Post-Quantum Security: Threads and Strategic Actions

(WSO2Con - Barcelona, Spain - March 20th, 2025)

Prof. Dr. Dr. h.c. Frank Leymann

WSO2 Technology Fellow

Agenda

The State: Classical Cryptography

The Threat: Quantum Computing

The Defense: Post-Quantum Cryptography

The Strategy: Becoming Quantum-Safe

Summary

Agenda

The State: Classical Cryptography

The Threat: Quantum Computing

The Defense: Post-Quantum Cryptography

The Strategy: Becoming Quantum-Safe

Summary

RSA

RSA is centered around prime numbers

- Public key is the product of two (secrete) large prime numbers
- Private key is computed from these prime via a well-known algorithm
- If the prime numbers can be computed, the private key can easily be derived

Thus, computing the prime numbers of the public key means to crack the private key

An algorithm to compute prime factors ("factorization") breaks RSA!

But all know classical algorithms are exponential ⇒ RSA is considered secure

DSA vs. RSA

DSA (Digital Signature Algorithm) uses different algorithms but its security is based on the same underlying mathematical problem ("computing discrete logarithms")

End-to-end, DSA and RSA are comparable in terms of performance and protection

- Encryption / decryption
- Signing / verifying

Degree of protection ("security level") depends on size of the keys

A mechanism with smaller keys but same security level is desirable

Elliptic Curves

An elliptic curve is a special kind of curve

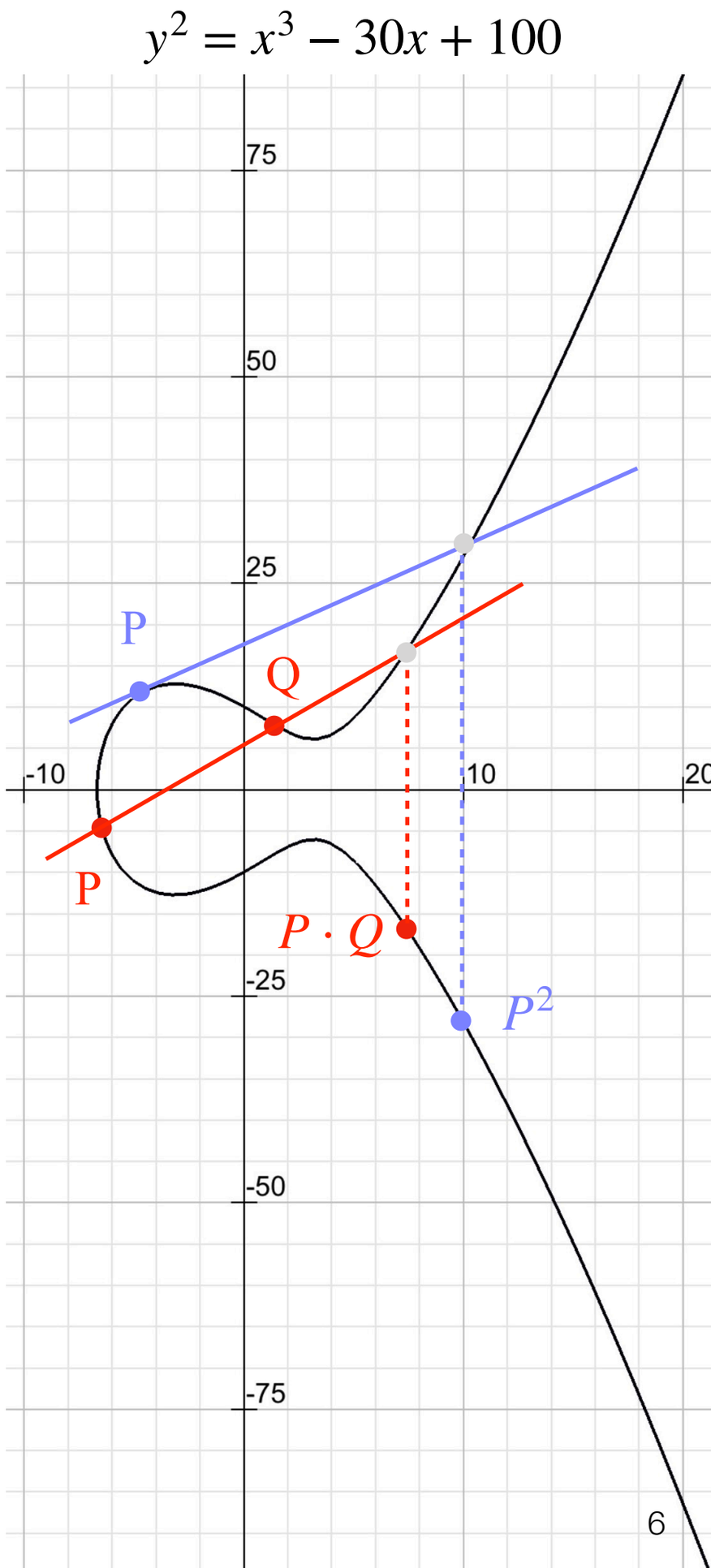
Computations can be performed with points of the curve

ECC (Elliptic Curve Cryptography) is based on these computations

Cracking a private key requires to solve a certain equation

All know classical algorithms
to solve this equation are exponential

⇒ ECC is considered secure



Public Key Infrastructure

Ubiquitous use of RSA, DSA, ECC, e.g.

