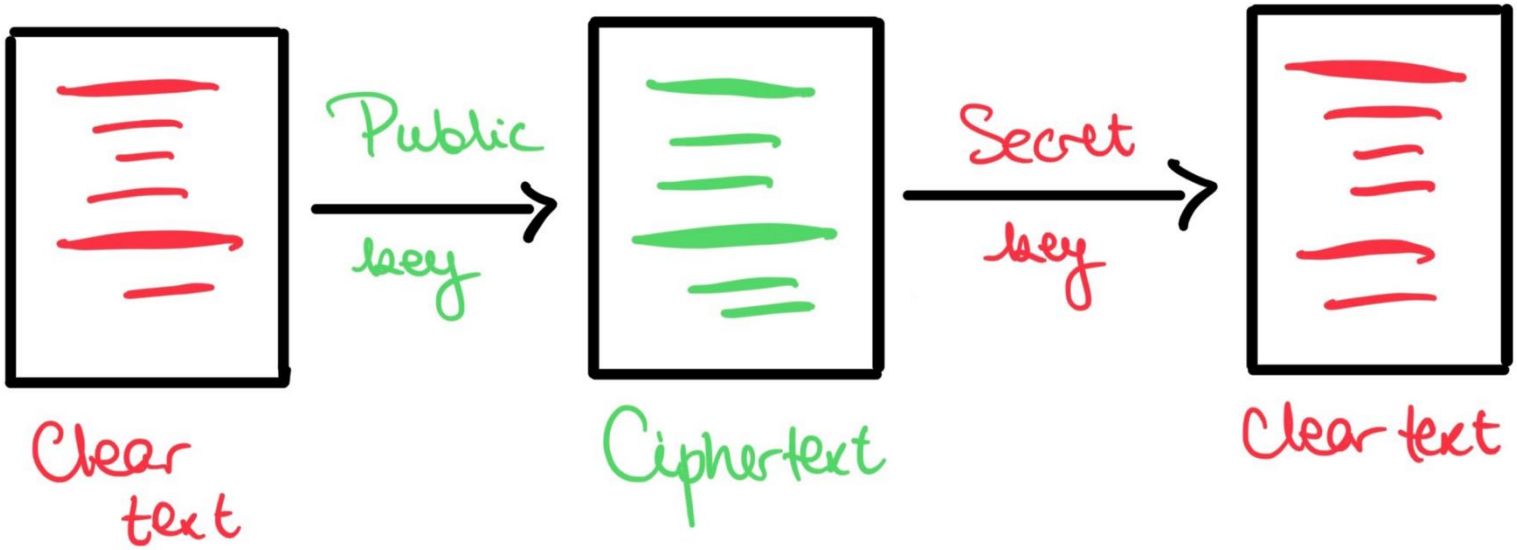
- TTM4138 Wireless Network Security
- TTM4195 Blockchain Technologies and Cryptocurrencies
- TTM4205 Secure Cryptographic Implementations
- IMT4217 Introduction to Data Privacy
- TMA4160 Cryptography
- TMA4162 Computational Algebra

