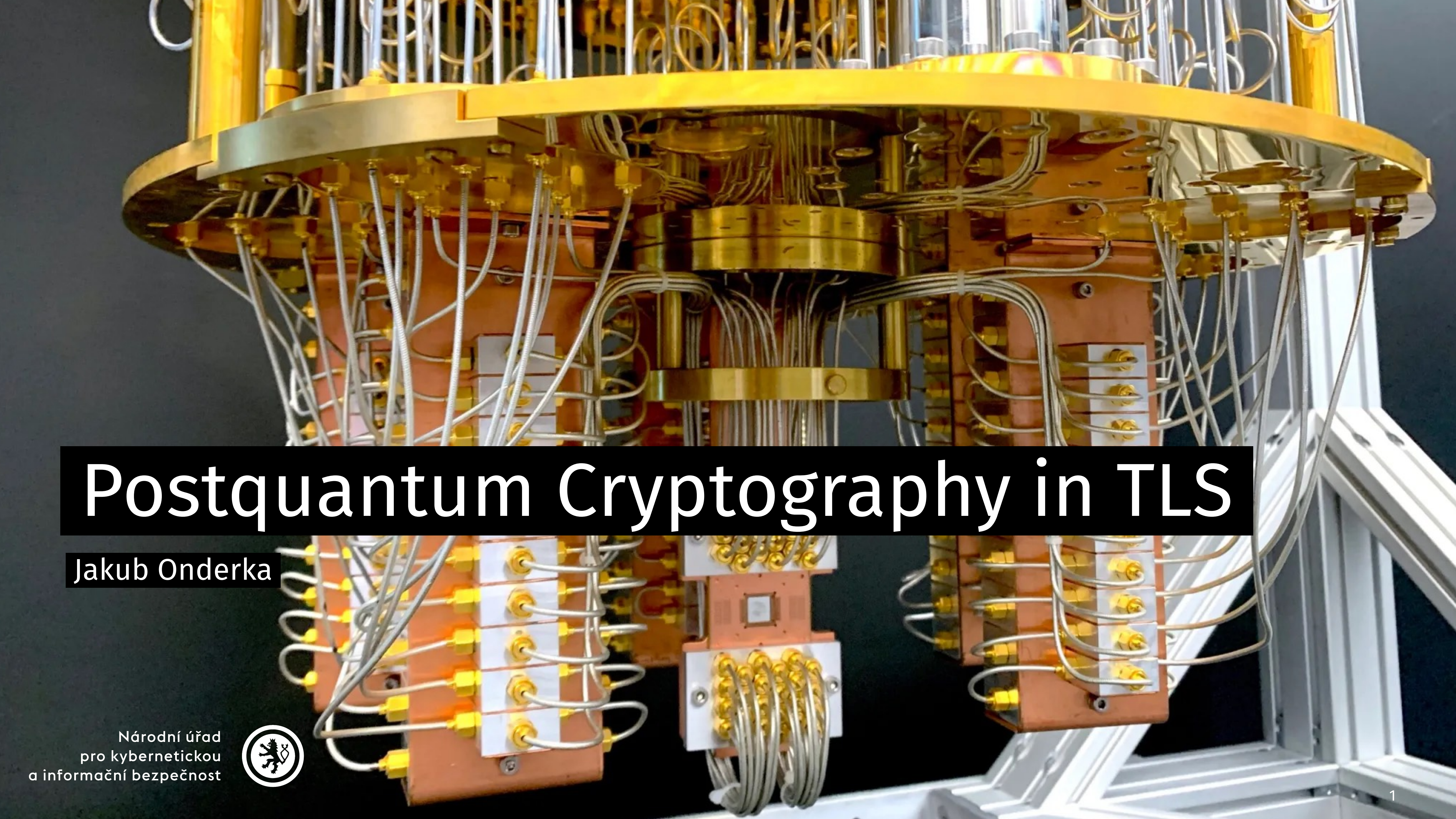


Postquantum Cryptography in TLS

Jakub Onderka

Národní úřad
pro kybernetickou
a informační bezpečnost

Jakub Onderka

Security analyst, GovCERT.CZ, NÚKIB

E-mail: jakub.onderka@nukib.gov.cz
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD
LinkedIn: https://www.linkedin.com/in/jakubonderka/

TLP:CLEAR

NÚKIB
National Cyber and Information Security Agency

GovCERT.CZ
Government Computer Emergency Response Team

TLP:CLEAR

Who are we? And what we do?

- Czech authority for information security (confidential, secret and top secret informations) and cybersecurity, based in Brno

- Securing confidential information in information systems
- Satellite systems security
- Cyber security ("NIS2")
  - Compliance
  - Regulation
  - GovCERT.CZ

TLP:CLEAR

I am developer (Rust+Python), not crypto expert

Why we need postquantum cryptography?