- TLS handshake
- Encryption, decryption
- Digital signatures
- Cryptocurrencies
- Secure Messaging
- Certificates
- …

Breaking these algorithms
is a major hit of today's IT Infrastructure

Serious impact on
companies, government, public life,…

Agenda

The State: Classical Cryptography

The Threat: Quantum Computing

The Defense: Post-Quantum Cryptography

The Strategy: Becoming Quantum-Safe

Summary

Meet the Qubit

A quantum bit is true (in state $|1\rangle$) and false (in state $|0\rangle$) at the same time

I.e. a qubit q is a superposition of $|1\rangle$ and $|0\rangle$

$$q = \alpha\,|0\rangle + \beta\,|1\rangle$$

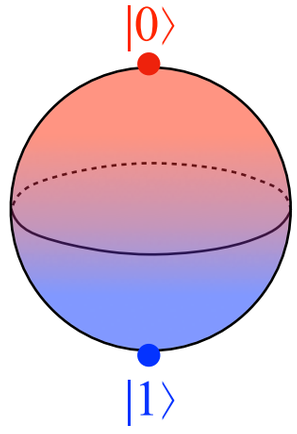
$|\alpha|^2$: Probability of measuring $|0\rangle$

$|\beta|^2$: Probability of measuring $|1\rangle$

When measuring, one of $|1\rangle$ or $|0\rangle$ will show up, i.e. it is $|\alpha|^2 + |\beta|^2 = 1$

Bit

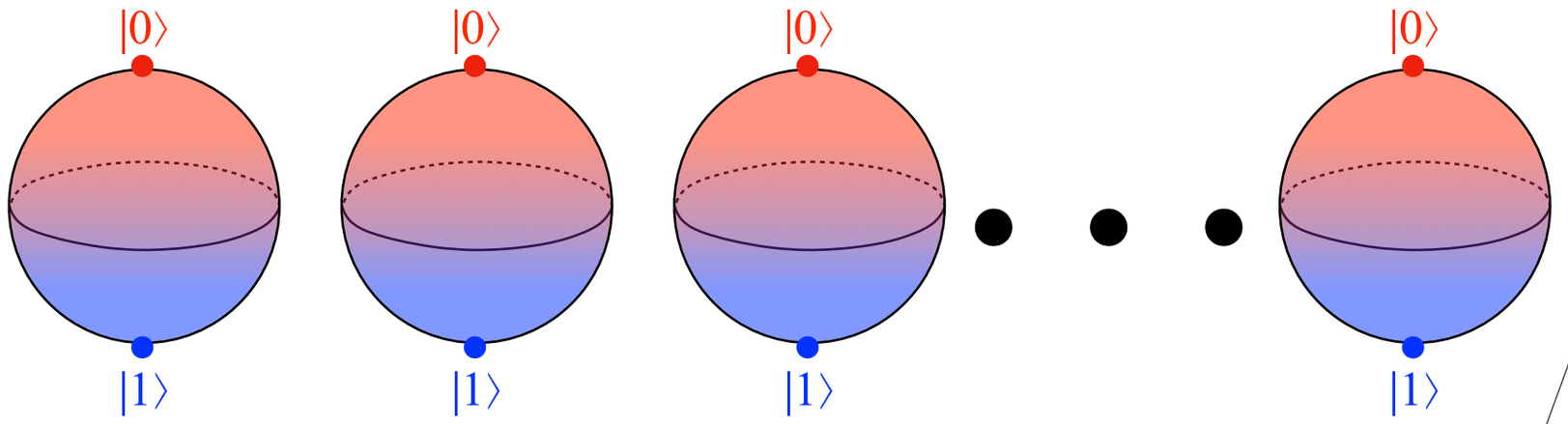
A bit is either "0" or "1"
→ Two possible values



Qubit

A qubit is an arbitrary point on the "Bloch sphere"
→ Infinitely many possible values

Quantum Register



IBM has ≈ **400 qubits** commercially available

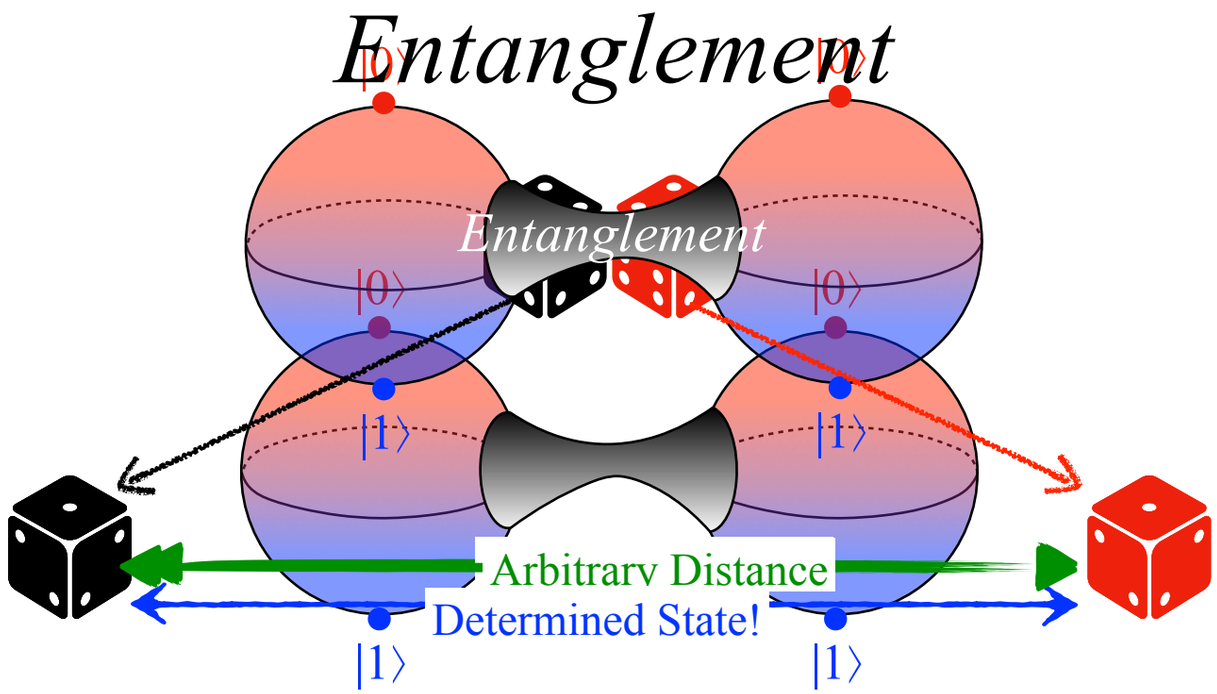
n qubits ⇒ superposition of 2^n values at the same time
(all combinations of $|0\rangle$ and $|1\rangle$, i.e. $|00\ldots0\rangle, |10\ldots0\rangle, |01\ldots0\rangle, \ldots, |11\ldots1\rangle$)

#atoms in universe $\leq 10^{90} = (10^3)^{30} \leq (2^{10})^{30} = 2^{300}$ ↦ n=300 Qbits

…and all values are manipulated at the same time!