Cryptography Today

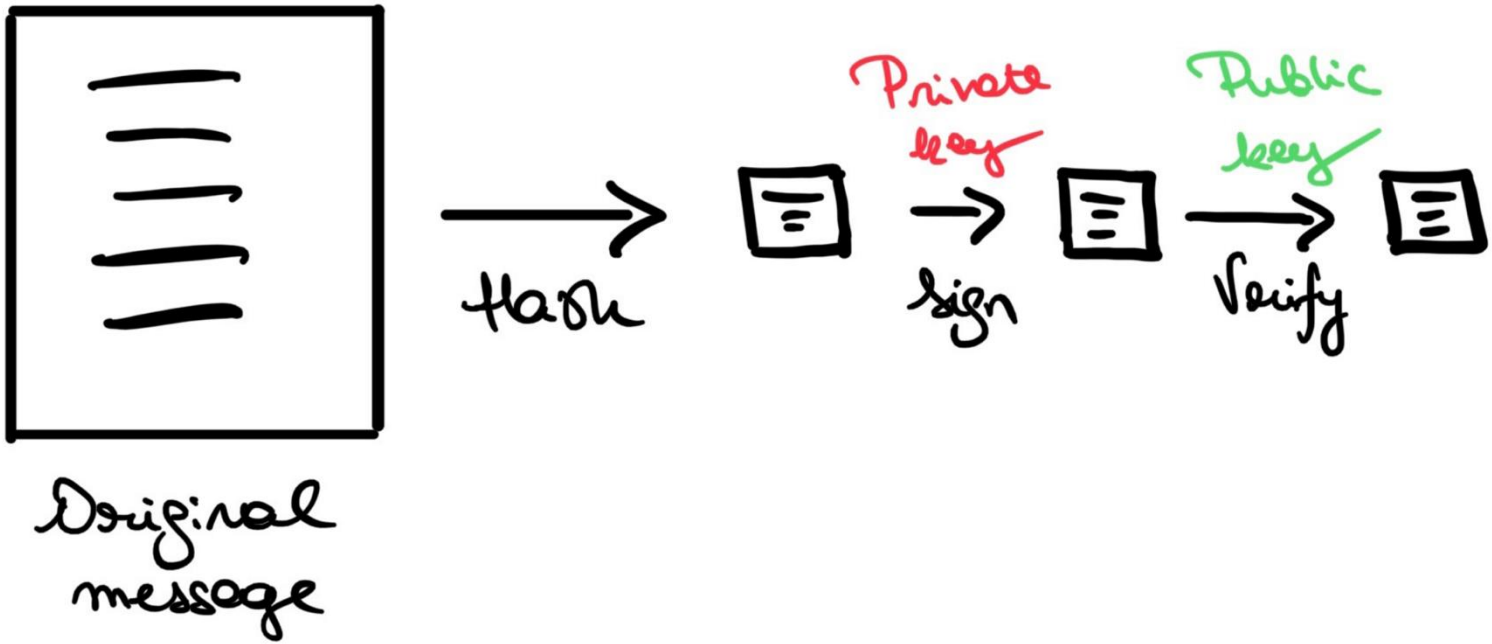
Secure messaging:	Signal, WhatsApp, iMessage
Secure connections:	TLS, SSH, IPsec
Digital authentication:	FIDO, Bank ID, Buypass ID
Payments:	PayPal, VISA / Mastercard, Apple / Google Pay, Vipps

Will these protocols be secure in the future?