CIA triade

TLP:CLEAR

Classical symmetric and asymmetric algos

Symmetric

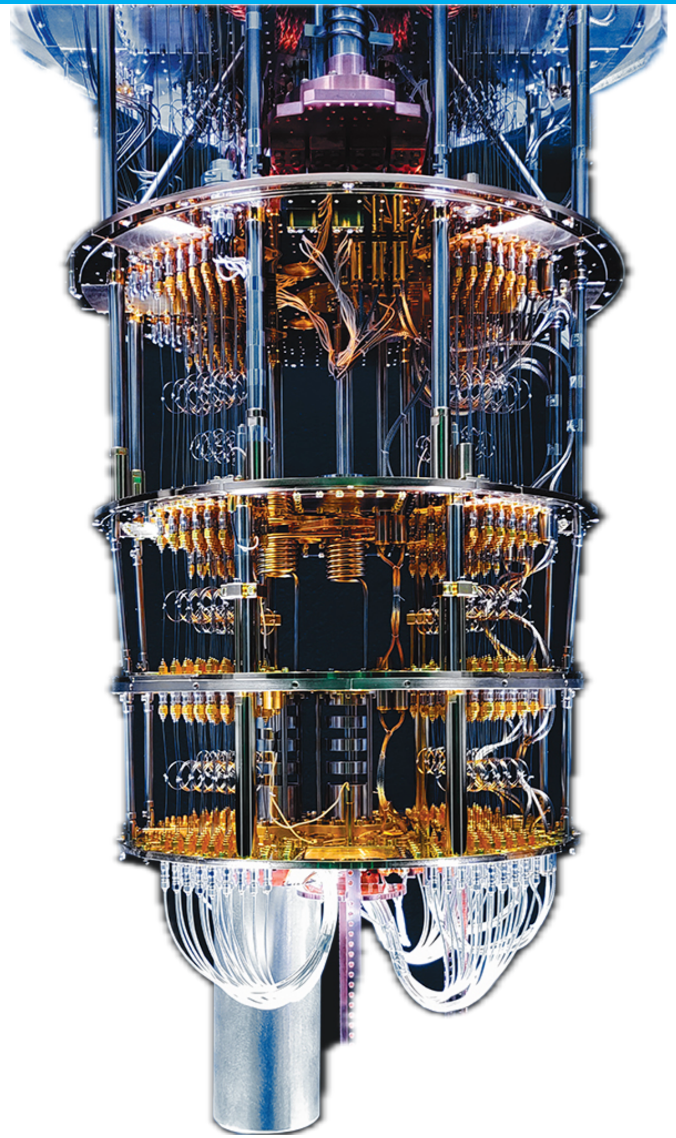
- AES
- ChaCha20

Asymmetric

- DSA
- RSA
- EC-DSA
- ECDH

Quantum computers

- Currently, only "quantum calculators" with around 200 qubits are available
  - The first Czech quantum computer, VLQ, based in Ostrava, operates with 24 qubits
- Cryptographically relevant quantum computer (CRQC)
  - quantum computer that can break classical cryptography algorithms
  - it needs at least 4 000 qubits (20x more that we have to now)
- When we will have them?
  - we don’t know, maybe there are already here, maybe never
  - **estimate: not before 2031, with a 50% chance**



