Quantensichere Kryptographie - der Weg zur langfristigen Sicherheit

FORUM 3-B | TUTORIAL

20. Januar 2025, Dr.-Ing. Tobias Fehenberger, Daniel Herzinger, Richard Zink

AGENDA

1. Warum brauchen wir quantensichere Kryptographie?
2. Handlungsempfehlungen
3. One Last Thing: Quantenschlüsselaustausch

POST-PRESENTATION SUMMARY

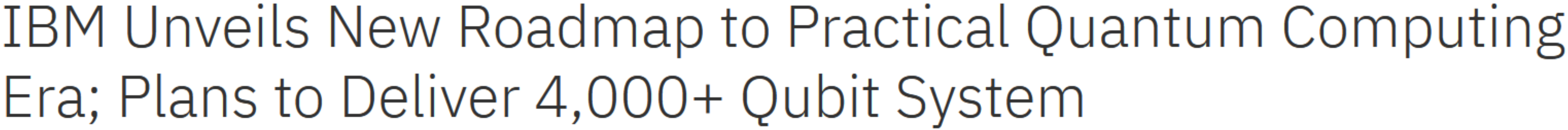
Current state of the art cryptography

- **RSA, Diffie-Hellman (DH) in finite fields, or elliptic-curve Diffie-Hellman (ECDH)** are currently used cryptography (you will find this everywhere)
- RSA, NIST P256, ECDSA are older standards
- Internet is moving over to Curve25519 and Ed25519 (faster, smaller, well analyzed security)
- In symmetric cryptography use AES and some MAC (AES-GCM), ChaCha20-Poly1305 or Ascon-AEAD128

Google claims its quantum computer can do the impossible in 200 seconds

By Charles Riley, CNN Business

Updated 1306 GMT (2106 HKT) October 23, 2019



IBM Unveils New Roadmap to Practical Quantum Computing Era; Plans to Deliver 4,000+ Qubit System

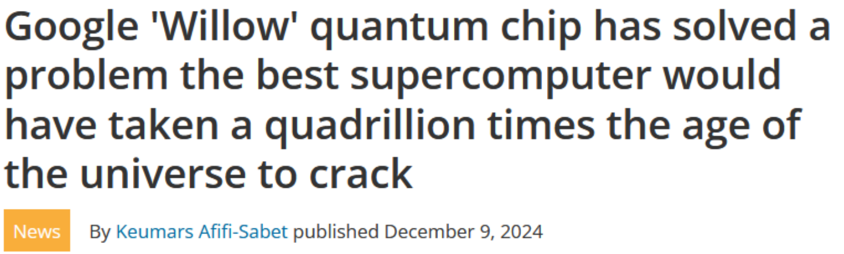
Google Announces a 72 Qubit Superconducting Quantum Chip

IBM Just Announced a 50-Qubit Quantum Computer

This is the most sophisticated quantum computer ever.

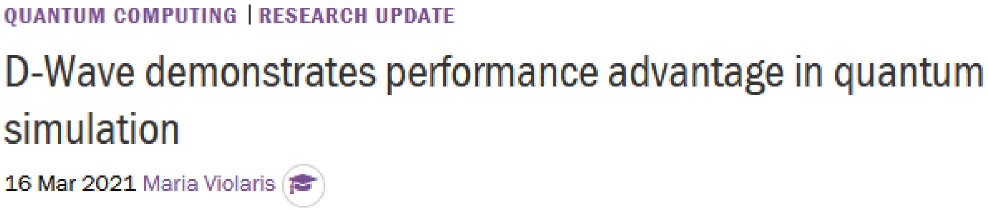
OpenSuperQ | A quantum computer based on superconducting integrated circuits

The OpenSuperQ project aims to enable European citizens to be able to use the final machine and learn about quantum computer programming in a guided way.



Google 'Willow' quantum chip has solved a problem the best supercomputer would have taken a quadrillion times the age of the universe to crack

News By Keumars Afifi-Sabet published December 9, 2024



QUANTUM COMPUTING | RESEARCH UPDATE

D-Wave demonstrates performance advantage in quantum simulation

16 Mar 2021 Maria Violaris

Why we need quantum-safe cryptography?

