Quantum Safe Cryptography

Surviving the Quantum Apocalypse

Christian Cohrs, SAP
May 21st, 2026

Agenda

Quantum Computers and how they affect classic cryptography

Quantum-Safe Cryptography in the SAP Cryptographic Library

Crypto Agility

Summary

Introduction

Quantum Computers and how they affect classic cryptography

Storing data in Classical and Quantum Computers: What is different?

Classical Computer

- Based on bits: **{0,1}**
- State of a bit is a scalar value, 0 or 1
- Operations based on Boolean Logic
- Value can be read at any time

Quantum Computer

- Quantum states that are based on Qubits:
  $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ or as a vector $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$
- State is a superposition of scalar values, where each value has a certain probability
- Operations based on Linear Algebra
- Value needs to be measured, at which point it collapses from a probability distribution to exactly one scalar value

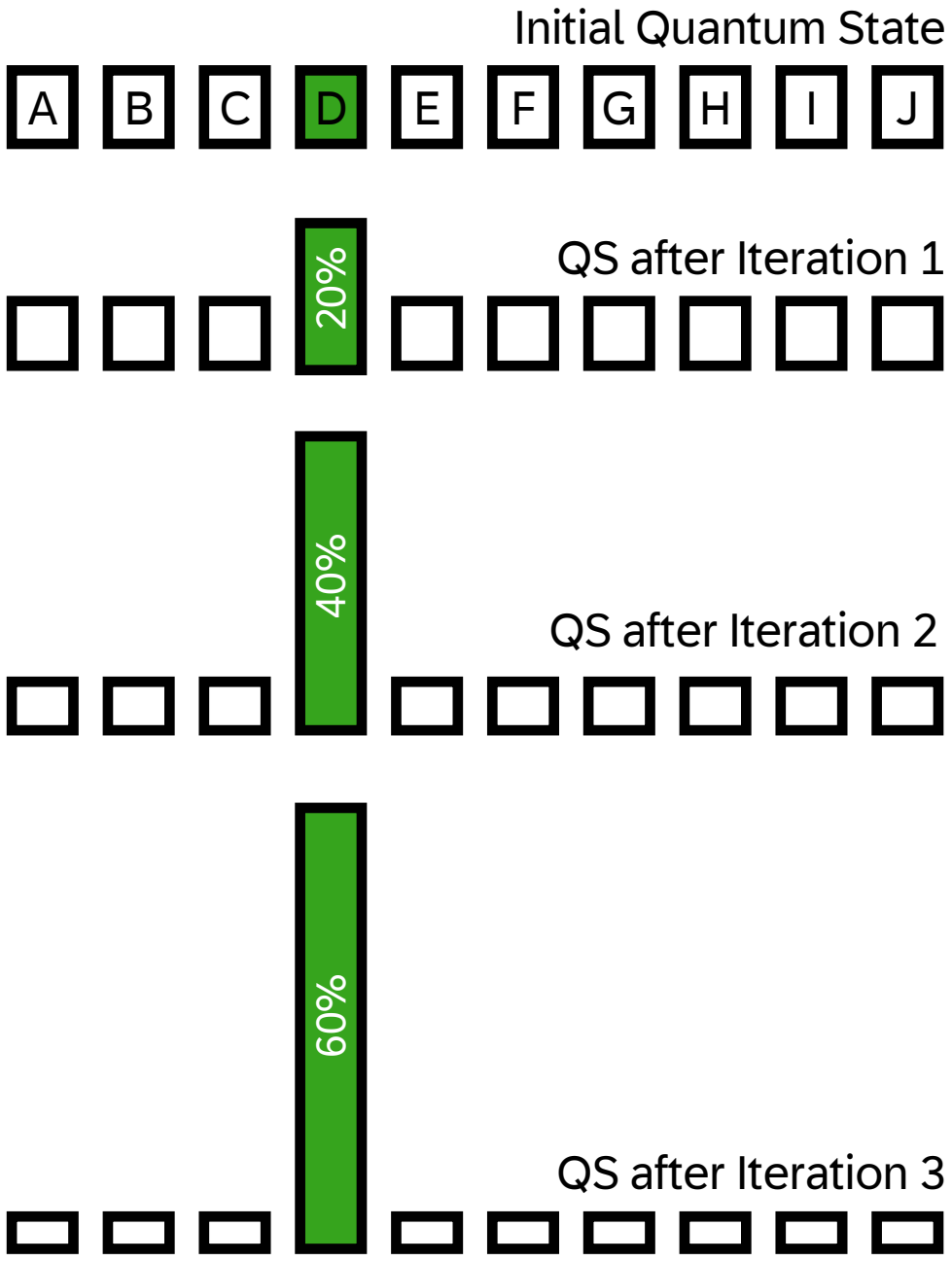
How does a Quantum Computer Program work?

Challenge to be solved: We know that for a given problem, one out of a set of ten values (A .. J) is the solution. We want to find that value.

Initial quantum state: A probability distribution of all possible values. Without any further knowledge, all values have the same probability, 10%.

Iterations: In each iteration, the quantum computer program increases the probability of the value that solves the problem, while reducing the probabilities for the other values.