Quantum Parallelism

The Miracle

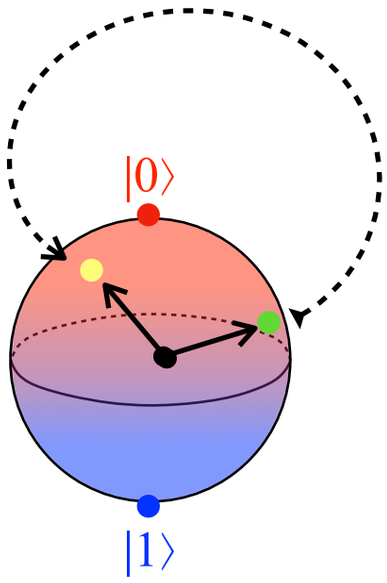


Entanglement is unique for quantum computing!

Every quantum algorithm showing exponential speedup compared to classical algorithms, must exploit entanglement.

Quantum Algorithm

$$U = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$



A qubit q is a vector of length 1
(i.e. a point on the Bloch sphere)

An operation on a qubit transforms it into another vector of length 1

Such a length-preserving map is called *unitary*

A series of such operations is again unitary

A quantum algorithm is a unitary transformation of a quantum register

This is very, very different from classical algorithms / programming!
(impact of skill planning)

Shor's Quantum Algorithm

- Quantum algorithm that can compute prime factors in polynomial time
  - …in fact, the algorithm can compute discrete logarithms
- Thus, a (future) quantum computer can crack today's cryptography based on, e.g., …
  - …prime factorization (e.g. RSA)
  - …elliptic curves (e.g. ECC)

CRQC

Cryptographically Relevant Quantum Computer

- It takes only days to crack RSA, hours to crack ECC

Why Should You Care Today?

Many data that are secret and have to be kept for many years are encrypted with current methods

⇒ These data can be cracked in the foreseeable future!

Quantum-safe procedures require changes to the (software) infrastructure

- E.g. new encryption algorithms

⇒ Building this infrastructure takes many years!