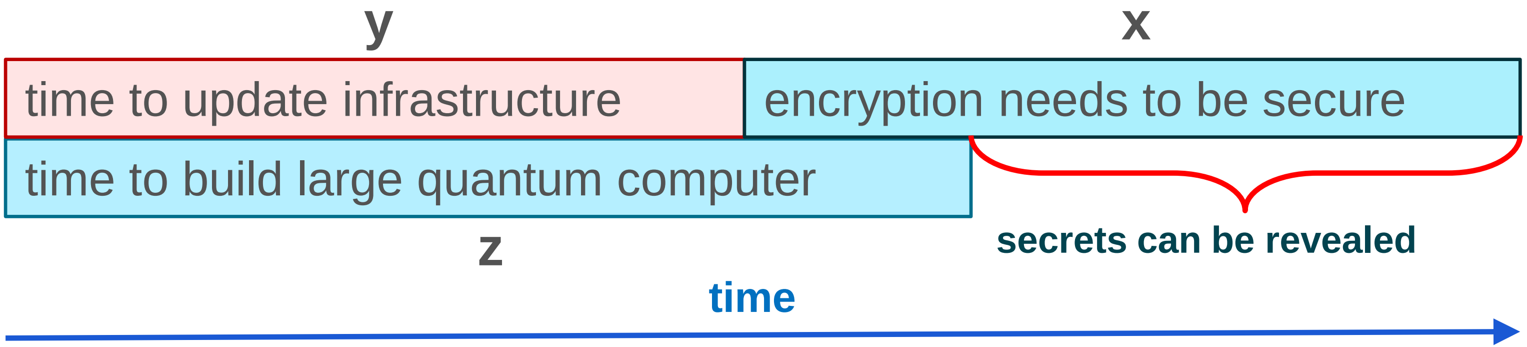
- Shor's (quantum) algorithm:
  - Solves the following problems in polynomial time: (this is bad)
    - Integer factorization (15 = 3 * 5) (**RSA is broken**)
    - The discrete-logarithm problem in finite fields ($g^x \; mod \; p = y$) (**DH + DSA is broken**)
    - The discrete-logarithm problem on elliptic curves ($y^2 = x^3 + ax + b$) (**ECDHE + ECDSA is broken**)

- Grover's (quantum) algorithm:
  - Speeds up brute-force searches:
    - Only 2^{64} quantum operations to break AES-128
    - Only 2^{128} quantum operations to break AES-256

2^{128} quantum operations are still very expensive but polynomial time is very bad

ESTIMATING Z

How soon do we need to worry?


y
x
time to update infrastructure
encryption needs to be secure
time to build large quantum computer
secrets can be revealed
z
time

If x + y > z, we have a serious problem today!

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

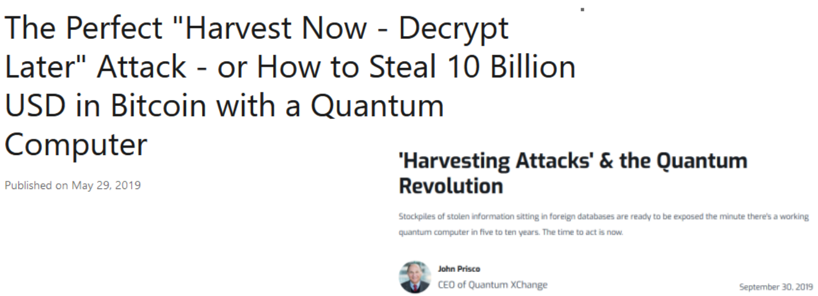
Likelihood of having a large quantum computer is 2/5 in 15 years! [1]

A NON-SPECIFIED ATTACKER (NSA) WITH BIG DATA CENTERS

How soon do we need to worry?

Store encrypted data ***now***

Decrypt ***later*** when large-scaled quantum computers are available.



The Perfect "Harvest Now - Decrypt Later" Attack - or How to Steal 10 Billion USD in Bitcoin with a Quantum Computer

Published on May 29, 2019

'Harvesting Attacks' & the Quantum Revolution

Stockpiles of stolen information sitting in foreign databases are ready to be exposed the minute there's a working quantum computer in five to ten years. The time to act is now.

John Prisco

CEO of Quantum XChange

September 30, 2019

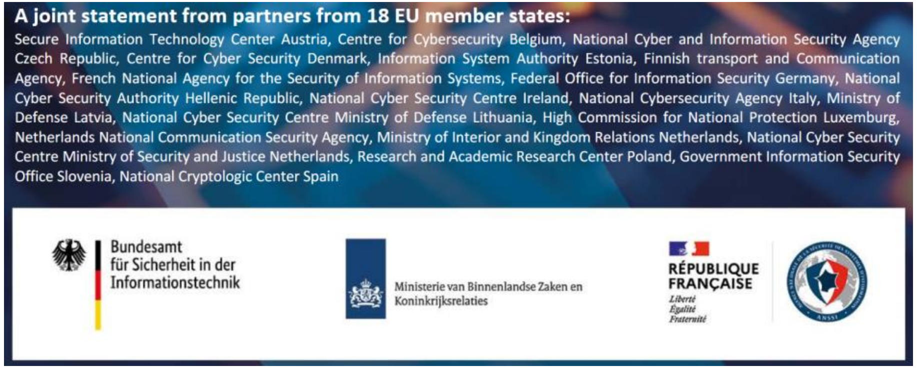
Utah data center [1]

[1] https://i.insider.com/51b20dd9eab8eaa874000001

Having quantum-safe encryption is essential **today**!