Measurement: At the end of the iterations, we need to determine the actual value that is the solution. In this example, if we measure the quantum state after iteration 3, the measured value will be “D” with a probability of 60%.



Example of a Quantum Computer's superiority Reverse Phonebook Search

You live in a city with 1.000.000 inhabitants, who all have a phone number

You have a phone book that lists the number for any person

Now you have a phone number and want to find the person

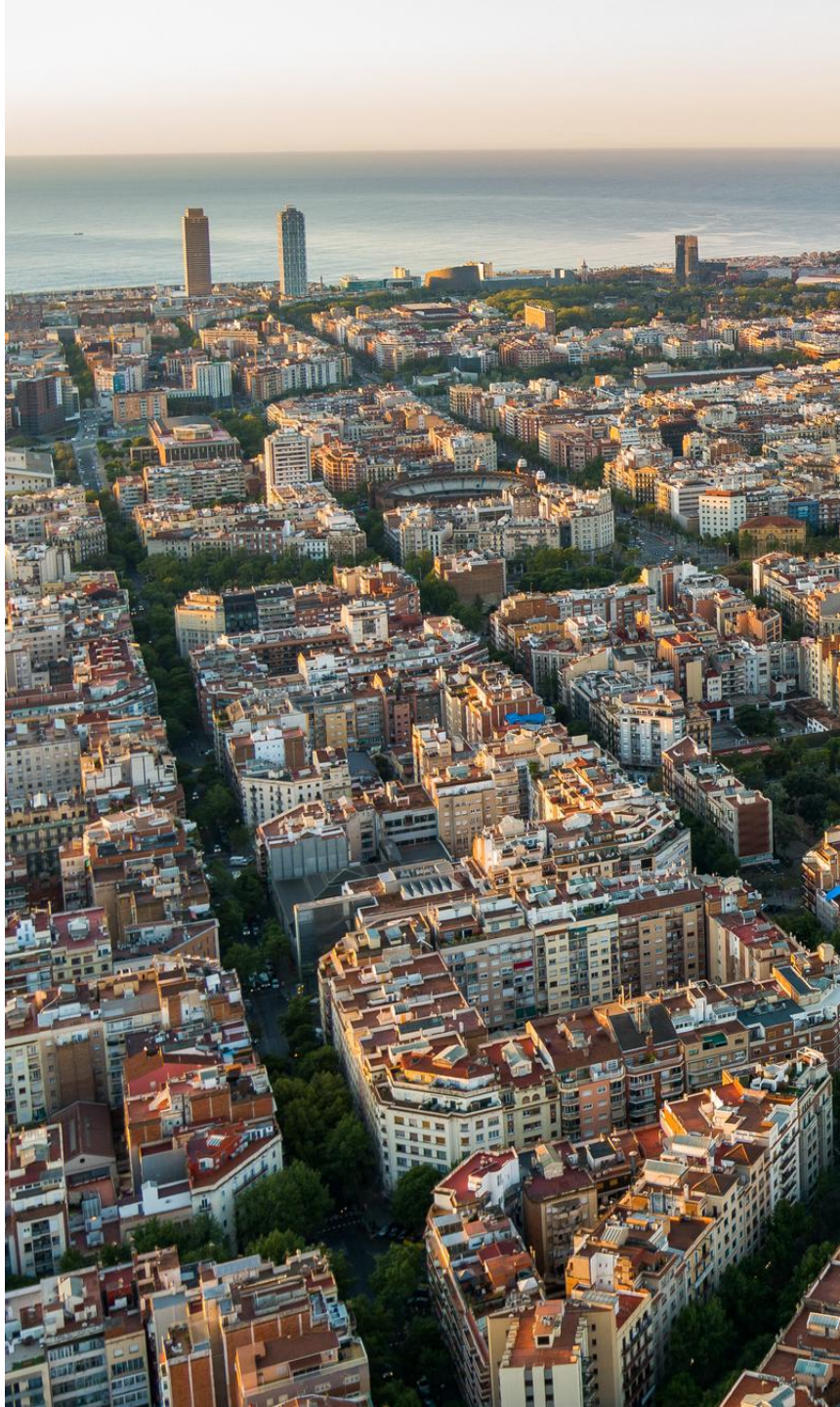
<u>Classic approach</u>

You read the phone book from A to Z until you find a name with the right number

On average you check **500.000** entries before you find it

<u>Quantum approach</u>

A Quantum Computer finds the right name with 99.9999% probability after **785** iterations on the quantum state, using "**Grover's algorithm**"



Attacking classic cryptographic algorithms with a Quantum Computer
Grover's algorithm

Grover's algorithm significantly reduces the time to break **symmetric encryption** (e.g. AES). However, by doubling the key size the original time can be restored.