TLP:CLEAR

Classical symmetric and asymmetric algos

Symmetric

- AES
- ChaCha20

✅

raise key size to 256 bits

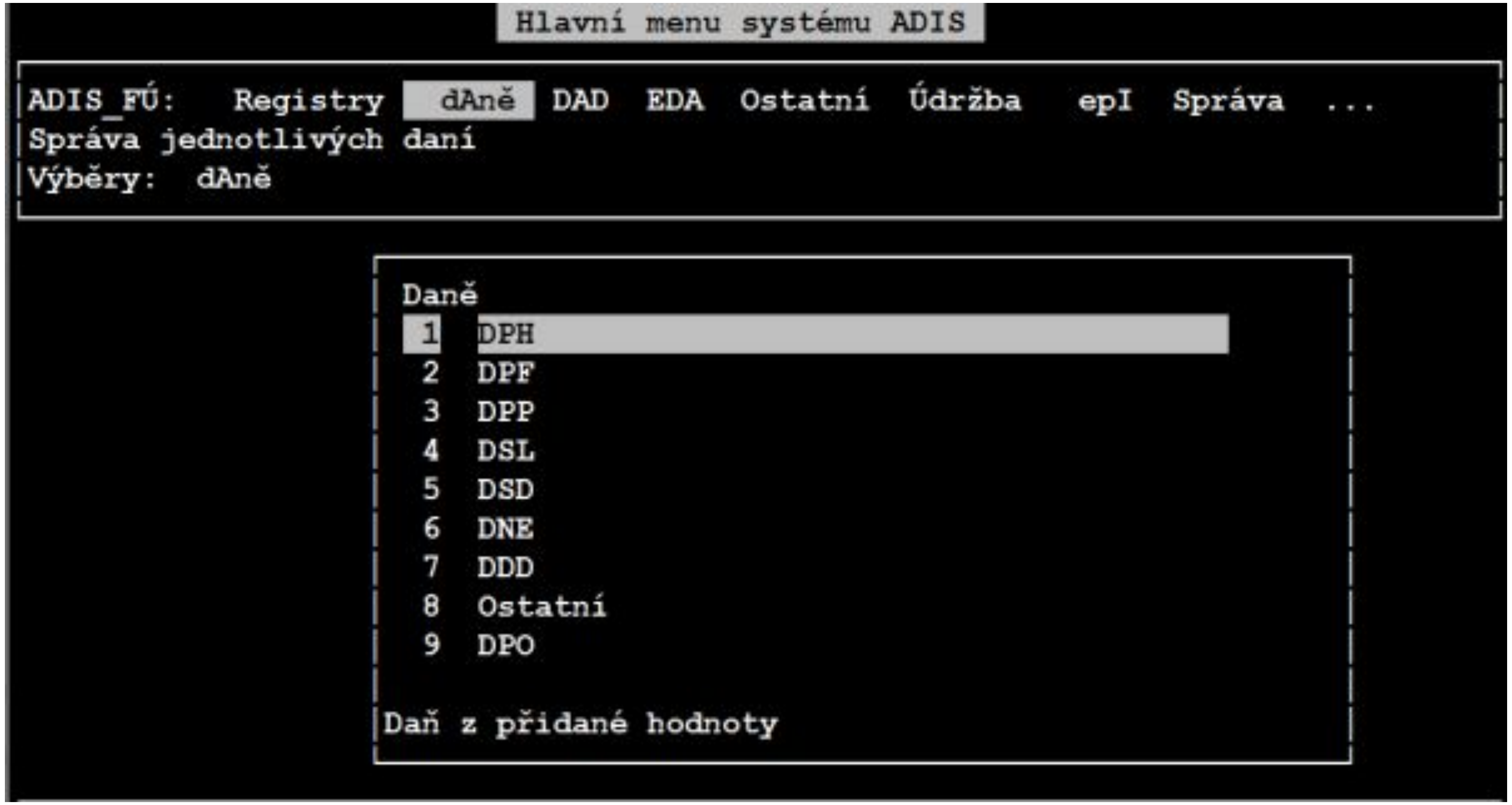
Asymmetric

- DSA
- RSA
- EC-DSA
- ECDH

❌

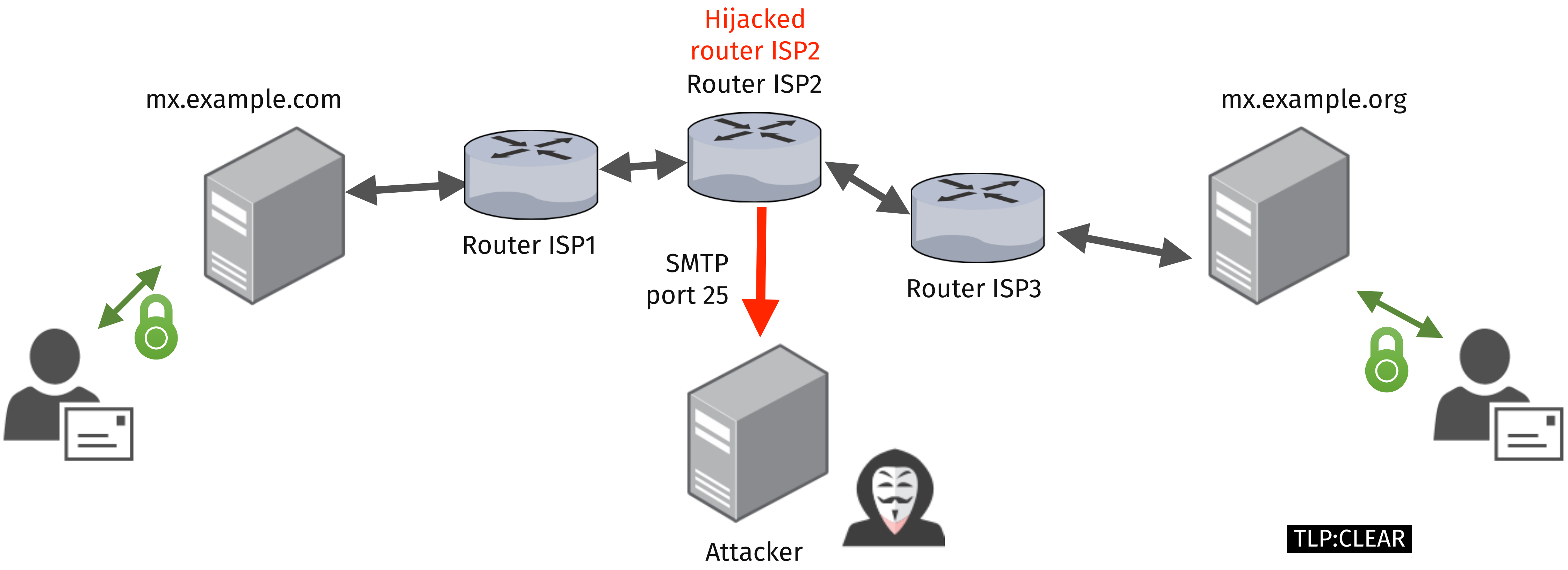
Why we have to solve it now

- Legacy IT systems
  - lifespan of IT system is usually 5-7 years, but sometimes even decades
  - backward compatibility



„Harvest now, decrypt later”

- An attacker can now harvest encrypted data and decrypt it after a cryptographically relevant quantum computer (CRQC) becomes available.
- Typical „secret” has lifespan 5 years (2031 - 5 = 2026)