FROM A POST-QUANTUM PERSPECTIVE

2024



A joint statement from partners from 18 EU member states:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain

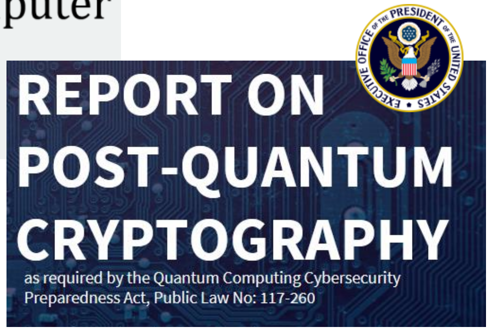
Bundesamt für Sicherheit in der Informationstechnik

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Status of quantum computer development

Entwicklungsstand Quantencomputer



REPORT ON POST-QUANTUM CRYPTOGRAPHY

as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Subcategory: Cryptography

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

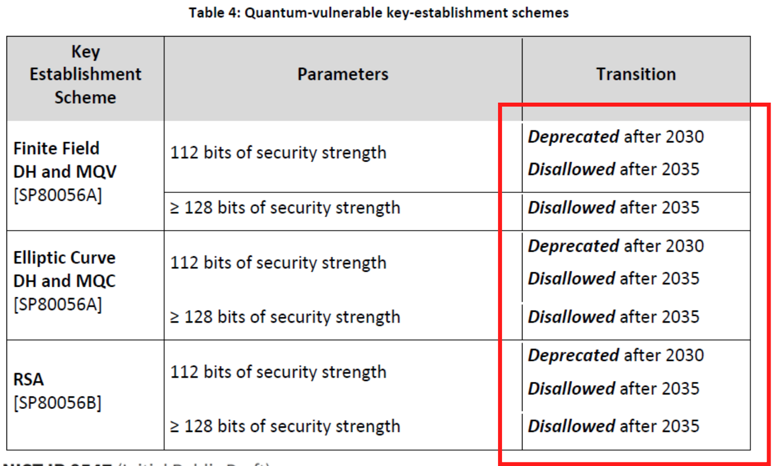


Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	*Deprecated* after 2030 *Disallowed* after 2035
	≥ 128 bits of security strength	*Disallowed* after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	*Deprecated* after 2030 *Disallowed* after 2035
	≥ 128 bits of security strength	*Disallowed* after 2035
RSA [SP80056B]	112 bits of security strength	*Deprecated* after 2030 *Disallowed* after 2035
	≥ 128 bits of security strength	*Disallowed* after 2035

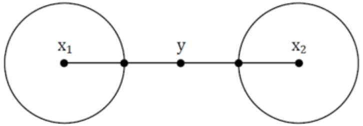
NIST IR 8547 (Initial Public Draft)

Transition to Post-Quantum Cryptography Standards

FROM THIRD ROUND FINALISTS TO PQC STANDARDS

A long and winding road! (to PQC standardization)

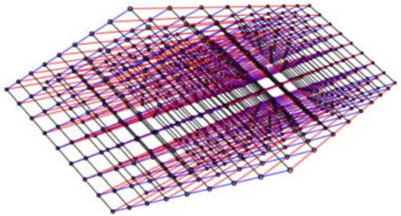
Code-based



$$H = YZ = \begin{pmatrix} \frac{1}{g(\alpha_0)} & \frac{1}{g(\alpha_1)} & \cdots & \frac{1}{g(\alpha_{n-1})} \\ \frac{\alpha_0}{g(\alpha_0)} & \frac{\alpha_1}{g(\alpha_1)} & \cdots & \frac{\alpha_{n-1}}{g(\alpha_{n-1})} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_0^{t-1}}{g(\alpha_0)} & \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \cdots & \frac{\alpha_{n-1}^{t-1}}{g(\alpha_{n-1})} \end{pmatrix}$$