The Integer Factorization Problem: Find the prime factors of a positive integer
A foundation for asymmetric cryptographic algorithms

Easy for 4 digits: $2025 = 81 \times 25 = 3^4 \times 5^2$

Not so easy for 250 decimal digits / 829 bits*:

RSA-250 =
2140324650240744961264423072839333563008614715144755017797754920881418023447
1401366433455190958046796109928518724709145876873962619215573630474547705208
0511905649310668769159001975940569345745223058932597669747168173806936489469
987157849497593749793 7

RSA-250 =
6413528947707158027879019017057738908482501474294344720811685963202453234463
0238623598752668347708737661925585694639798853367
×
3337202759497815655622601060535511422794076034476755466678452098702384172921
0037080257448673296881877565718986258036932062711

* https://en.wikipedia.org/wiki/RSA_numbers

Attacking classic cryptographic algorithms with a Quantum Computer Grover's algorithm and Shor's algorithm

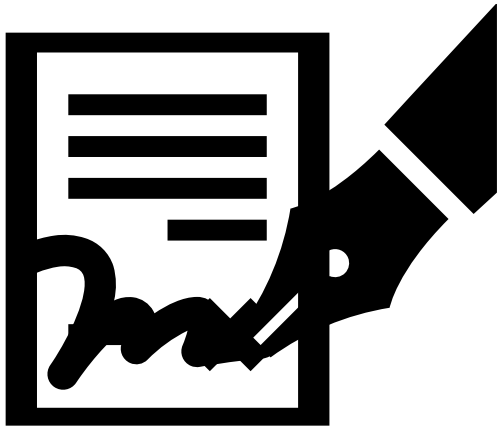
Grover's algorithm significantly reduces the time to break **symmetric encryption** (e.g. AES). However, by doubling the key size the original time can be restored.

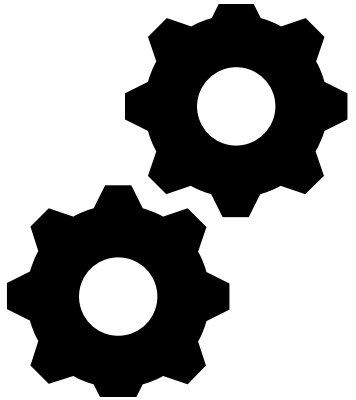
For **asymmetric cryptographic** algorithms (RSA, Diffie-Hellman, Elliptic Curve Cryptography,..), the efforts to find the solution are exponential on a classic computer, but only polynomial on a quantum computer, using **Shor's** algorithm

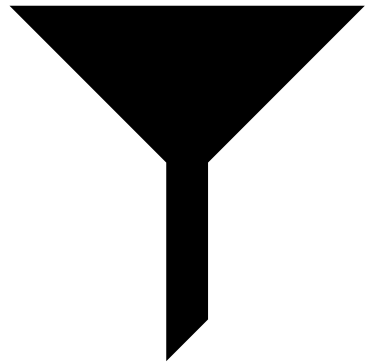
Cryptography in the Web and the Quantum Apocalypse

Broken by Shor's algorithm

Still OK despite Grover's algorithm





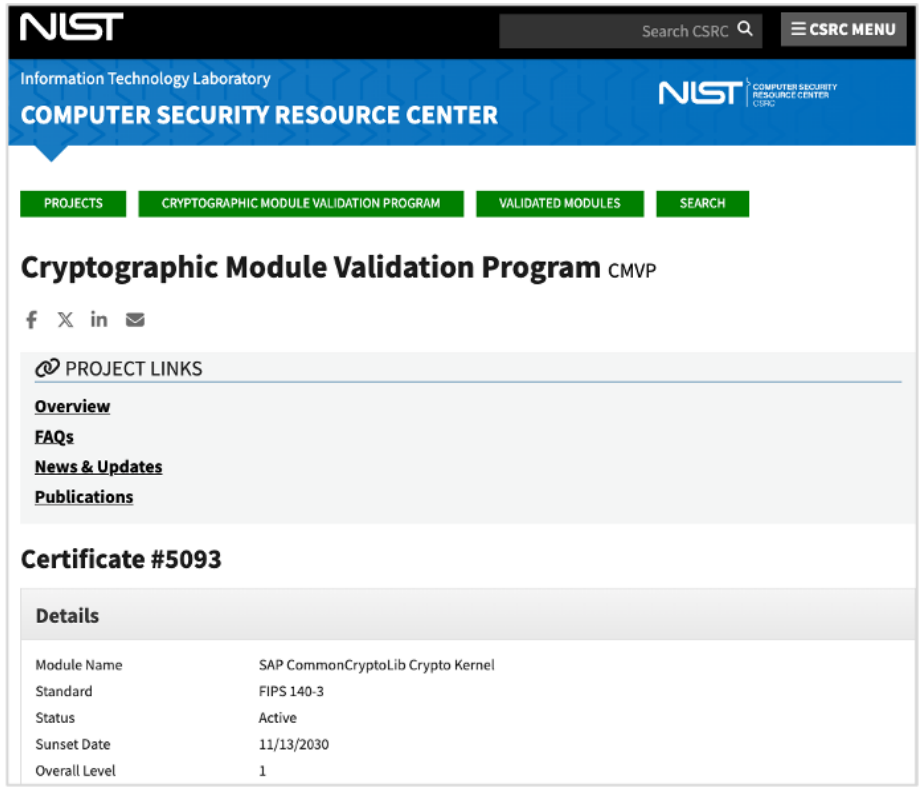


Key Agreement / Public-Key Encryption	Digital Signature / X.509 Certificate	Symmetric Encryption	Hash Function
RSA / (EC)DHE	RSA / (EC)DHE	AES-256	SHA-2 / SHA-3
Establish a **secure session key** for symmetric encryption	Verify **authenticity** of messages	Ensure **confidentiality**	Verify **integrity** of data

Quantum-Safe Cryptography in the SAP Cryptographic Library

Implementation in the SAP Cryptographic Library
Learnings and challenges when migrating to quantum-safe algorithms

SAP CommonCryptoLib Crypto Kernel is FIPS 140-3 validated!