TLP:CLEAR

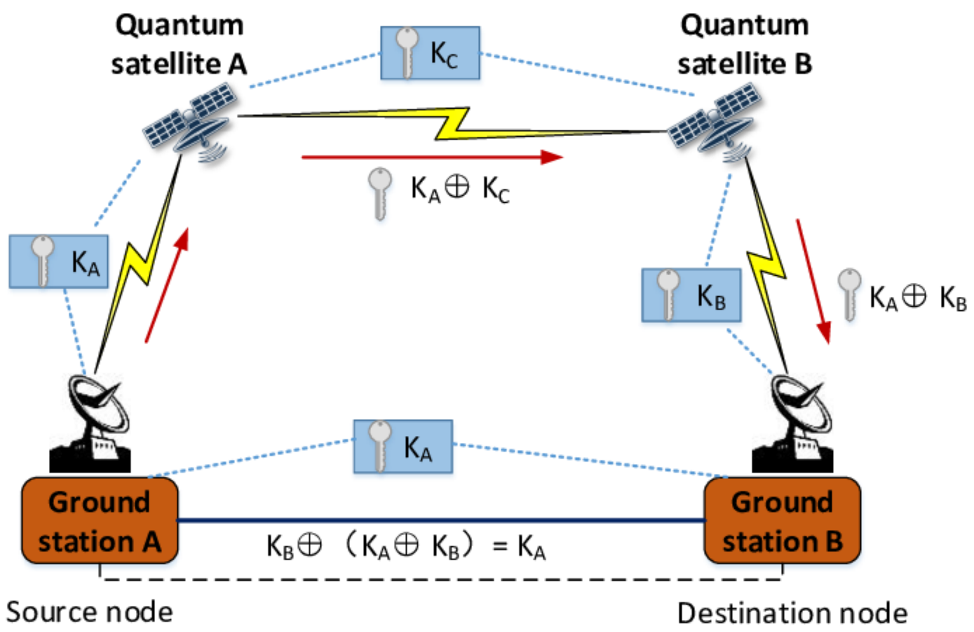
TLS protocol

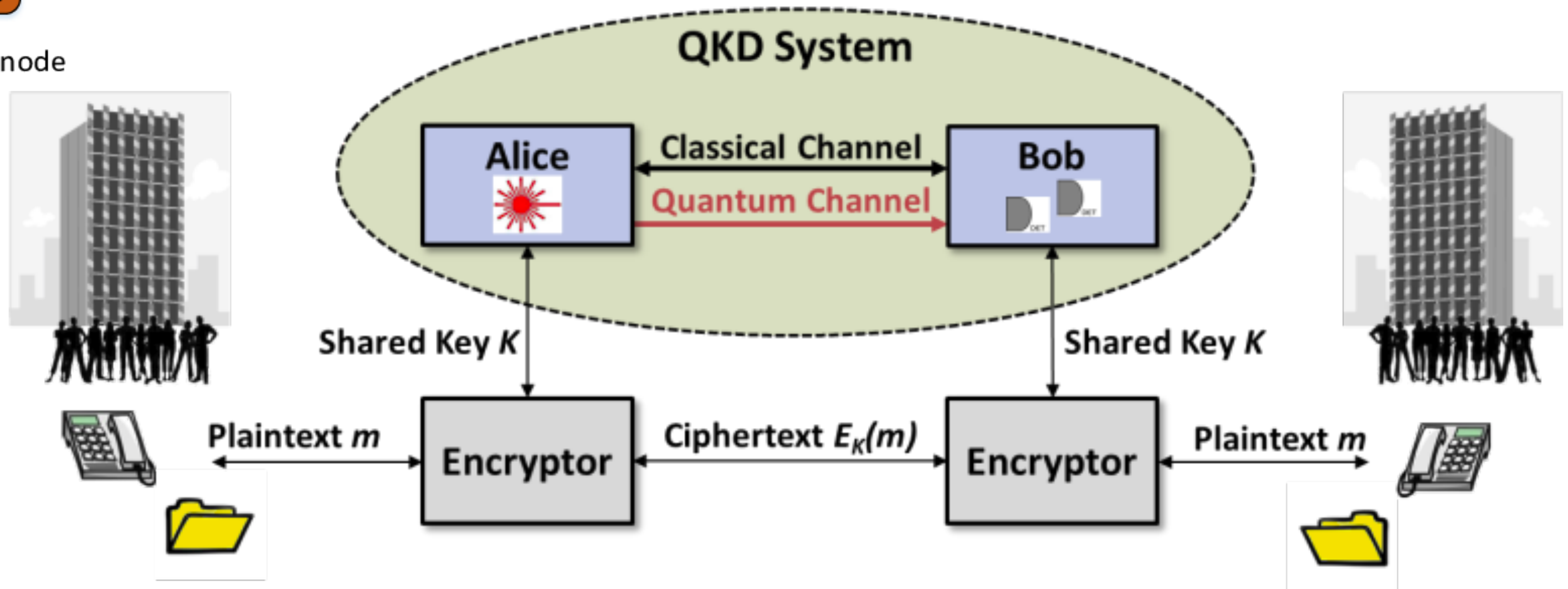
- Most common protocol for secure communication

- It uses cryptography for three things:
  - check server identity (certificate) ⚠️
  - key agreement ❌
  - symmetric encryption ✅

How we can protect our communication

Quantum key distribution – QKD





Postquantum cryptography

Národní úřad
pro kybernetickou
a informační bezpečnost

- NIST competition, first winner was algo for key exchange
- In competition with name CRYSTALS-Kyber
- Standardized as ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)

NIST
National Institute of Standards and Technology

KYBER


Check for updates

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

Hybrid approach

- Cryptologists still don't fully trust new post-quantum algorithms
  - SIKE cracked in 62 minutes on one CPU

- A hybrid approach is being promoted – a combination of classical and post-quantum algorithms

☹️ higher latency when establishing a connection (because of key size)
☹️ computational complexity
🤩 higher security – both algorithms must be broken to break the communication

Hybrid approach in TLS

~~X25519Kyber768Draft00~~

↓

X25519MLKEM768

RFC: draft-ietf-tls-ecdhe-mlkem-01

Hybrid approach in TLS

Key exchange algorithm	PQ	Key size (in bytes)		Ops/sec (more is better)	
		Client	**Server**	**Client**	**Server**
X25519	❌	32	32	17 000	17 000
MLKEM768	✅	1 184	1 088	31 000	70 000
X25519MLKEM768	✅	1 216	1 120	11 000	14 000

Source: Cloudflare

Current state of X25519MLKEM768 in TLS

Current support – web browsers

✅ Google Chrome since version 131

✅ Firefox since version 132

✅ Safari on macOS 26 or iOS 26 (released last month)

- All major web browsers in latest versions already supports

Current support – TLS libraries

✅ BoringSSL

✅ AWS-LC

✅ oqsprovider – Open Quantum Safe provider for OpenSSL (3.x) – extension for OpenSSL 3.x

✅ Go language standard library since 1.24

✅ 🎉 OpenSSL 3.5 (released April 2025)

Current support – operating systems

✅ macOS 26, iOS 26, iPadOS 26 (released last month)

✅ Alpine 3.22 (May 2025)

✅ Debian Trixie (September 2025)

?? RHEL 10 a derivates, it should be included also in RHEL 9.7

not enable by default, it is necessary to turn it on manually

❌ Windows 11 should support PQC with update that will be released this year

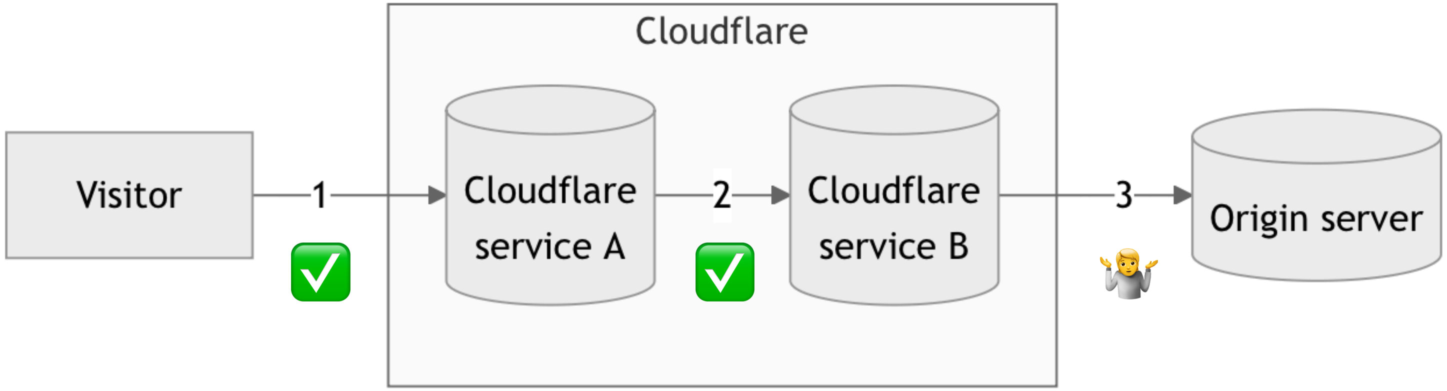
Current support – web apps

✅ Google (also SMTPS for Gmail)