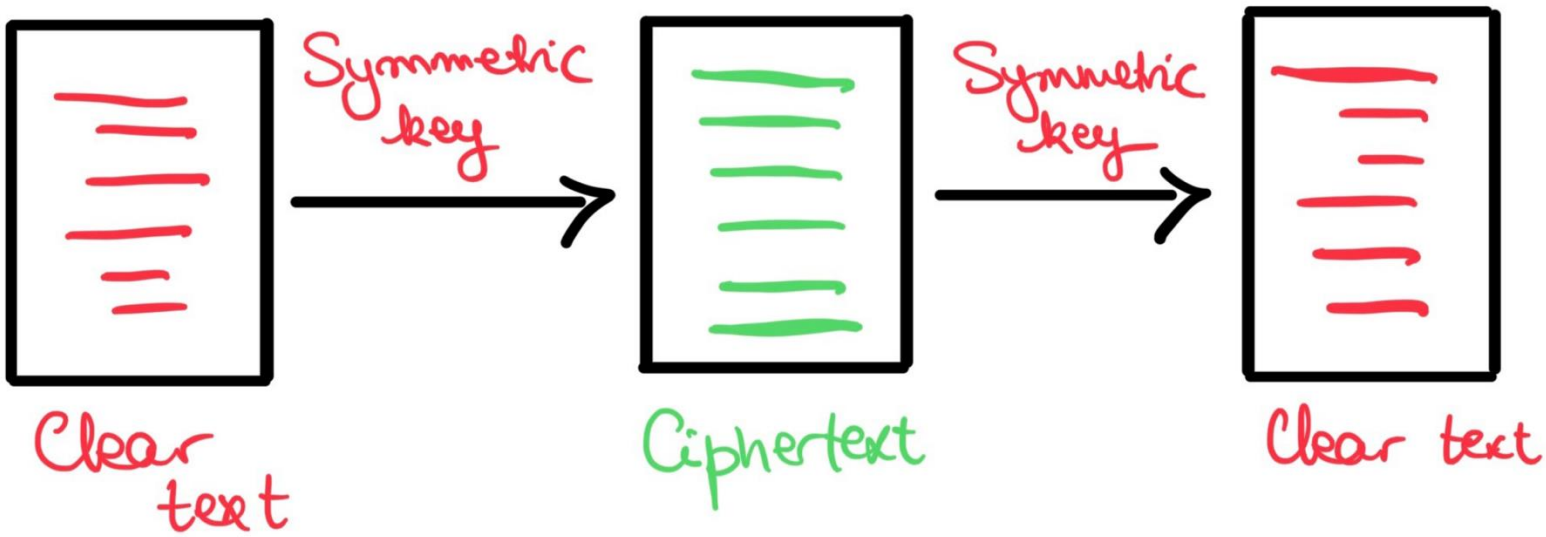
Public Key Encryption



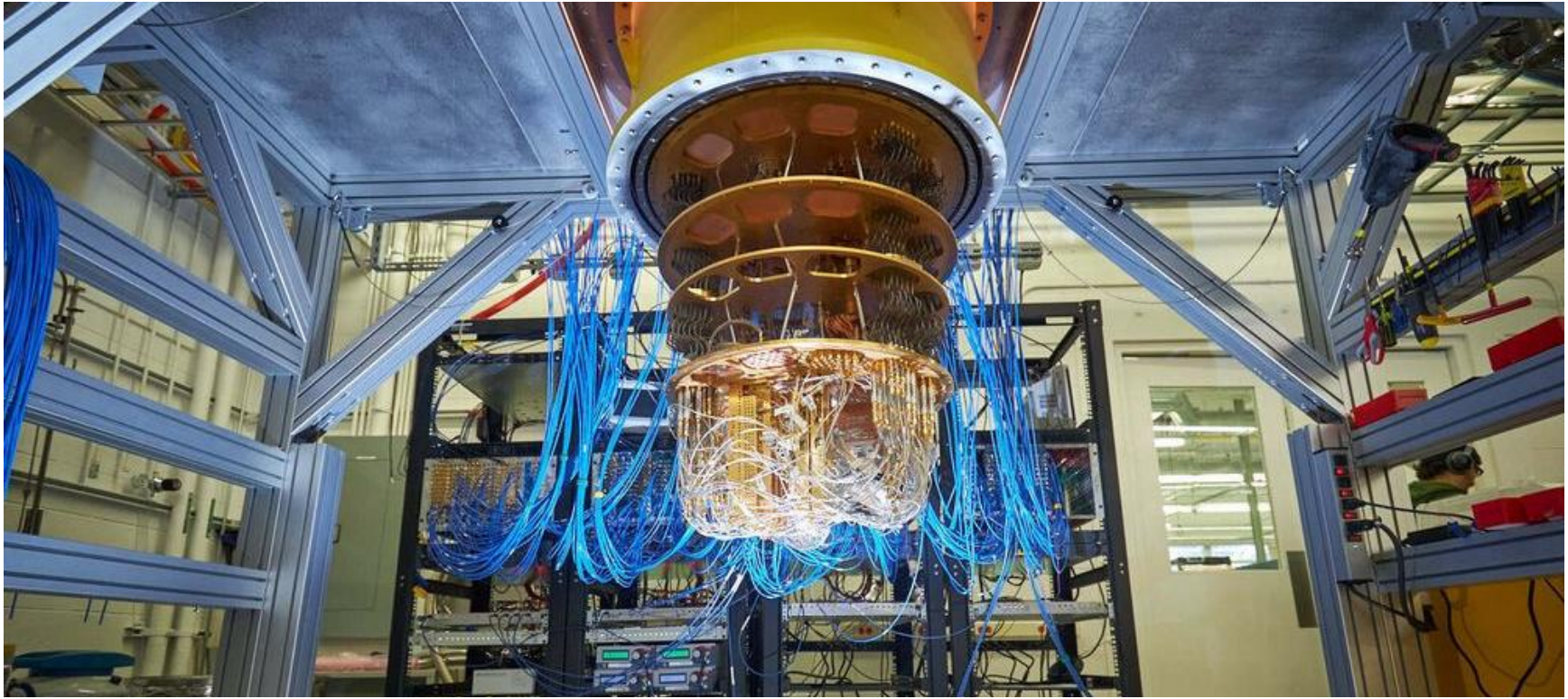
Digital Signatures



Symmetric Key Encryption



Quantum Computers



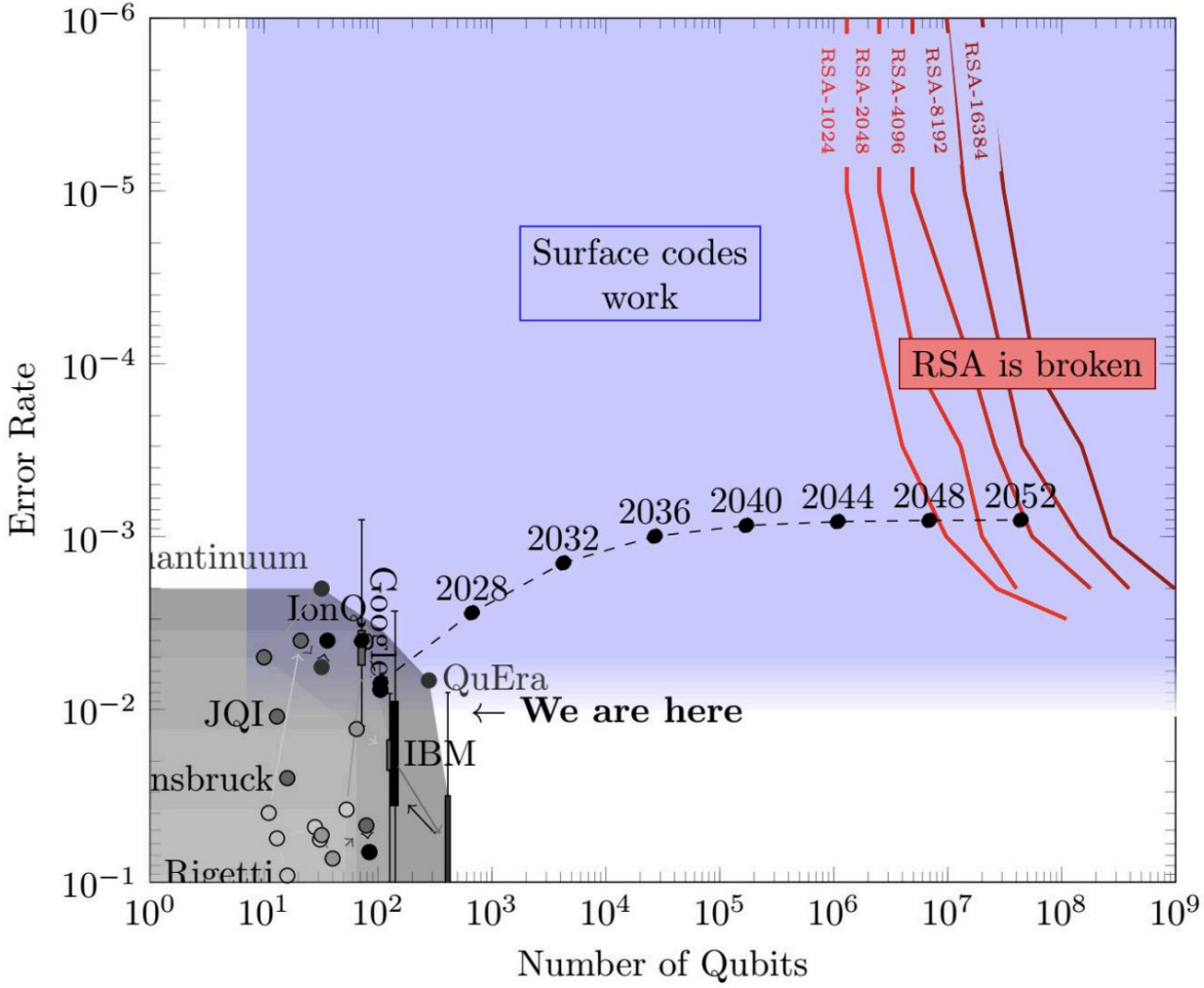
The Quantum Threat

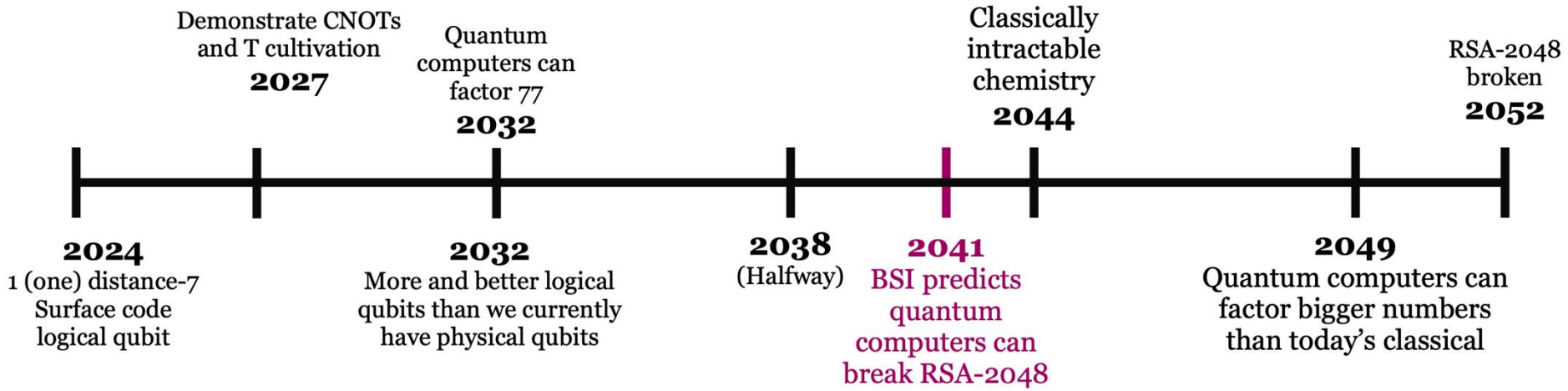
Quantum computers are not better; they are different

They will generally be worse, but do specific things better

In theory, they can break public key encryption and digital signatures based on factoring and discrete log assumptions

There are many recent developments in quantum computing


Error Rate
Number of Qubits
Surface codes work
RSA is broken
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
2028
2032
2036
2040
2044
2048
2052
← We are here
QuEra
IBM
JQI
IonQ
Google
Rigetti


Demonstrate CNOTs and T cultivation
2027
Quantum computers can factor 77
2032
Classically intractable chemistry
2044
RSA-2048 broken
2052
2024
1 (one) distance-7 Surface code logical qubit
2032
More and better logical qubits than we currently have physical qubits
2038
(Halfway)
2041
BSI predicts quantum computers can break RSA-2048
2049
Quantum computers can factor bigger numbers than today's classical