"SAP **CommonCryptoLib Crypto Kernel v8.6.1** is a shared library, i.e. it consists of software only. SAP CommonCryptoLib Crypto Kernel provides an API in terms of C/C++ methods for key management and operation of cryptographic functions."

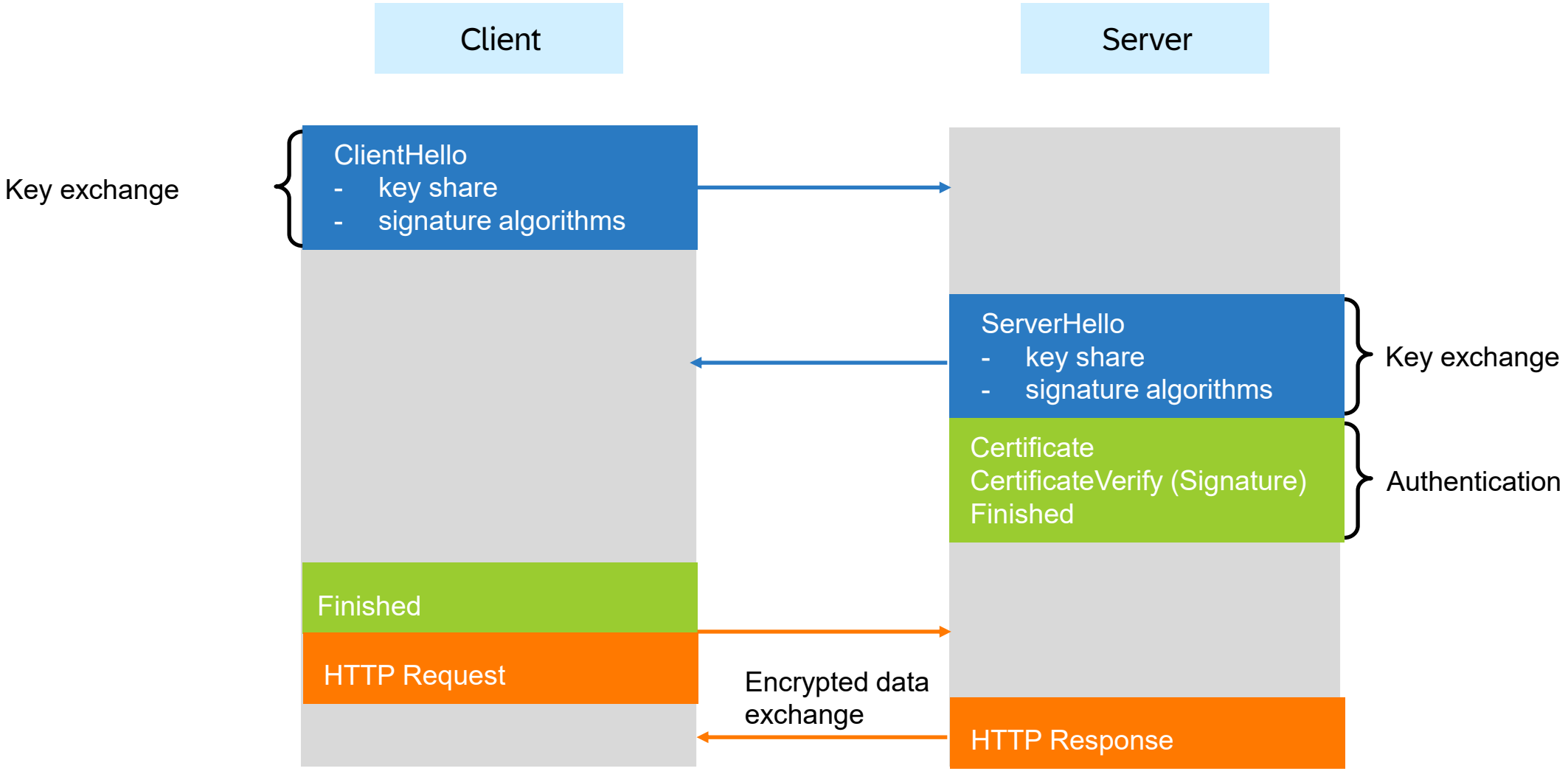
Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
5093	SAP SE	SAP CommonCryptoLib Crypto Kernel	Software	11/14/2025	Active

Quantum-safe Algorithms in SAP CommonCryptoLib (CCL)

- SAP CCL integrates open-source implementations of quantum-safe algorithms

- Quantum-safe algorithms in the latest CCL release
  - Module-Lattice-based **Key Encapsulation Mechanism** (ML-KEM, FIPS 203)
  - Module-Lattice-based **Digital Signature Standard** (ML-DSA, FIPS 204)

Cryptography in TLS 1.3 Handshake



Is TLS 1.3 quantum-safe?