✅ Cloudflare

✅ Portál NÚKIB (August 2024, our reporting platform for NIS2 directive)

- 28 % of domain from list of 100 thousands most visited domains
  - but 27 % from them because of Cloudflare (data from March 2025)



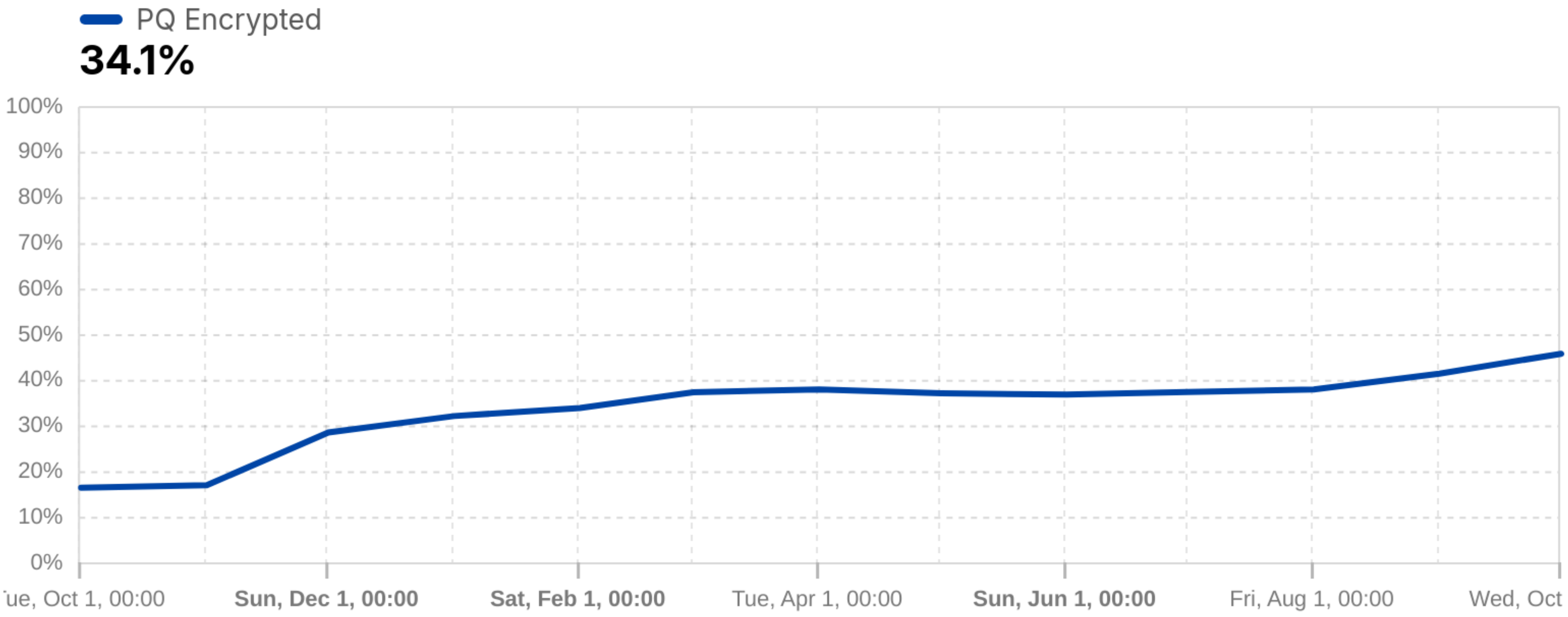
Source: https://www.netmeister.org/blog/pqc-use-2025-03.html

TLP:CLEAR

HTTPS communication protected by PQC

Post-quantum encryption adoption worldwide

Post-Quantum encrypted share of human HTTPS request traffic



Cloudflare Radar

Last 12 months | Oct 5, 2025, 07:00 UTC

It is not just about TLS…

SSH

- sntrup761x25519-sha512 since OpenSSH 9.0
- mlkem768x25519-sha256 since OpenSSH 9.9
- Warning when using non-PQC key exchange algo since OpenSSH 10.1 (released this week)

```
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
```

Signal

Národní úřad
pro kybernetickou
a informační bezpečnost

Signal

The PQXDH Key Agreement Protocol

Revision 3, 2023-05-24, Last Updated: 2024-01-23 [PDF]