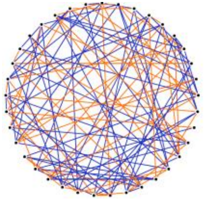
Classic McEliece
(BSI TR-02102-1)

Lattice-based



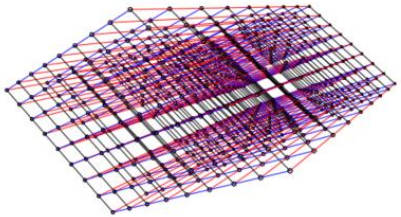
ML-KEM
(FIPS 203, ipd)
FrodoKEM
(BSI TR-02102-1)

SIDH



*

Signature



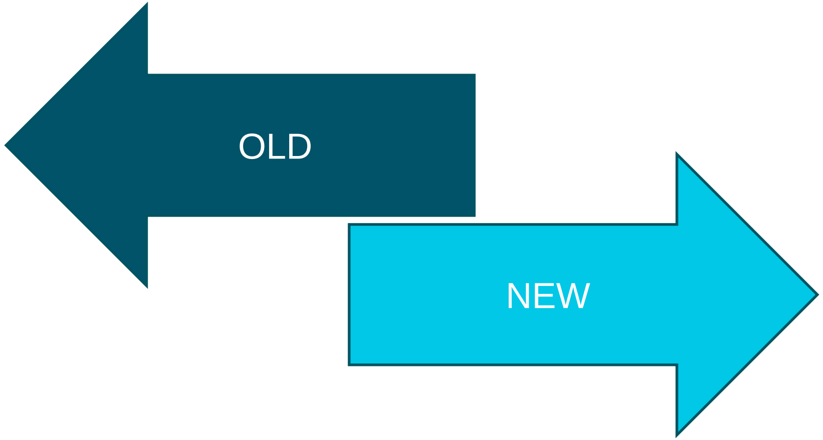
ML-DSA (FIPS 204, ipd)
SLH-DSA (FIPS 205, ipd)
FN-DSA (FIPS 206, n/a)

$\underbrace{\hspace{4cm}}_{\text{longest history}}$ $\underbrace{\hspace{12cm}}_{\text{general-purpose algorithms (It's a lattice world, baby)}}$

[*] https://eprint.iacr.org/2022/975.pdf

The Big Bang – NIST standards

- DH
- EC-DH
- DSA
- EC-DSA



OLD

NEW

- **ML-KEM**
- ML-DSA
- SLH-DSA

Just use ML-KEM?

- What and where do we need to migrate
- There are many dependencies we need to consider first
- Compatibility

→ It's not that easy

Cryptographic Inventory – Idea

https://www.pexels.com/de-de/foto/mann-person-menschen-frau-6169027/

Cryptographic Inventory – Reality

https://www.pexels.com/de-de/foto/beine-berg-zuhause-liegend-4553182/

Cryptographic Inventory – Where to Start?

- Expert Interview – Talk to your admins
- Asset Inventory
- Connection Monitoring

genua cognitix threat defender

Migration planning

- Risk-based approach
- Focus on store now, decrypt later
- Identifying migration obstacles
- Interviewing manufacturers about their PQC-strategy
- Practicability

https://de.freepik.com/vektoren-kostenlos/infografik-vorlage-mit-verlaufsfahrplan_15592047.htm#fromView=search&page=1&position=1&uuid=796c9010-9da5-470d-8074-d9b4d69d2846&new_detail=true