Encryption of payload: symmetric cryptography like AES256-GCM is quantum-safe

Key agreement

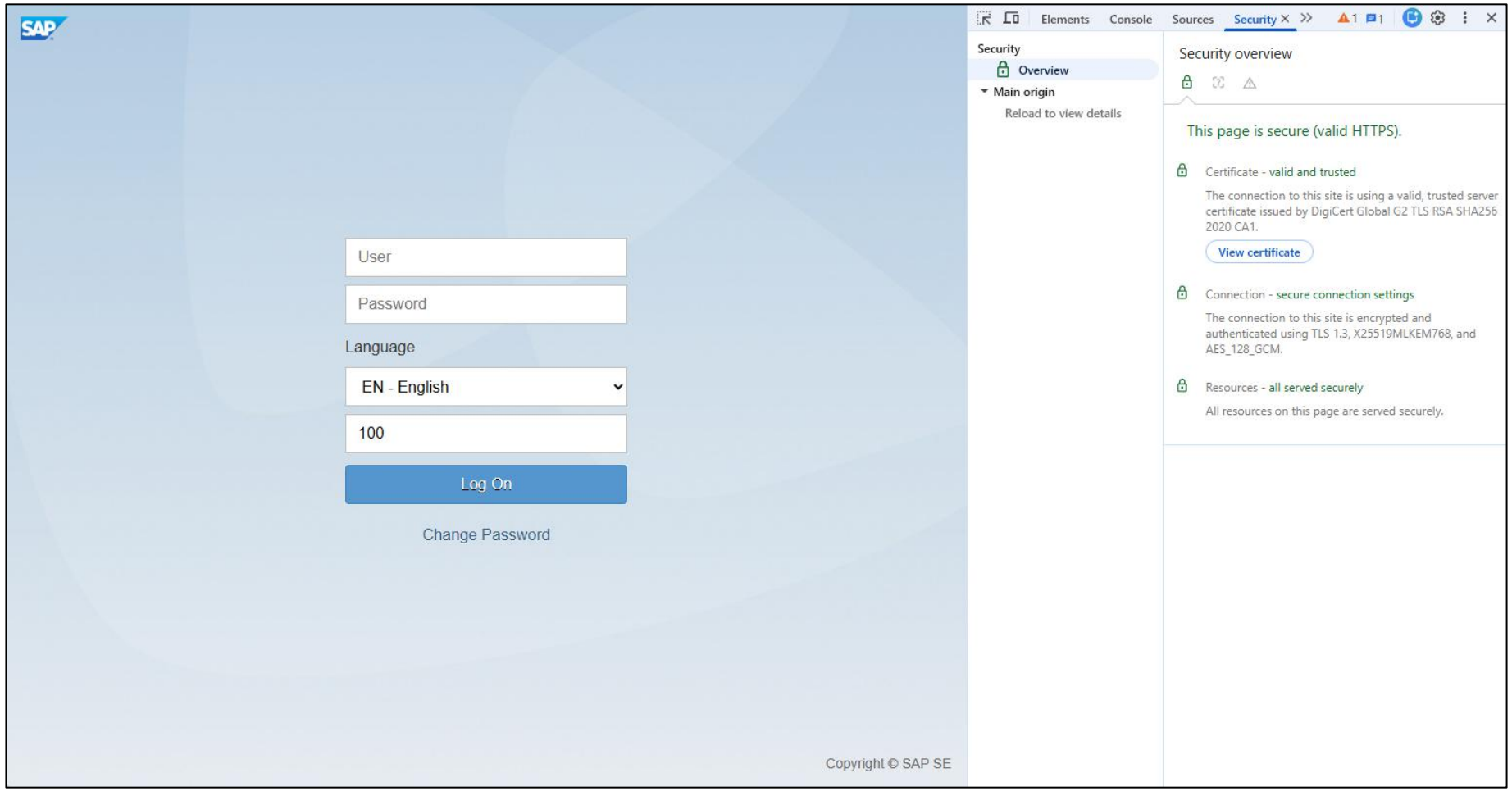
- RSA- and ECDHE-based key exchange schemes are vulnerable to quantum analysis
- Attack “Harvest-now-decrypt-later”
  - Now: harvest and store encrypted data
  - Later: compute the encryption key with a quantum computer, and decrypt the stored data

Authentication

- Classic digital signature algorithms like RSA and ECDSA are vulnerable to quantum analysis
- Attack: forge signatures using cryptographically relevant quantum computers