Agenda

The State: Classical Cryptography

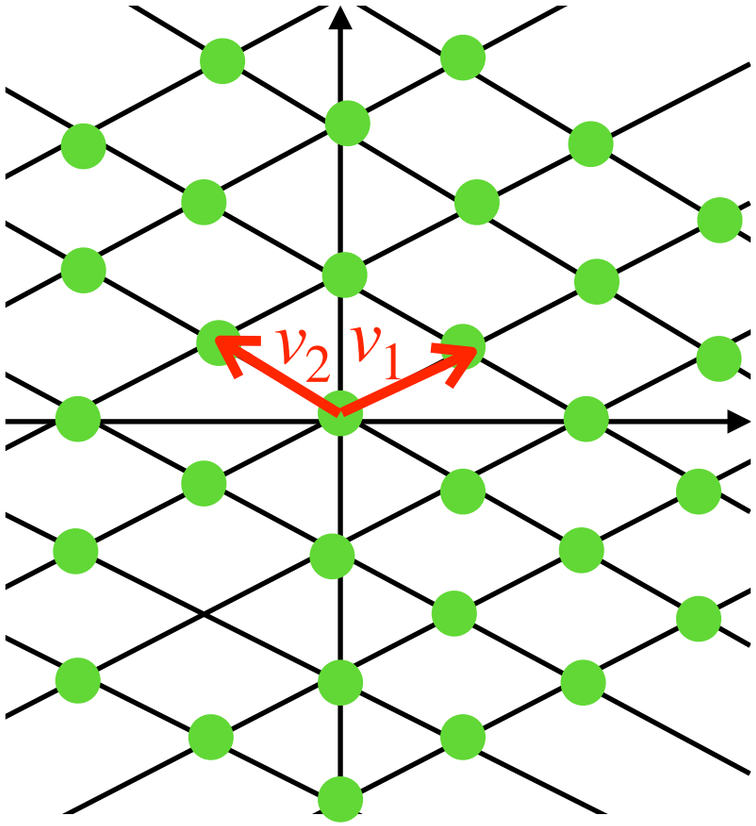
The Threat: Quantum Computing

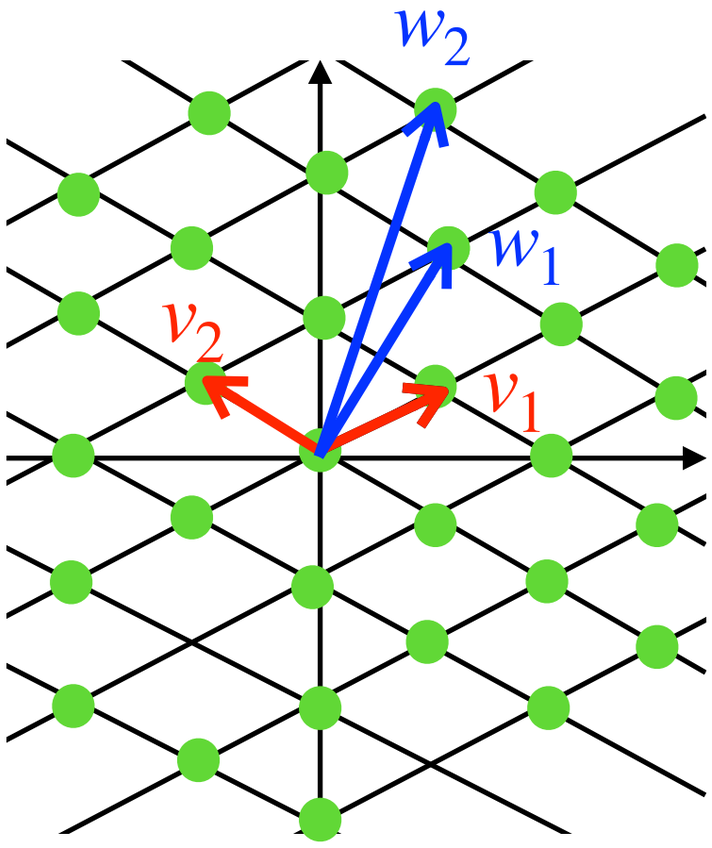
The Defense: Post-Quantum Cryptography

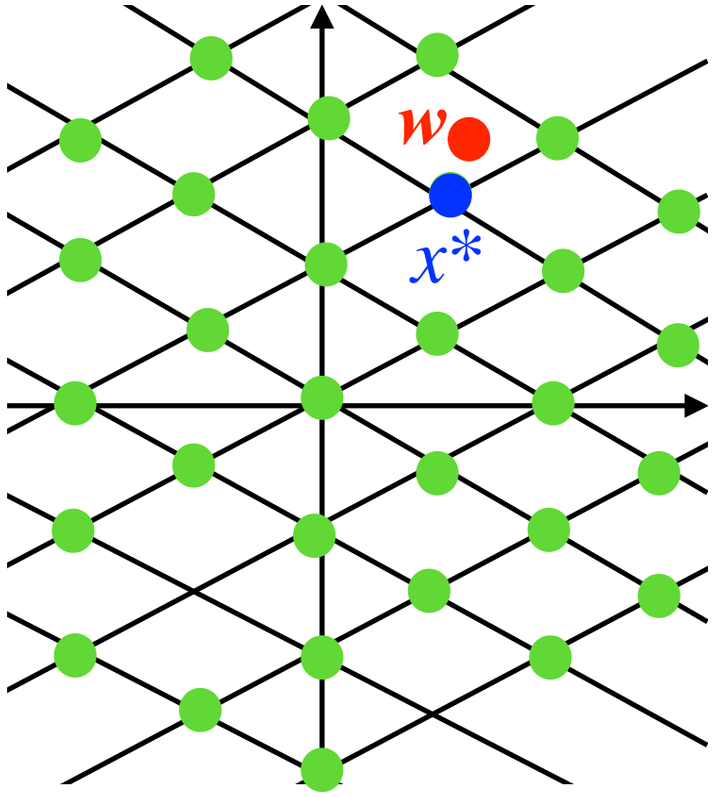
The Strategy: Becoming Quantum-Safe

Summary

Lattice-Based Cryptography







"Closest Vector Problem"

- "Good basis" v_1, v_2 is private key, "bad basis" w_1, w_2 is public key
- A message / document is transformed into point w (encryption)
- Computing the closest vector x^* and "smart rounding" means decryption

All know algorithms (classical and quantum) are exponential

⇒ Lattice-based cryptography is considered secure

Post-Quantum Cryptography (PQC)

(aka: Quantum-Safe or Quantum-Resistant)

...this refers to cryptographic algorithms which, according to todays knowledge, are secure against attacks with a quantum computer

- I.e. no quantum algorithm is known to crack such an algorithm

- Most of the algorithms "common" today are <u>not</u> quantum-safe
  - Factorization, elliptical curves,…

But:
There is no guarantee that these algorithms cannot be cracked at some point by quantum computers (or even classic computers)!

NIST PQC

(Post Quantum Cryptography)

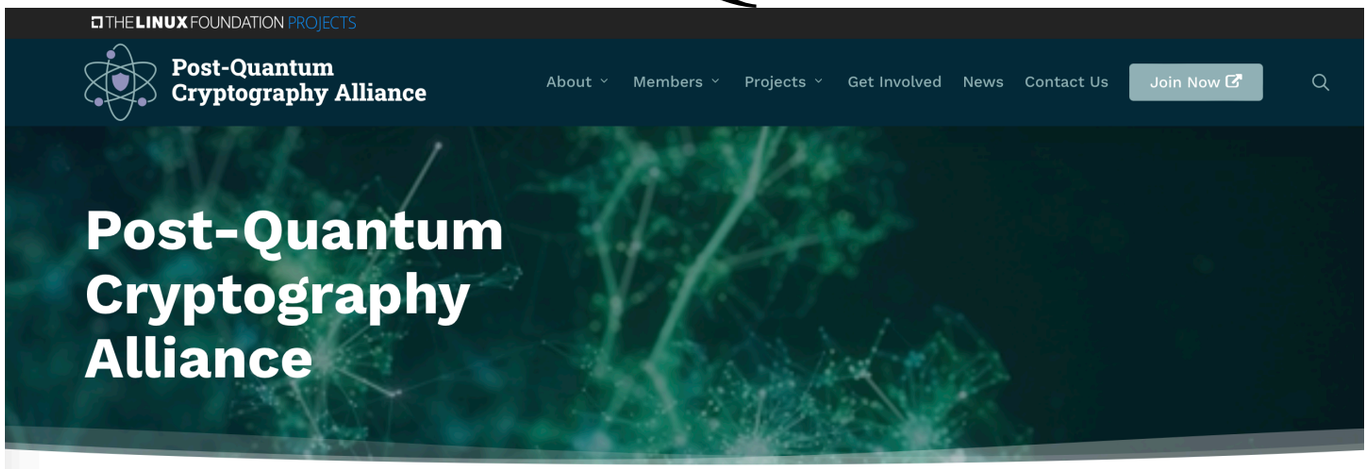
Website: https://csrc.nist.gov/projects/post-quantum-cryptography

Process to submit, evaluate, recommend, and standardize quantum-safe algorithms

Published standards

- Module-Lattice-based Key-Encapsulation Mechanism
  - https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
- Module-Lattice-Based Digital Signature Standard
  - https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf
- Stateless Hash-Based Digital Signature Standard
  - https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

PQCA



To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.

https://pqca.org/

Projects

Open Quantum Safe

Open Quantum Safe (OQS) project aims to support the development and prototyping of quantum-resistant cryptography.