Use hybrids

VPN-appliance genuscreen

Use also ML-KEM

FSP 3000 S-Flex™

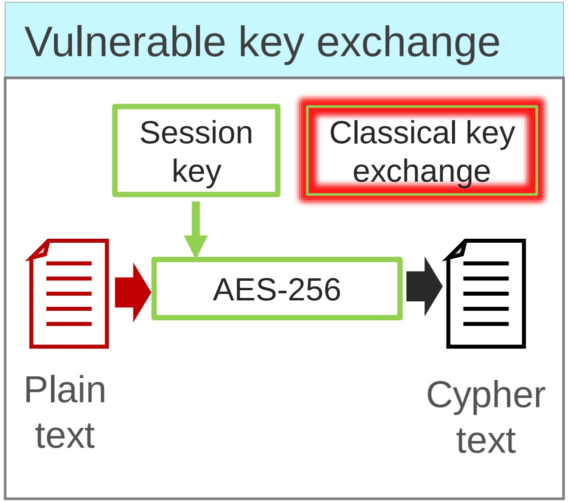
Up to
64GFC

400GbE

Recommended Actions – Summary

1. Create a cryptographic inventory
2. Preplan the upcoming migration
3. Use hybrids where possible

Making encryption quantum-safe and future-proof



Vulnerable key exchange

Session key

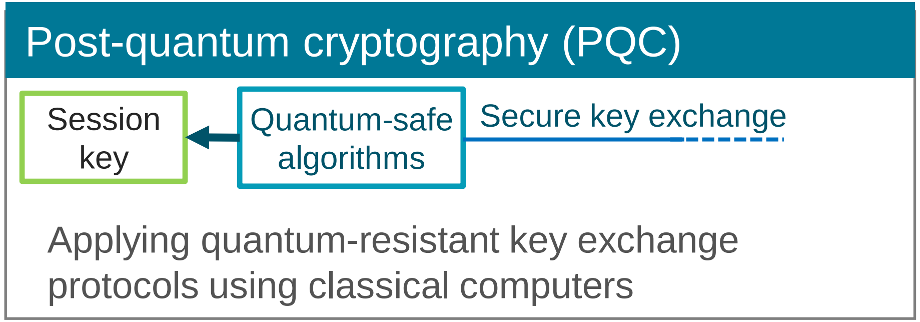
Classical key exchange

AES-256

Plain text

Cypher text

Mitigation



Post-quantum cryptography (PQC)

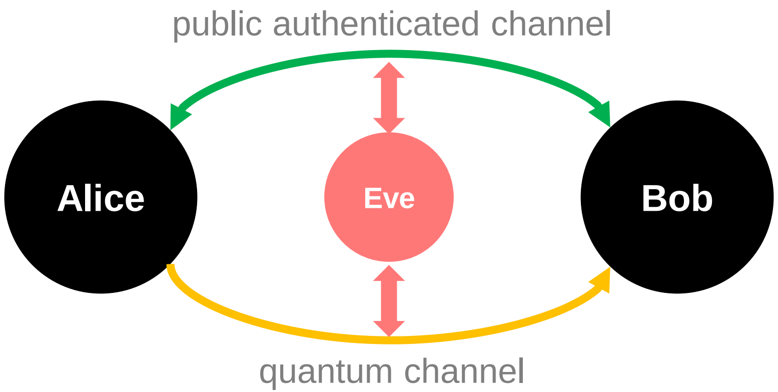
Session key

Quantum-safe algorithms

Secure key exchange

Applying quantum-resistant key exchange protocols using classical computers

The QKD principle



Principle

Key exchange based on quantum physics

- Heisenberg’s uncertainty principle
- No-cloning theorem

Types of QKD

Discrete variable QKD

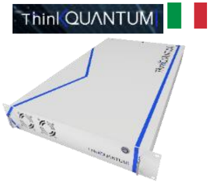
- Most established QKD variant
- Requires single-photon detectors