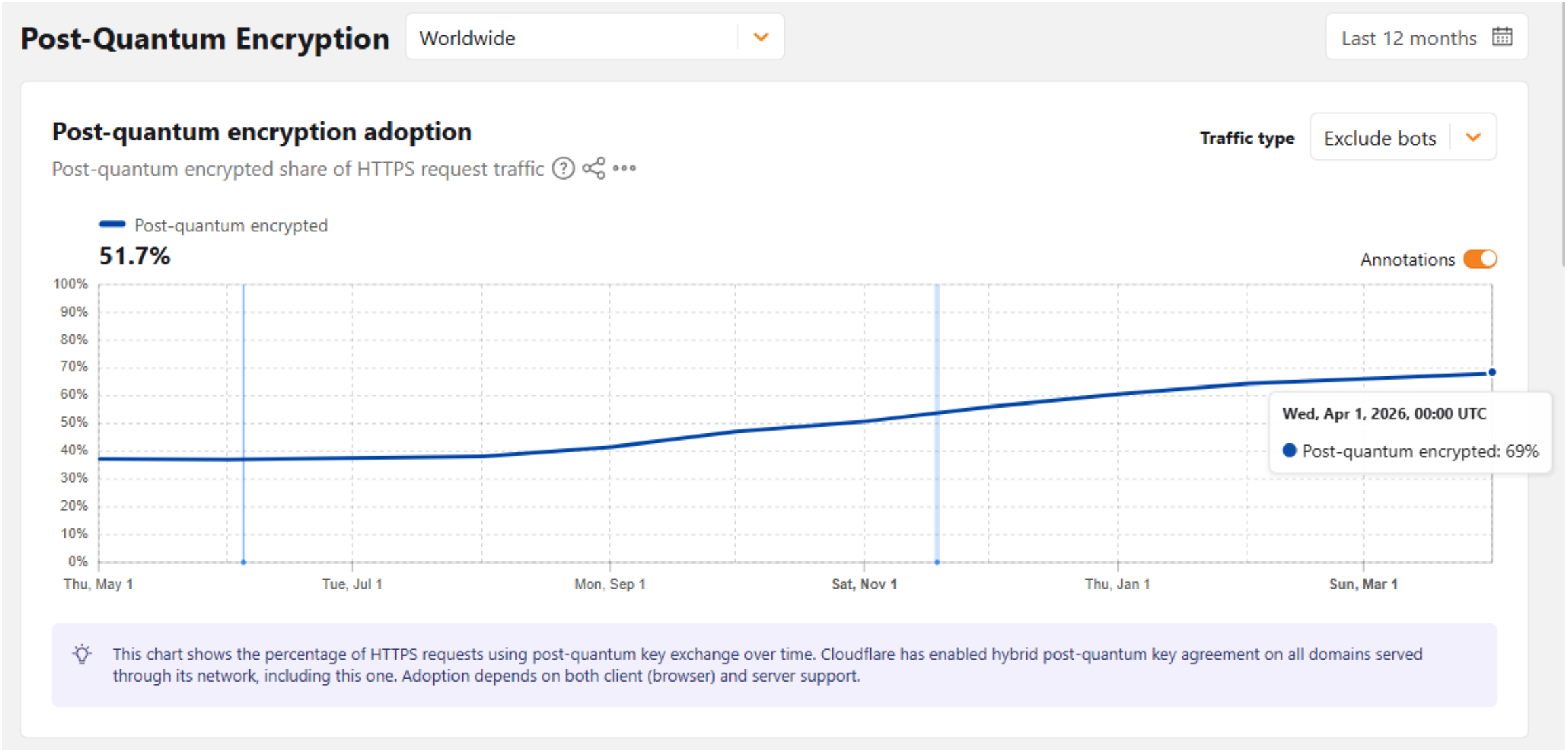
Migrating key agreement to quantum-safe cryptography is more urgent than authentication