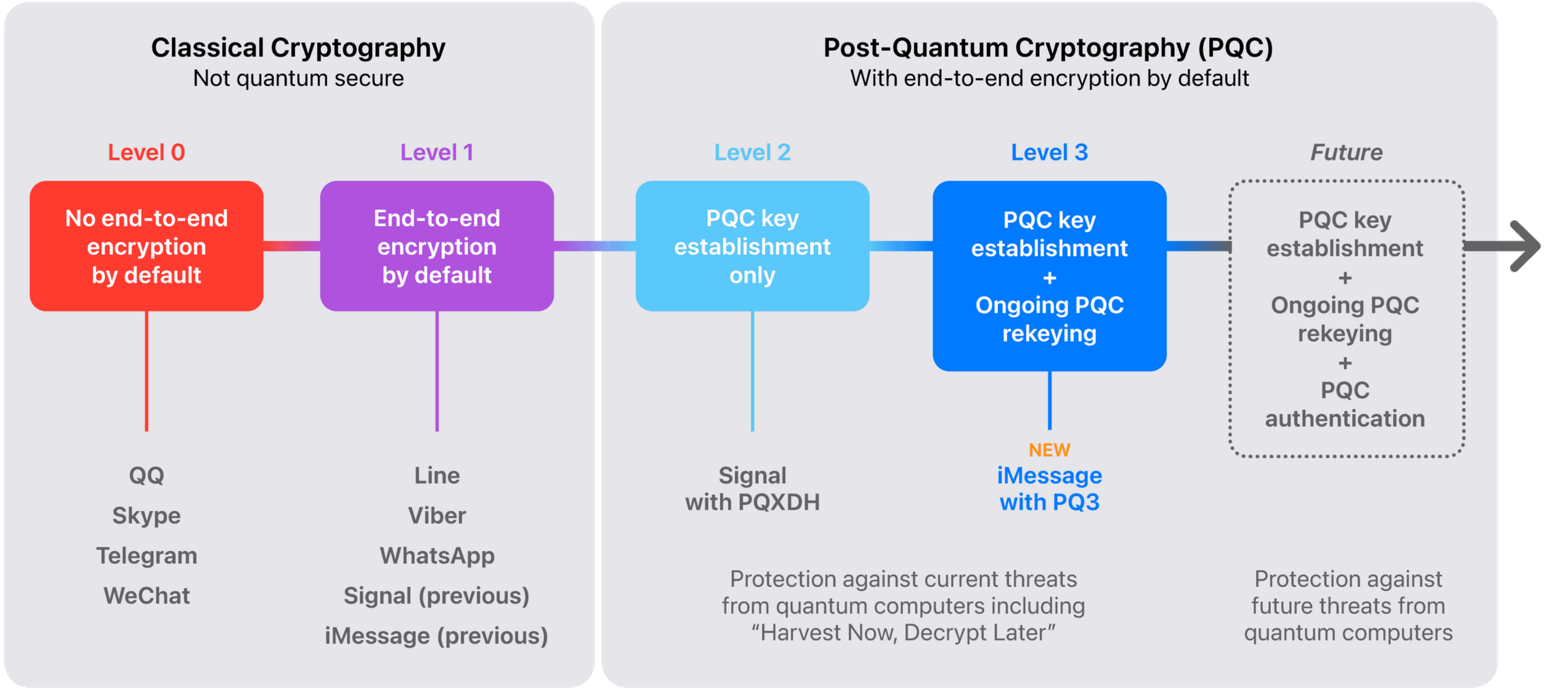
Ehren Kret, Rolfe Schmidt

Table of Contents

Apple iMessages

„Support for PQ3 will start to roll out with the public releases of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4"

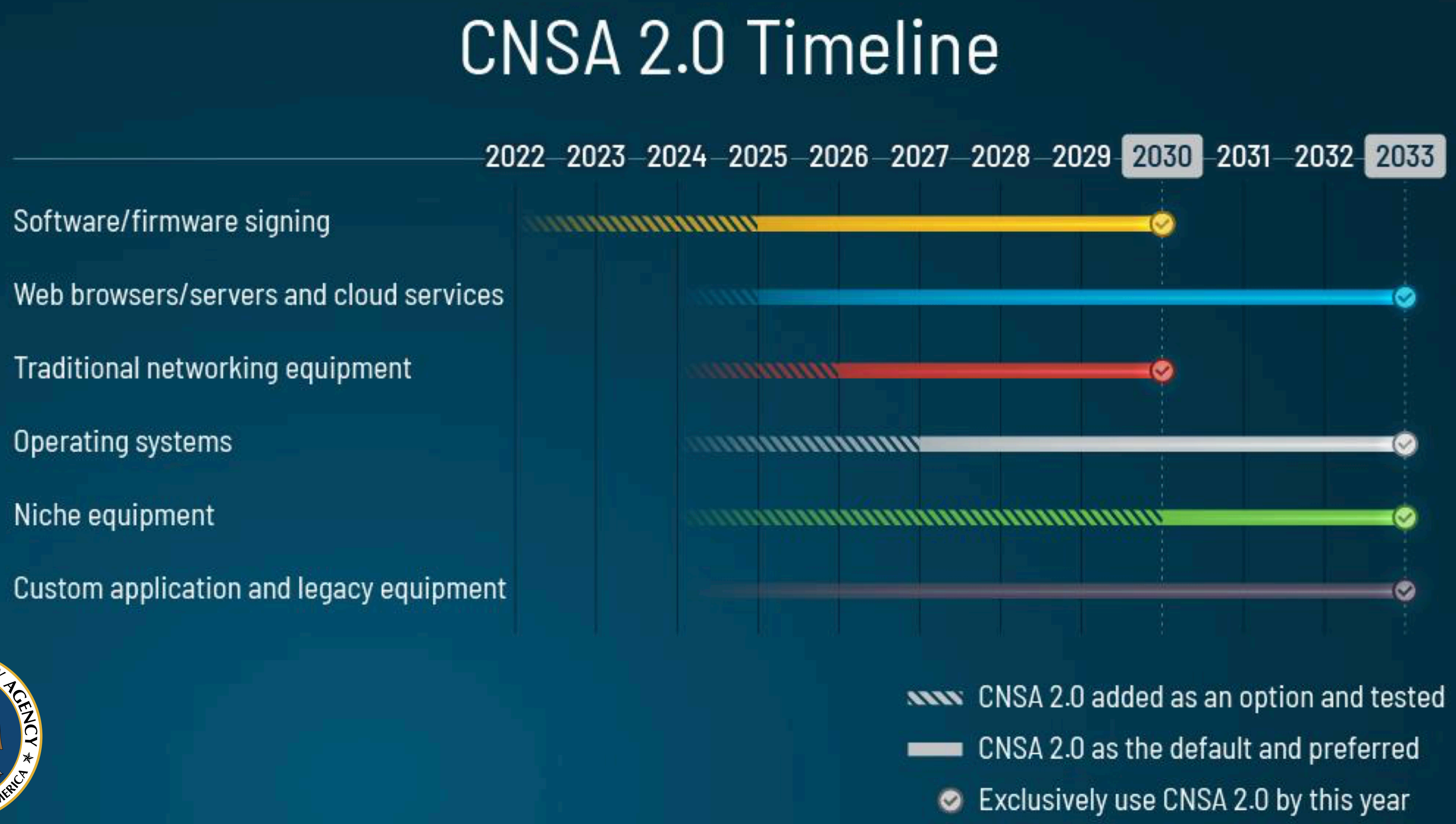
Quantum-Secure Cryptography in Messaging Apps



Note: This comparison evaluates only the cryptographic aspect of messaging security, and therefore focuses on end-to-end encryption and quantum security. Such a comparison doesn't include automatic key verification, which we believe is a critical protection for modern messaging apps. As of the time of this writing, only iMessage and WhatsApp provide automatic key verification. The iMessage implementation, called Contact Key Verification, is the state of the art – it provides the broadest automatic protections and applies across all of a user's devices.