Continuous variable QKD

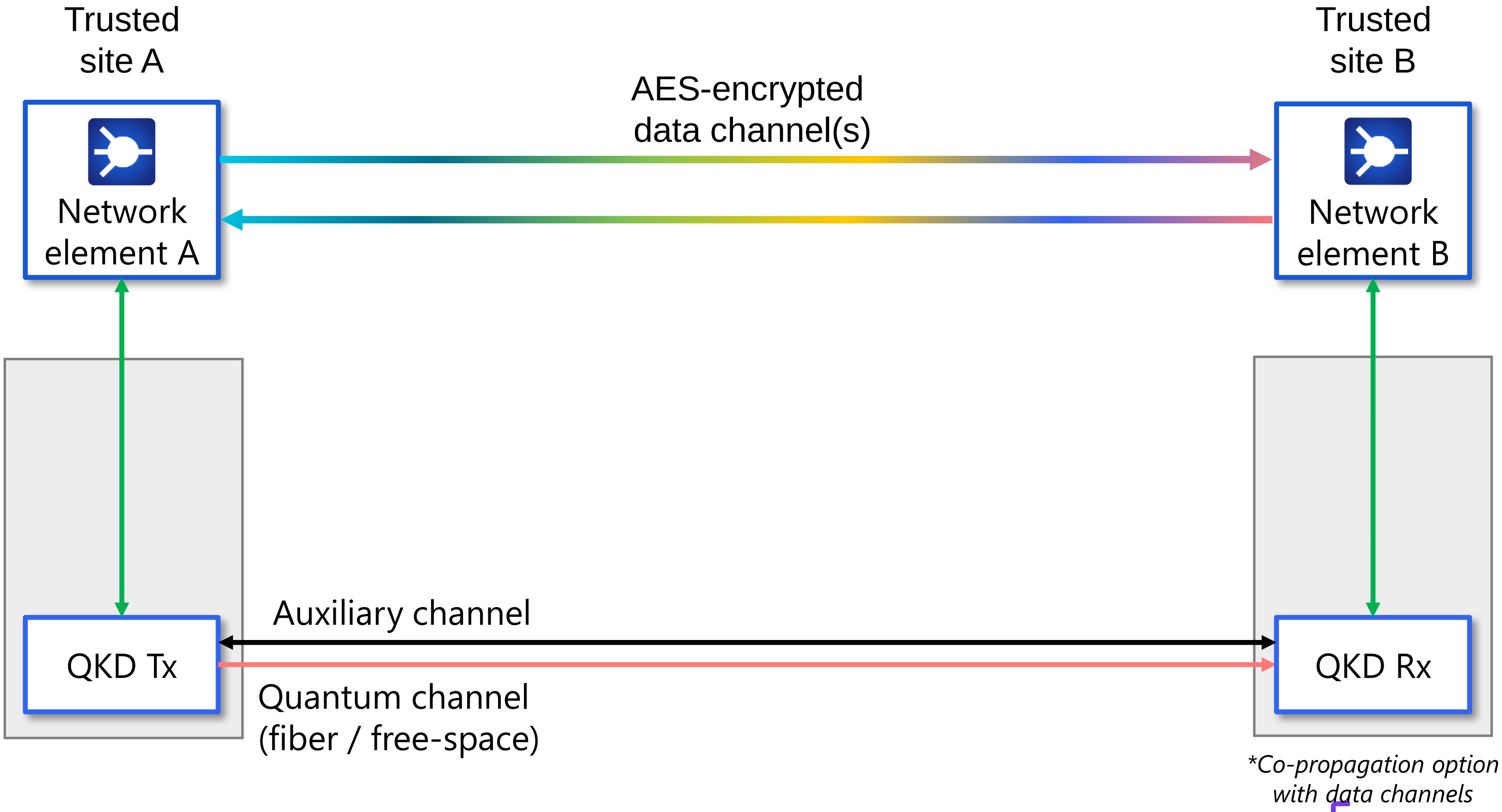
- Technology from optical transport
- Complex post-processing