Quantum-Safe Key Exchange in SAP S/4HANA



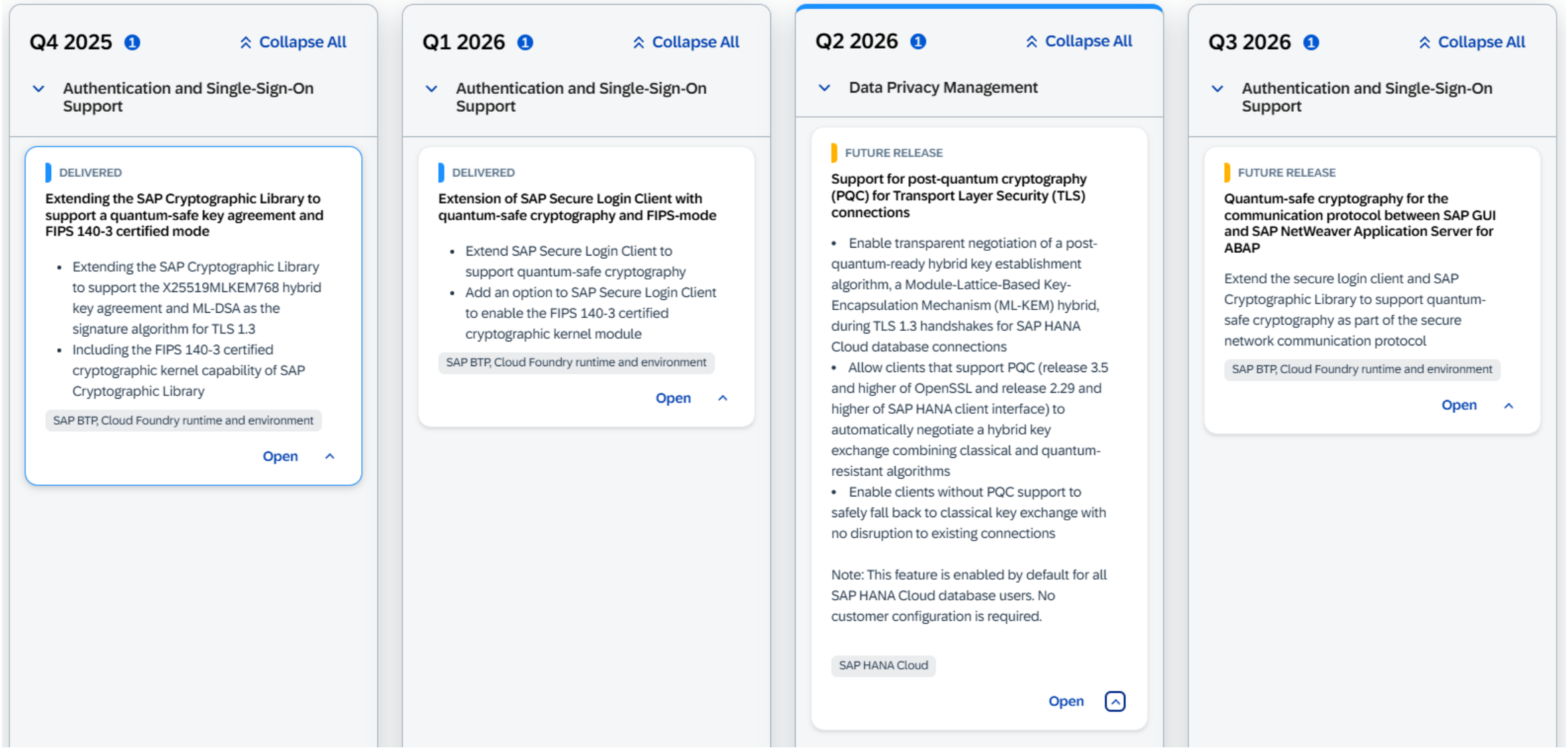
Prerequisites: TLS 1.3 & SAP Cryptographic Library 8.6 and better

Adoption of quantum-safe key agreement: X25519MLKEM768



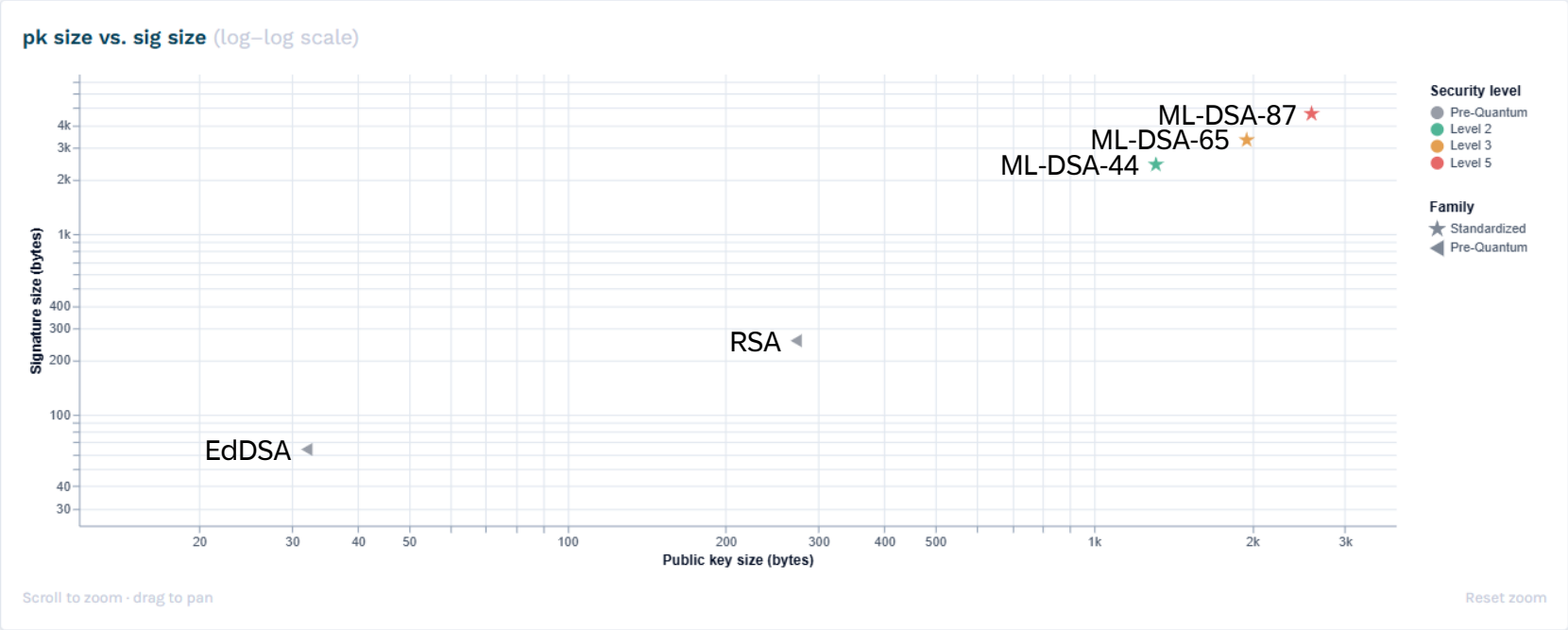
https://radar.cloudflare.com/adoption-and-usage