Learn More

PQ Code Package

Creating and maintaining high-assurance implementations of standards-track post-quantum cryptography algorithms.

Learn More

OQS: Open Quantum Safe

(https://openquantumsafe.org/)

Open-source project to support development and prototyping of quantum-resistant cryptography

Two main lines of work

- liboqs — open source C library for quantum-resistant cryptographic algorithms
- Prototype integrations into protocols and applications

Everything is in Github repositories

Lots of contributors
(from companies like AWS, IBM, Microsoft, Cloudflare, Intel, Cisco as well as universities)

Agenda

The State: Classical Cryptography

The Threat: Quantum Computing

The Defense: Post-Quantum Cryptography

The Strategy: Becoming Quantum-Safe

Summary

Quantum Computing Cybersecurity Preparedness Act

US Law

Public Law 117 - 260 - Quantum Computing Cybersecurity Preparedness Act

Summary | Related Documents

Category	Bills and Statutes
Collection	Public and Private Laws
SuDoc Class Number	AE 2.110:117-260
Law Number	Public Law 117-260
Date Approved	December 21, 2022
Full Title	An act to encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.
Bill Number	H.R. 7535
Report Number	S Rept. 117-251
Statutes at Large Citations	136 Stat. 2389, 2390, 2391 and 2392
United States Code Citations	44 U.S.C. 3502, 3552 and 3553 Chapter 35
Legislative History	LEGISLATIVE HISTORY–H.R. 7535 (S. 4592):

https://www.govinfo.gov/app/details/PLAW-117publ260

THE WHITE HOUSE

Administration Priorities The Record Briefing Room Español MENU

MAY 04, 2022

Home

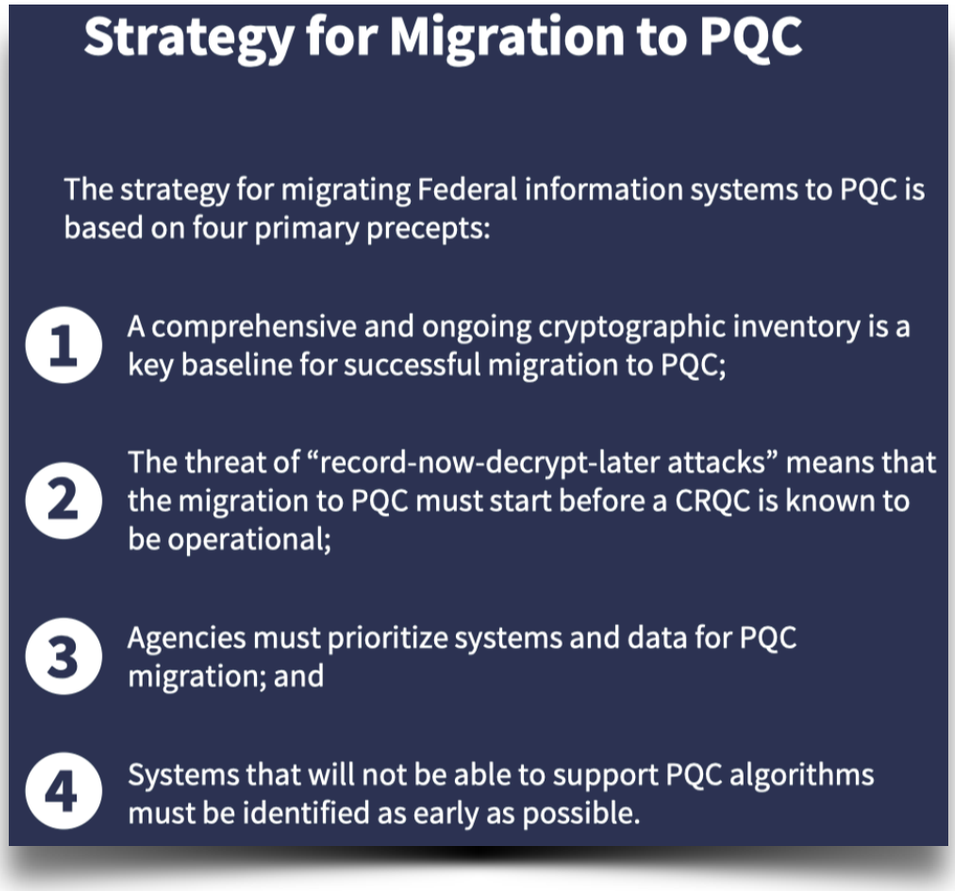
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