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

Quantum Safe Cryptography

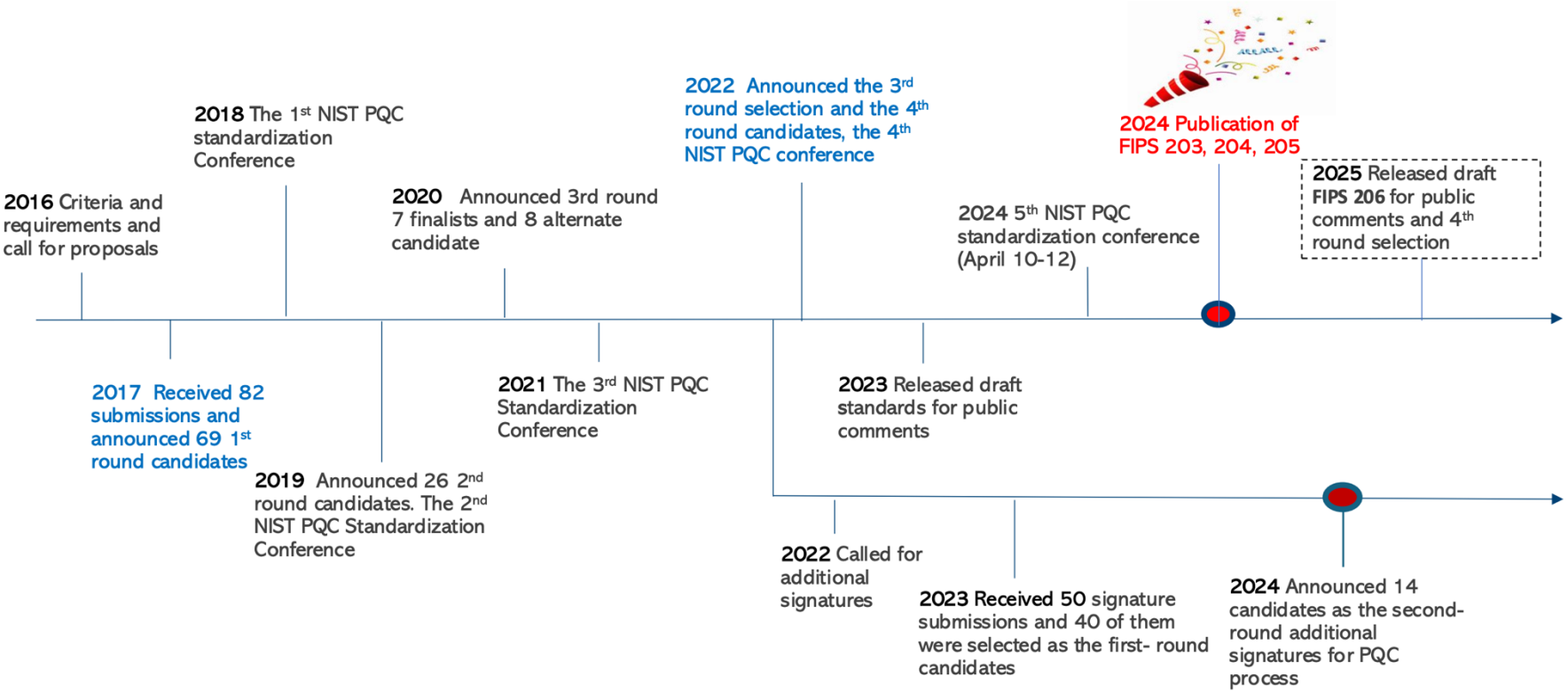
Cryptography that runs on classical computers, but is secure against attacks from quantum computers

Cryptographers have been working on this since the 90s

We have recently standardized several algorithms

There are tradeoffs in choosing which algorithms to use

Timeline


2016 Criteria and requirements and call for proposals
2017 Received 82 submissions and announced 69 1st round candidates
2018 The 1st NIST PQC standardization Conference
2019 Announced 26 2nd round candidates. The 2nd NIST PQC Standardization Conference
2020 Announced 3rd round 7 finalists and 8 alternate candidate
2021 The 3rd NIST PQC Standardization Conference
2022 Announced the 3rd round selection and the 4th round candidates, the 4th NIST PQC conference
2022 Called for additional signatures
2023 Released draft standards for public comments
2023 Received 50 signature submissions and 40 of them were selected as the first- round candidates
2024 5th NIST PQC standardization conference (April 10-12)
2024 Publication of FIPS 203, 204, 205
2024 Announced 14 candidates as the second-round additional signatures for PQC process
2025 Released draft FIPS 206 for public comments and 4th round selection