When we have to switch to PQC only?

NSA post quantum timeline



NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

Národní úřad
pro kybernetickou
a informační bezpečnost

POLICY AND LEGISLATION | Publication 23 June 2025

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC).

Quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. This threat can be countered by a timely, comprehensive and coordinated transition to Post-Quantum Cryptography (PCQ).

Therefore, on 11 April 2024, the Commission has published a Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. For the development of this Roadmap, the Commission recommended to establish a work stream on PQC with the NIS Cooperation Group. This document is the first deliverable and is meant to be a first high-level paper aimed at Member States. It includes a set of recommendations that Member States need to implement for a synchronised transition to PQC, as well as measures to ensure that all stakeholders are well informed on the quantum threat to cryptography.

AdobeStock © ipopba

Downloads

Roadmap for the Transition to Post-Quantum Cryptography — Download

Related topics

Cybersecurity | Advanced and Cloud Computing | Quantum

TLP:CLEAR

EU roadmap

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

NÚKIB approach

TLP:CLEAR

NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení v oblasti kryptografické bezpečnosti

Verze 4.0, platná ke dni 5. 2. 2025

TLP:CLEAR

Source: https://nukib.gov.cz/download/uredni_deska/Minimalni_pozadavky_v4_FINAL.pdf

4 Kvantově odolné asymetrické algoritmy (postkvantová kryptografie)

Přechod k náhradě kvantově zranitelné kryptografie bude mimořádně náročný. Proto doporučujeme se seznámit s podrobnějšími vysvětleními a doporučeními uvedenými v příloze „Kvantová hrozba a kvantově odolná kryptografie“.

a) Samostatný postkvantový algoritmus pro ustanovení klíčů

1. ML-KEM-1024

ML-KEM-1024 je standardizovaná verze algoritmu Kyber-1024 (též označovaného jako CRYSTALS-Kyber úrovně 5). Pro samostatné použití je nutná implementace dle standardu NIST (FIPS 203)[5].

b) Hybridní kvantově odolná kryptografie pro ustanovení klíčů

Kombinuje jeden z následujících postkvantových algoritmů KEM/Encryption:

1. ML-KEM-1024/Kyber-1024, ML-KEM-768/Kyber-768
2. FrodoKEM-1344, FrodoKEM-976
3. mceliece8192128, mceliece6688128, mceliece460896, mceliece8192128f, mceliece6688128f, mceliece460896f

s některým z klasických algoritmů pro ustanovení klíčů z kapitoly 3 písm. b), a to takovým způsobem, že bezpečnost hybridní kombinace zůstane zachována i v případě, kdy bude jedna z jejích složek prolomena.

Doporučení: V hybridní kombinaci je možné použít jak standardizovaný algoritmus ML-KEM, tak původní algoritmus Kyber. Nicméně doporučujeme preferovat ML-KEM a do budoucna předpokládáme schválení pouze této standardizované verze.

Portal NUKIB

Národní úřad
pro kybernetickou
a informační bezpečnost

PORTÁL
NÚKIB

I want to settle it. | Cybersecurity Act | NIS2 | Information service | IN | Log

Incident reporting

Incident Information - Malware

Incident description *

Date and time of incident occurrence

YYYY-MM-DD | hh:mm

Date and time of incident detection

YYYY-MM-DD | hh:mm

What is the current status? *

Select an option

Do you need help with analysis? *

Select an option

What is the value of the assets being attacked?

Select an option

What is the impact of the incident?

Select an option

Malicious code description

In which network segments was the malware found?

- [ ] DMZ (demilitarized zone)
- [ ] office network
- [ ] network with critical systems
- [ ] other

Basic information
Who reports?
Reporter
Incident type
Incident details
Contact information
Form generation

Why we implemented PQC in Portal NUKIB

- Higher probability of attack by a state actor
- Gaining experience implementing post-quantum cryptography in real world usage
- Postquantum promotion

- It was also a bonus when we switched from OpenSSL to BoringSSL
  - At the time, OpenSSL didn't support QUIC (HTTP3)

Our experience

- No report from our users
- No real slowdown
- No increase in CPU usage

- Only problem: maintenance of BoringSSL
  - We have to compile it ourselves
  - BoringSSL doesn’t have stable versions (you just compile latest commit)
  - Probably in future, we will switch back to OpenSSL