...the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography

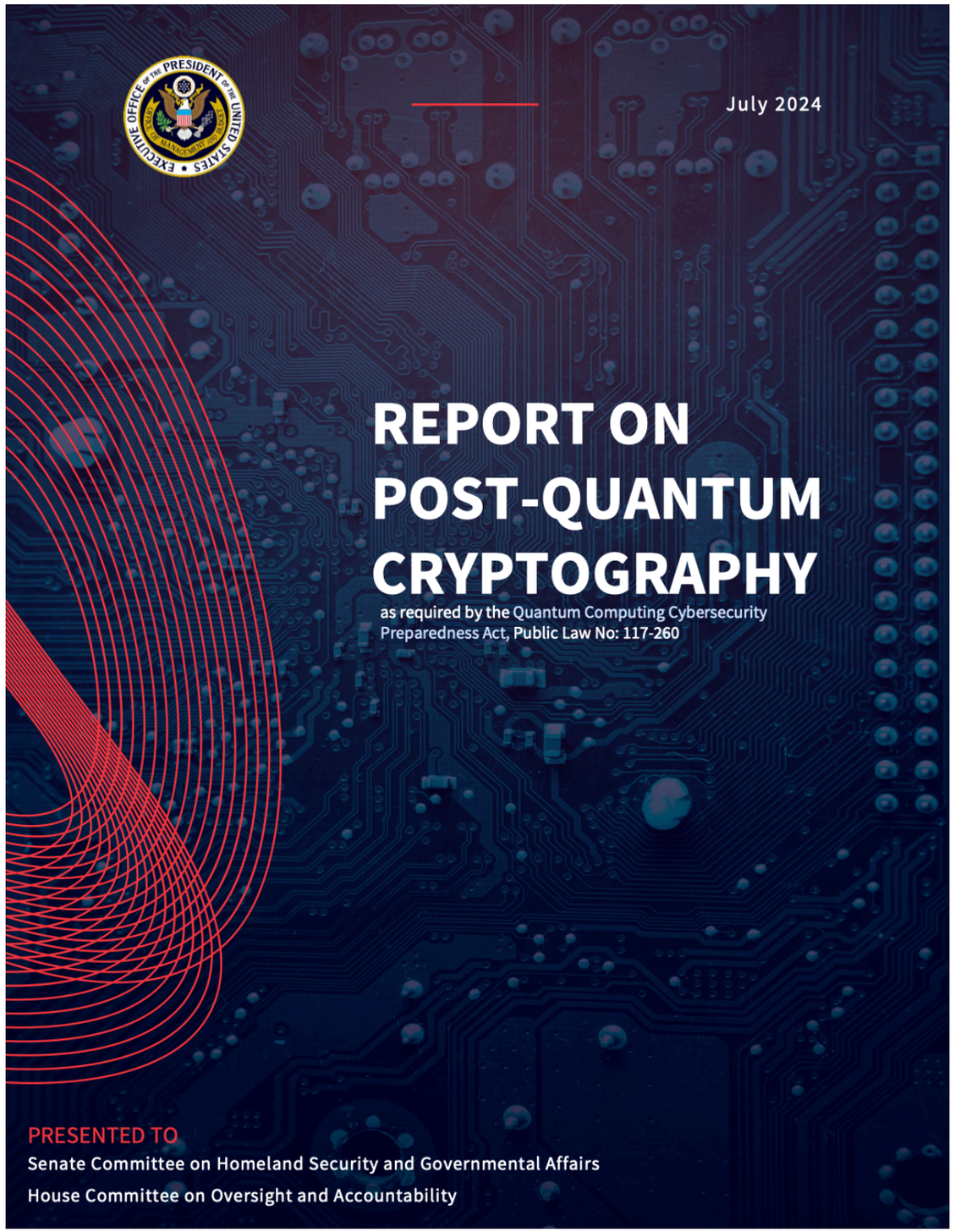
https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

US Gov Strategy

Strategy in reaction to the preparedness act



Cost to migrate Gov IT > 7 Billion US$



EU is Acting Too

EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

https://ec.europa.eu/newsroom/dae/redirection/document/104249

Companies

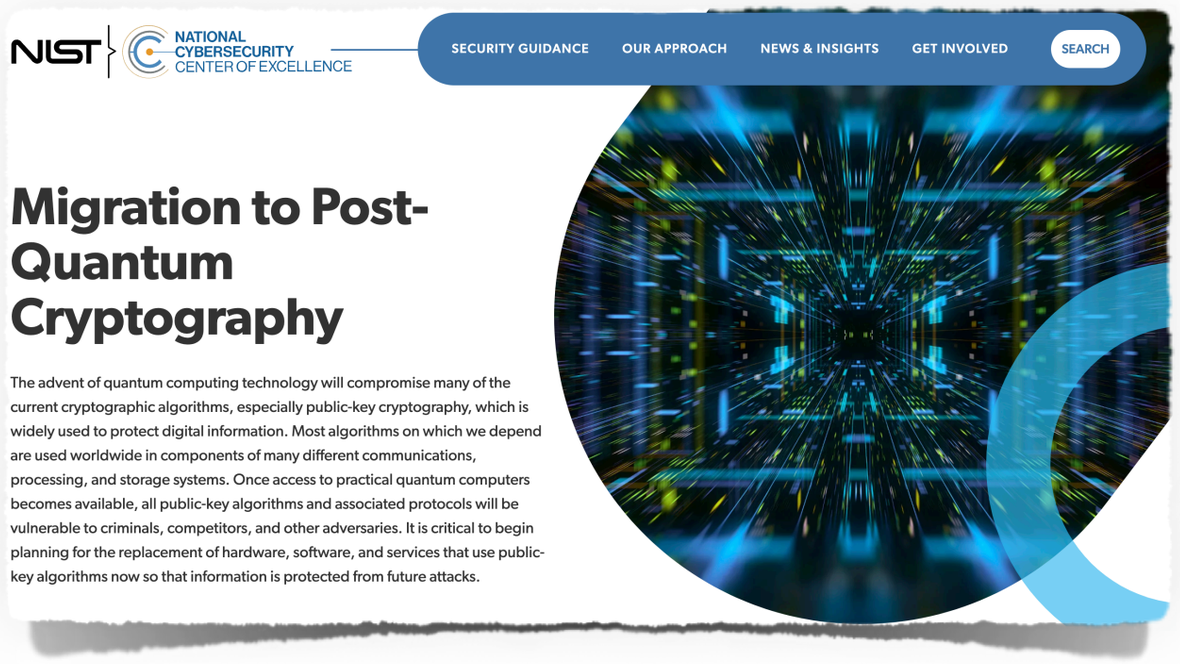
- AWS
- Microsoft
- Google
- IBM
- Cloudflare
- …
- WSO2
  - Ballerina "quantum-safe"
  - IS / Asgardeo communication & data protection

Crypto-Agility

≡ protect against the failure of encryption procedures

- Since (some) post-quantum procedures may also be cracked, the new infrastructure must make it as easy as possible to exchange such procedures

- Instead of a simple exchange, there are also approaches to combine procedures in such a way that the overall procedure remains secure, even if a procedure involved is cracked



https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Systematic Review

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of current version 07 February 2025.