Entanglement-based QKD

- Entanglement source needed
- Lean QKD system and security proof

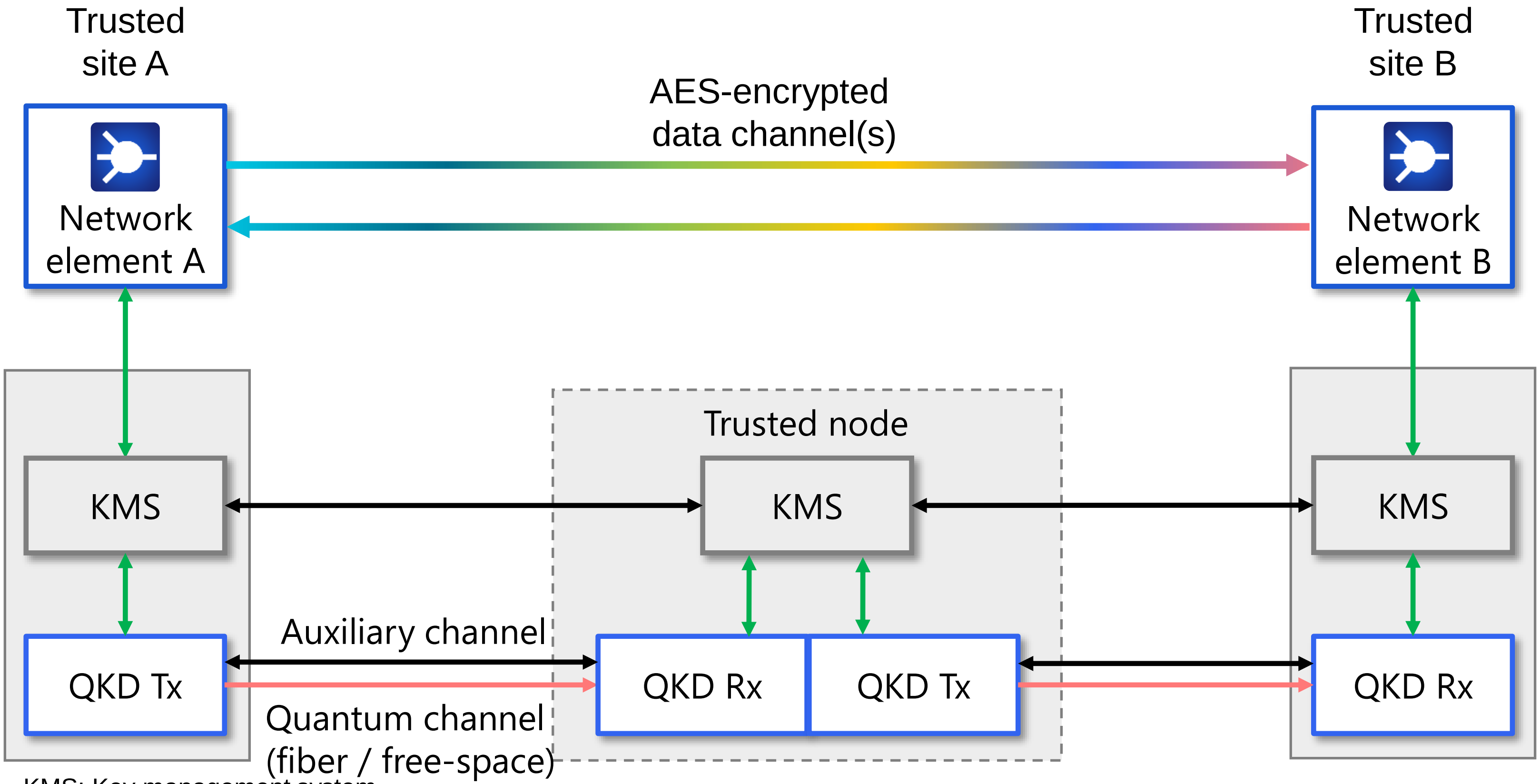


QKD is part of a larger network encryption solution …



**Co-propagation option with data channels*

… and creates dependencies important to understand



KMS: Key management system

Practical issues of QKD

Technology

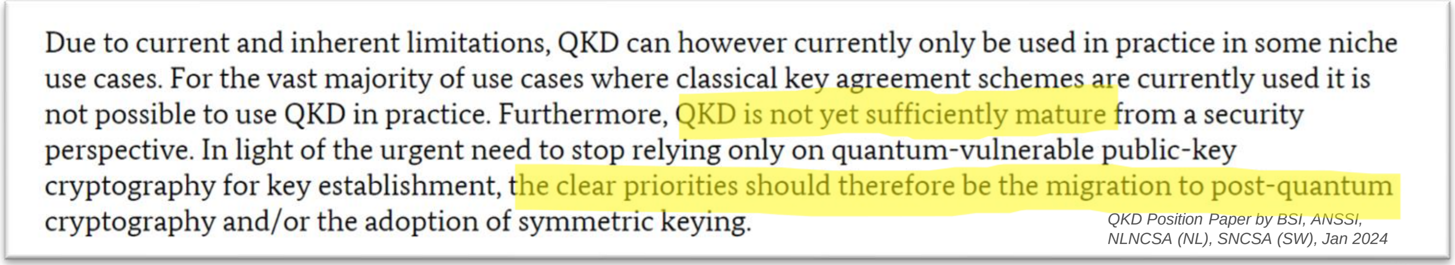
- QKD devices not fully matured
  - Stability, integration into management systems, …
- Limited reach
  - “QKD amplifiers” are research topics
- Infrastructure expansion
  - QKD devices are expensive
  - Transport medium: optical fibers / satellite links

Security

- No certified QKD devices
  - No standards
  - No security proofs
  - No evaluation criteria
- Trusted nodes need to be present
  - Exception: short data center interconnect

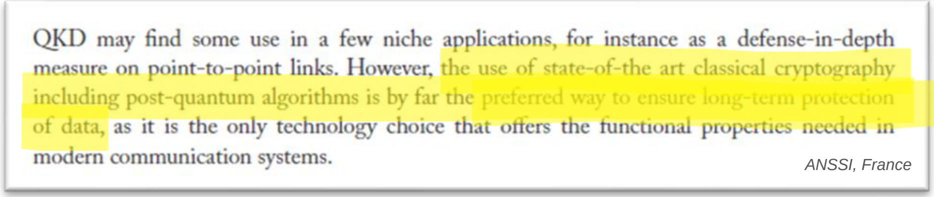
QKD does not offer end-to-end security

QKD: View by security agencies



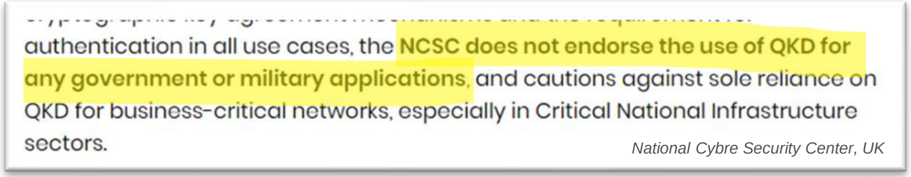
Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