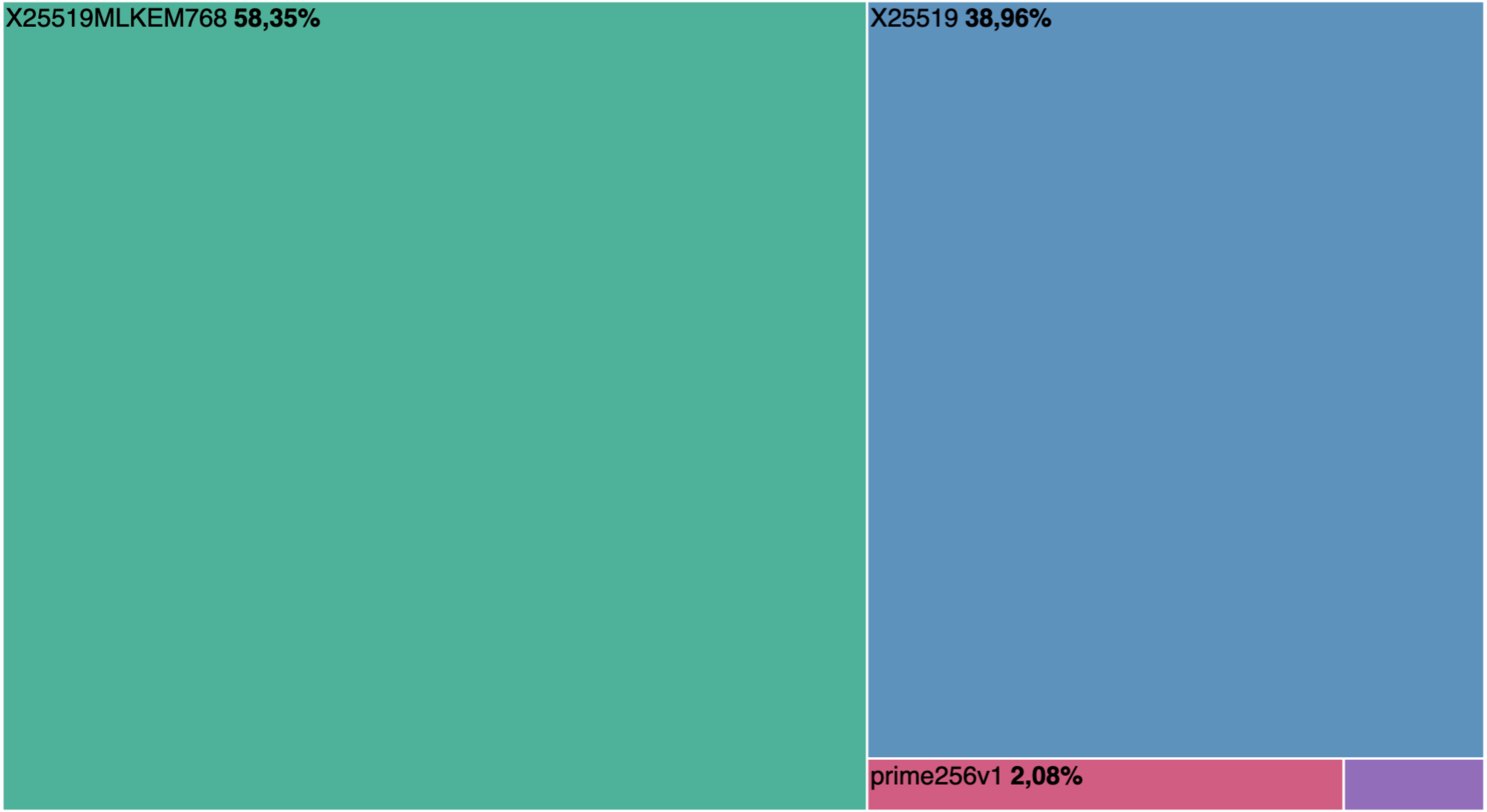
BoringSSL

BoringSSL is a fork of OpenSSL that is designed to meet Google's needs.

Although BoringSSL is an open source project, it is not intended for general use, as OpenSSL is. We don't recommend that third parties depend upon it. Doing so is likely to be frustrating because there are no guarantees of API or ABI stability.

Adoption rate – public part

Národní úřad
pro kybernetickou
a informační bezpečnost



TLP:CLEAR

Adoption rate – internal part

It is time for PQC

- **2025 is the year of implementation of support for post-quantum key agreements**

- It is possible that the implementation of PQC will be mandatory for systems regulated under the Cybersecurity Act (NIS2)
- And it is likely that browsers will force the implementation of PQC much earlier
- It is necessary to prepare now, otherwise the implementation costs will be higher

- Post-quantum certificates are not yet solved, but we still have time

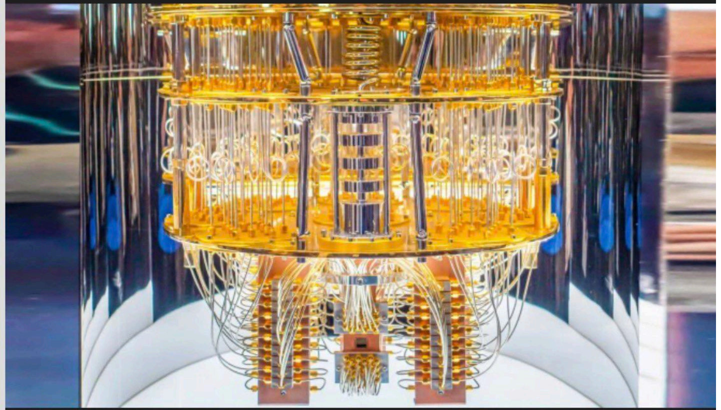
How to prepare

- **As a software or hardware developer**
  - Prepare your products to support post-quantum key agreement now
- **As an application and systems administrator**
  - Buy just products that already supports PQC or at least ask vendors when they plan to implement PQC support
  - When purchasing new systems and require so-called “cryptographic agility”
- **As a security manager**
  - Map out which systems will need to implement post-quantum cryptography as a priority

PQC in TLS: how to deploy everything you need today

ROOT.CZ_

Postkvantová kryptografie v protokolu TLS: jak nasadit vše potřebné už dnes



Kvantové počítače sice ještě neumějí lámat šifrovací algoritmy používané v TLS, ale komunita se na tento moment připravuje už dnes. Článek vysvětlí, proč již dnes a jak zavádět kvantově odolné kryptografické algoritmy.

JAKUB ONDERKA | Dnes Doba čtení: **21 minut**

https://www.root.cz/clanky/postkvantova-kryptografie-v-protokolu-tls-jak-nasadit-vse-potrebne-uz-dnes/

Post-quantum cryptography is not a problem of the distant future but a real issue that needs to be addressed **today**.

Questions?

E-mail: jakub.onderka@nukib.gov.cz
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD
LinkedIn: https://www.linkedin.com/in/jakubonderka/