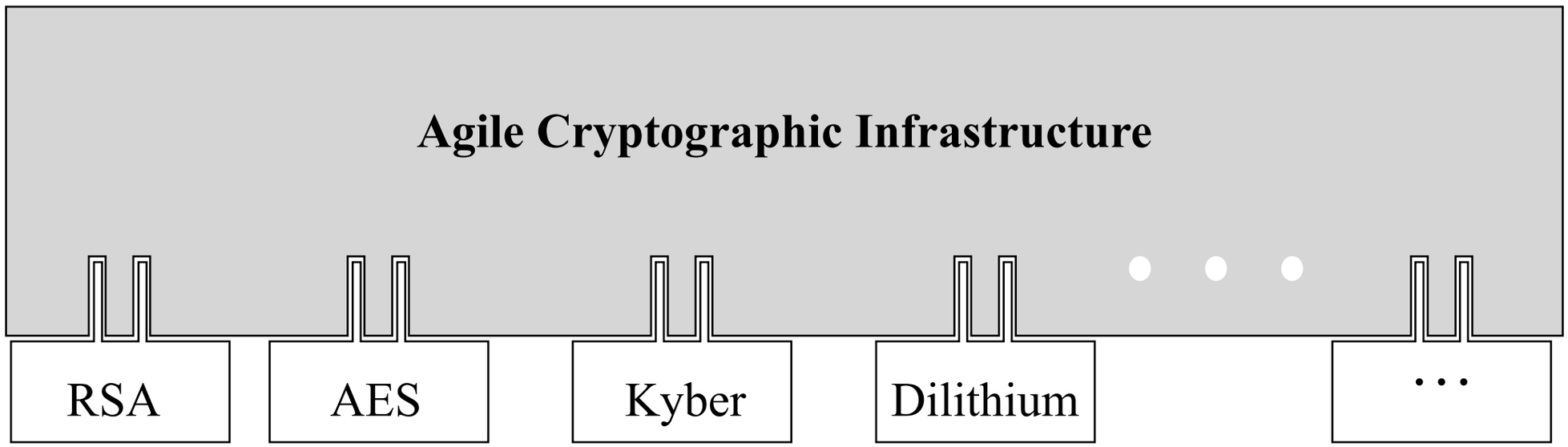
Digital Object Identifier

Toward a Common Understanding of Cryptographic Agility – A Systematic Review

CHRISTIAN NÄTHER[1], DANIEL HERZINGER[2], JAN-PHILIPP STEGHÖFER[1], (Member, IEEE), STEFAN-LUKAS GAZDAG[2], EDUARD HIRSCH[3], AND DANIEL LOEBENBERGER[4]

https://arxiv.org/abs/2411.08781

High-Level Architecture

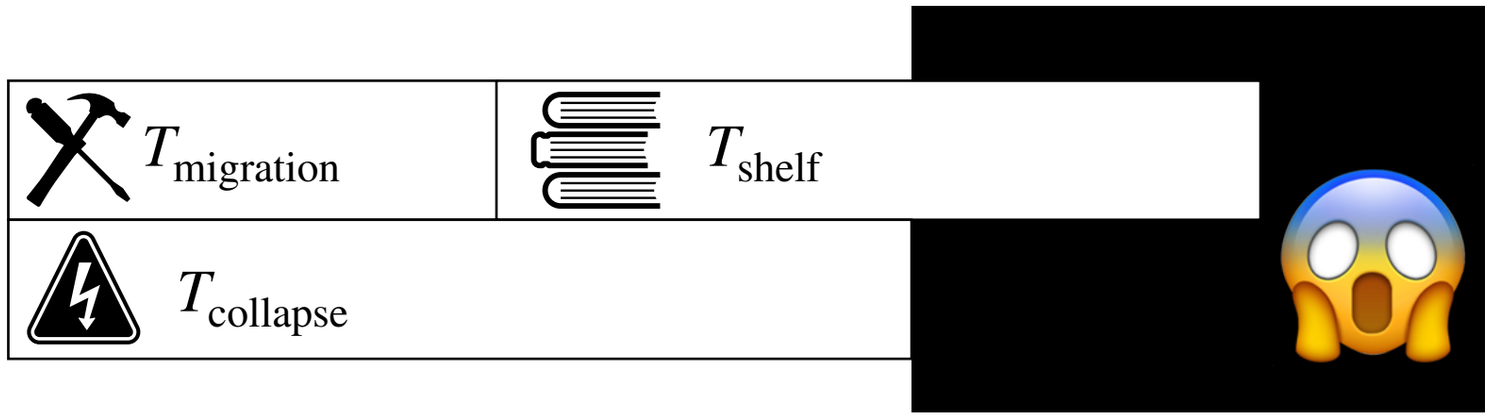


How Much Time Do You Have?

(Mosca's Inequality(*))

- Collapse Time T_{collapse} : number of years until a CRQC is available
- Migration Time $T_{\text{migration}}$: number of years needed to realize a quantum-safe solution
- Shelf-Life Time T_{shelf} : number of years information must be kept secrete

You are in trouble if: $T_{\text{shelf}} + T_{\text{migration}} > T_{\text{collapse}}$