QKD Position Paper by BSI, ANSSI, NLNCSA (NL), SNCSA (SW), Jan 2024



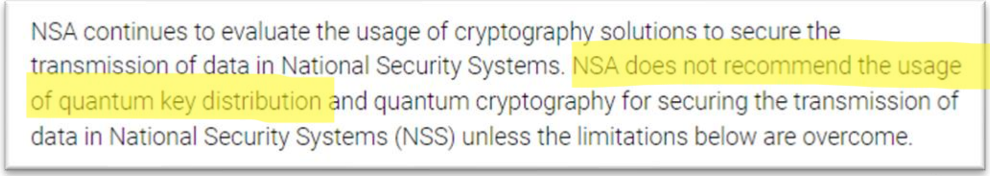
QKD may find some use in a few niche applications, for instance as a defense-in-depth measure on point-to-point links. However, the use of state-of-the art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long-term protection of data, as it is the only technology choice that offers the functional properties needed in modern communication systems.

ANSSI, France



authentication in all use cases, the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.

National Cybre Security Center, UK

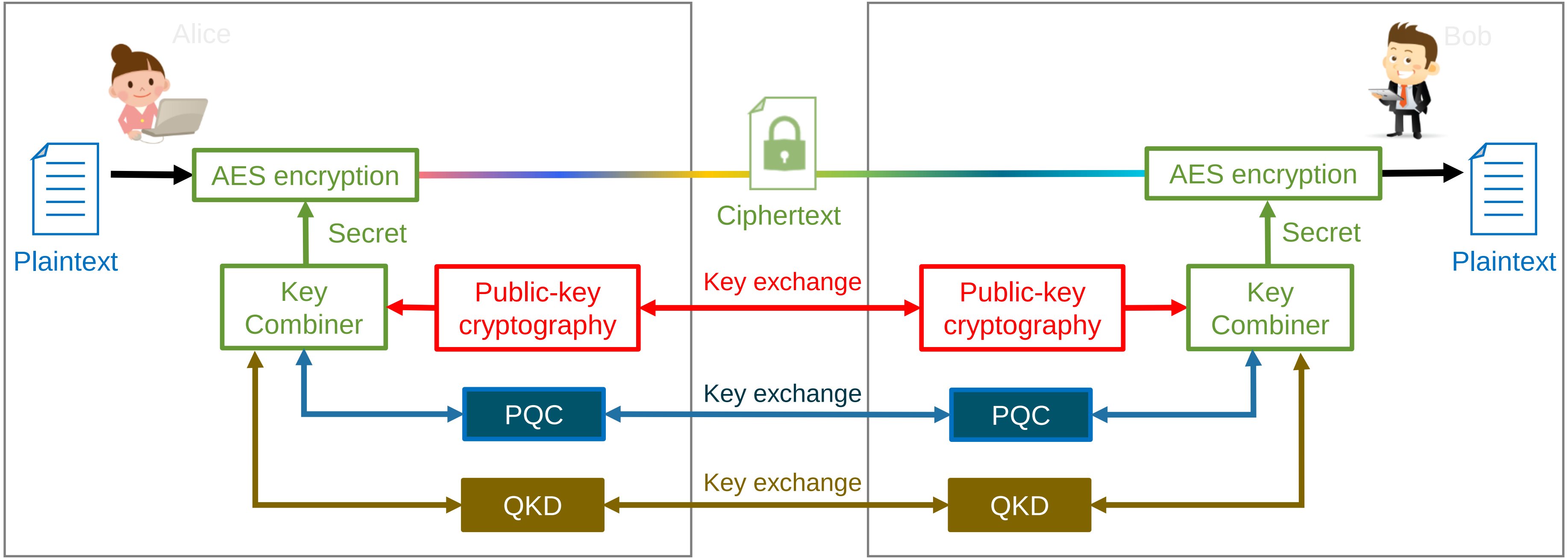


NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

National Security Agency, USA

Focus on PQC!

Hybrid key exchange is key



Combining the best and most secure of both worlds

Towards post-quantum secure networks

Migration to PQC needs to start now

Concrete actions are proposed

QKD can be addon to PQC

Adva and genua are pioneering quantum-safe cryptography for highest security demands

Quantum-safe communication today

Adva
NETWORK SECURITY

genua.

Thank you!