Related Roadmap Items



https://roadmaps.sap.com/board?range=FIRST-LAST&q=quantum-safe#Q4%202025

Post-Quantum Signature Schemes



Performance note: Timings are taken from the scheme submissions and may not reflect optimised implementations. Cycle counts marked with a wavy underline are extrapolated from reported millisecond timings assuming a 2.5 GHz processor — comparisons across such values should be treated with caution.

Scheme ▲	Category	Status	Parameter Set	Level	pk (B)	sig (B)	pk+sig (B)	Sign	Verify	Assumption
EdDSA	Pre-Quantum	Classic	Ed25519	Pre-Quantum	32	64	96	42K	130K	Elliptic Curves
ML-DSA	Lattices	FIPS	ML-DSA-87	5	2,592	4,627	7,219	642K	280K	MLWE/MSIS
ML-DSA	Lattices	FIPS	ML-DSA-65	3	1,952	3,309	5,261	529K	179K	MLWE/MSIS
ML-DSA	Lattices	FIPS	ML-DSA-44	2	1,312	2,420	3,732	333K	118K	MLWE/MSIS
RSA	Pre-Quantum	Classic	2048	Pre-Quantum	272	256	528	27.0M	45K	Factoring

5 parameter sets

Built by Thom Wiggers / PQShield. https://pqshield.github.io/nist-sigs-zoo/?s=EdDSA%2CML-DSA%2CRSA

Crypto Agility

Crypto Agility is a Prerequisite

What is Crypto Agility

Applications built with Crypto Agility in mind allow you to replace cryptographic capabilities without the need to modify or refactor other parts of the application.

Examples

- Introducing **new protocols** such as TLS 1.3
- **Replacing insecure algorithms** (SHA-1, 3DES, DSA,..) or key lengths with better alternatives (SHA-2, AES, ECDSA,..)
- Protecting applications against attacks based on quantum computers by **replacing classic cryptographic capabilities** with post-quantum cryptography

Crypto Agility is a Prerequisite

Steps towards Crypto Agility

- Have an up-to-date inventory of cryptographic implementations and artifacts across all relevant systems.
- Rely on cryptographic components that have a proven track record of fast delivery for new cryptographic algorithms.
- Integrate cryptographic components with clearly defined, minimal dependencies to application coding.
- Automate the update process as much as possible.

Crypto Agility Drivers

Technological development

- Migration to quantum-safe cryptographic algorithms
- Weaknesses in algorithms discovered
- Standardization

Compliance

- Sector-specific: business with US Federal Agencies requires using FIPS 140-3 validated crypto modules by October 2026
- Country/region-specific
- Export control restrictions

Summary

- Quantum computers exist today
- While they are not yet cryptographically relevant, progress towards these kinds of machines is made rapidly
- A cryptographically relevant quantum computer can weaken or even defeat many of today's cryptographic algorithms
- New cryptographic algorithms are available that are believed to be immune to quantum computer-based attacks
- Migration needs to start now, due to the duration of the migration project and the harvest-now-decrypt-later attacks
- We need to be crypto-agile to handle future attacks quickly
- TLS 1.3 is a prerequisite for quantum-safe cryptography

Additional Resources

References

- Quantum Computation and Quantum Information by Michael A. Nielsen & Isaac L. Chuang
- Introduction to Quantum Information Science by Scott Aaronson
- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer by Peter Shor
- Introduction to lattice-based post-quantum cryptography
- New version 8.6 of the SAP Cryptographic Library with quantum-safe cryptography and FIPS 140-3 mode

Notes

- 1848999 - Central Note for CommonCryptoLib 8 (SAPCRYPTOLIB)
- 2004653 - CommonCryptoLib 8 cryptographic algorithms
- 3559399 - How to use the FIPS 140-3 certified SAP CommonCryptoLib Crypto Kernel
- 2180024 - HANA & ABAP: Option to Enable/Disable FIPS 140-3 certified SAP CommonCryptoLib Crypto Kernel
- 3318423 - Is TLS 1.3 Supported by SAP Kernel for ABAP and SAP S/4HANA?
- IBM–SAP Collaboration Delivers the First Quantum-Safe SAP CommonCryptoLib

Additional Resources

Influence Request

- Development Request for ACME-based Certificate Renewal Solution for Systems in SAP Private Cloud

Thank you.

Contact information:

Christian Cohrs (christian.cohrs@sap.com)

SAP Bring out your best.