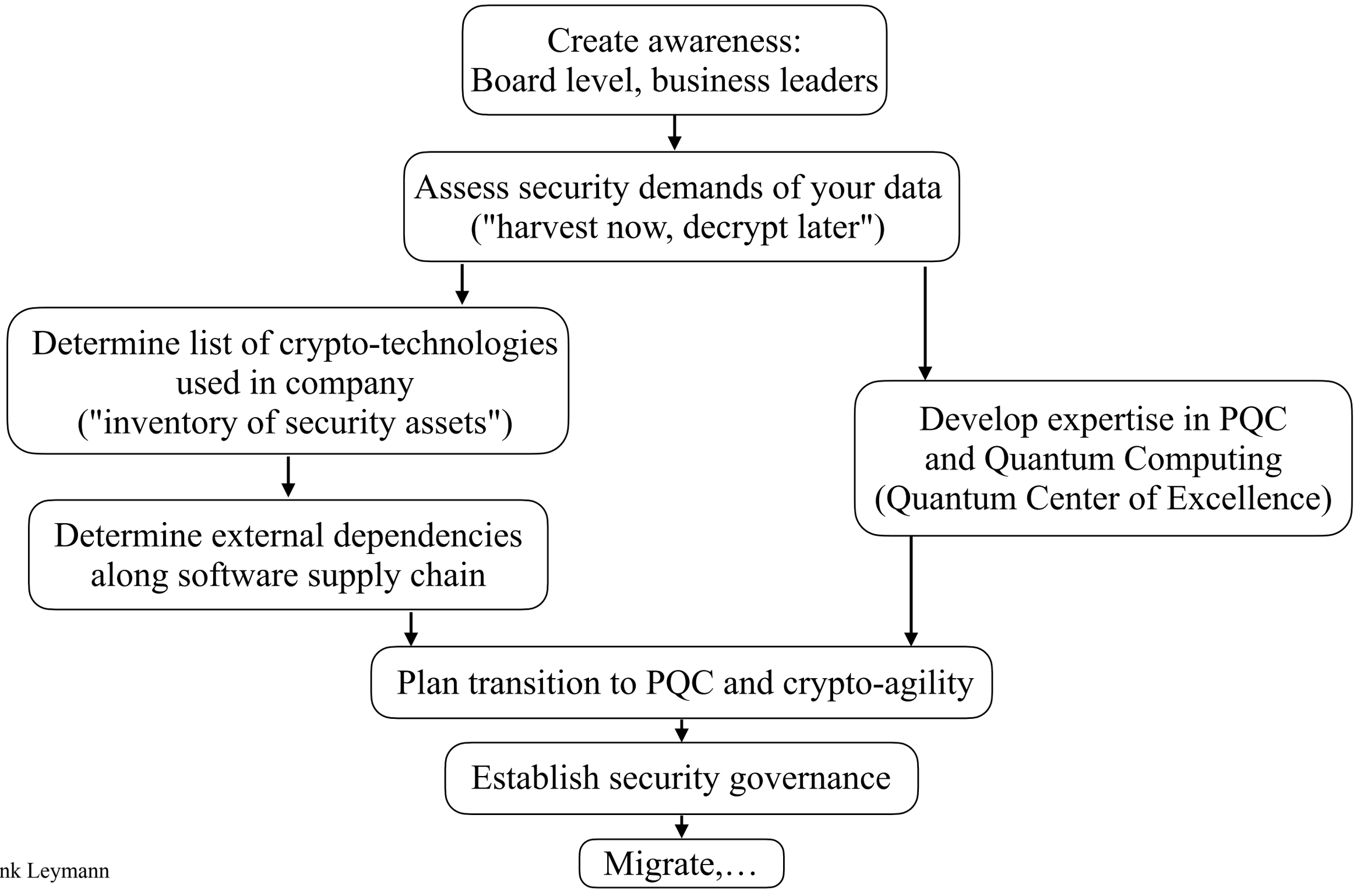


The time you have: $T^{\max}_{\text{migration}} := T_{\text{collapse}} - T_{\text{shelf}}$

- Assume $T_{\text{collapse}} = 10$ y , $T_{\text{shelf}} = 10$ y $\Rightarrow$ $T^{\max}_{\text{migration}} = 0$ y. **You must begin now!**

(*) https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

Sample Steps to Follow



Agenda

The State: Classical Cryptography

The Threat: Quantum Computing

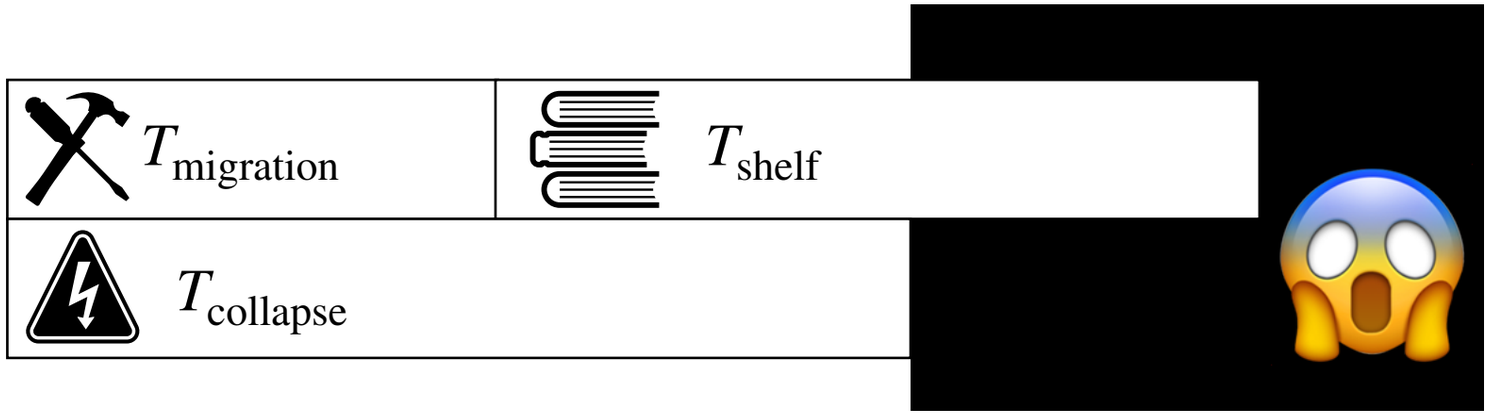
The Defense: Post-Quantum Cryptography

The Strategy: Becoming Quantum-Safe

Summary

Summary

- Today's crypto infrastructure relies on hardness of discrete logarithm problem
- Quantum computers will be able to crack this infrastructure mid-term
- Lattice-based cryptography seems to be a rescue
- Standards for post-quantum security are published, more under development
- Open source prototypes of these standards are available
- Quantum-safe infrastructure must be agile
- Time to act is now!



If you want to read more background:

Post-Quantum Security:
Origin, Fundamentals, and Adoption

Johanna Barzen[0000-0001-8397-7973] and Frank Leymann[0000-0002-9123-259X]

https://arxiv.org/abs/2405.11885 or

The End