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Quantum Migration

Be aware of the «Harvest now, decrypt later» attack today

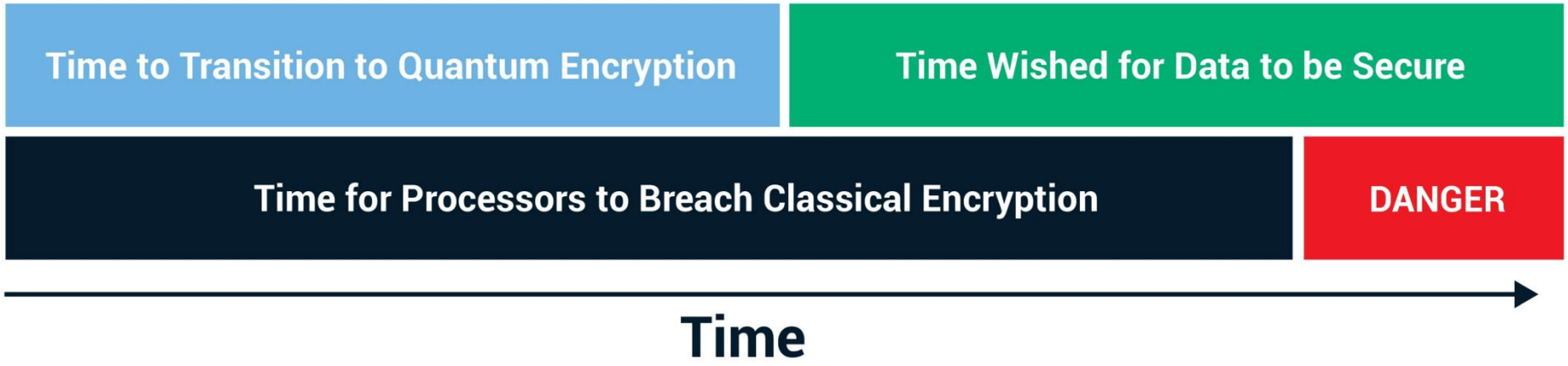
Digital signatures must be replaced in time; this is crucial

The most important step today is to get a complete overview

Get familiar with new standards and recommendations

Make a plan for the transition in your own organization

Urgency: Mosca's Inequality



Don't wait - upgrade your encryption now!

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Nye, kvantesikre standarder som erstatter dagens kryptografi, er underveis internasjonalt. NSM gir norske virksomheter råd om hvordan gjennomføre kvantemigrasjonen, en forflytning til kvantesikre IT-systemer og kryptografiske løsninger.

Sårbare algoritmer

Oversikt over utvalg av algoritmer som er i bruk i dag, men som vil være sårbar overfor kryptografiske relevante kvantedatamaskiner. Listen blir oppdatert.

Oversiktsrapport for kryptografiske ressurser og systemer

Se NSMs liste på informasjon om kryptografiske løsninger som kan være viktig å inkludere i en oversiktsrapport i forbindelse med kvantemigrasjon.

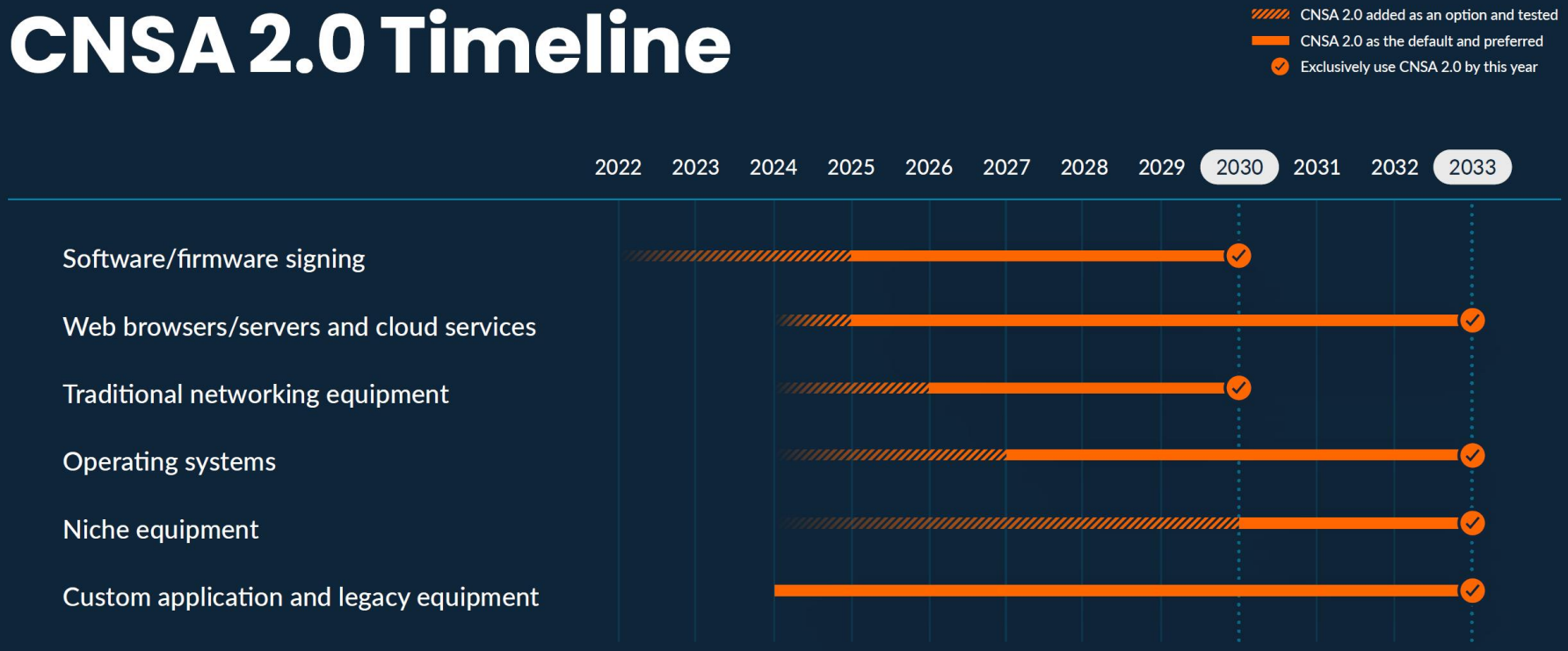
Veileder: Kvantemigrasjon

Denne veilederen gir en innføring i aktuelle problemstillinger og råd om hvordan virksomheter kommer i gang med kvantemigrasjon.

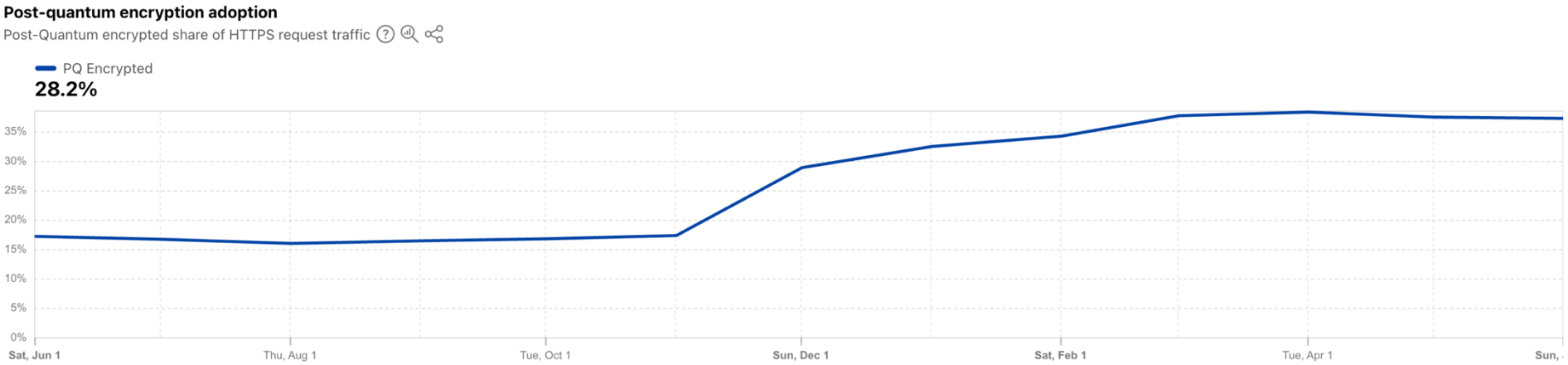
Hva er kvantemigrasjon?

Når såkalte kryptoanalytiske relevante kvantedatamaskiner blir tilgjengelige, blir mye av eksisterende kryptering ubrukelig.

CNSA 2.0 Timeline



Google Chrome + Cloudflare servers



Main Takeaways

Start the migration process today: overview, standards,…

Make a plan, tie it to budgeting, staffing, and responsibilities

Pay attention to the news, recommendations, and activities

Talk to your partners or others who can help with migration

Norwegian University of
Science and Technology

THANKS!