Adtran

Is QKD or PQC ready to quantum secure optical networks?

Netnod Tech Meeting 2024

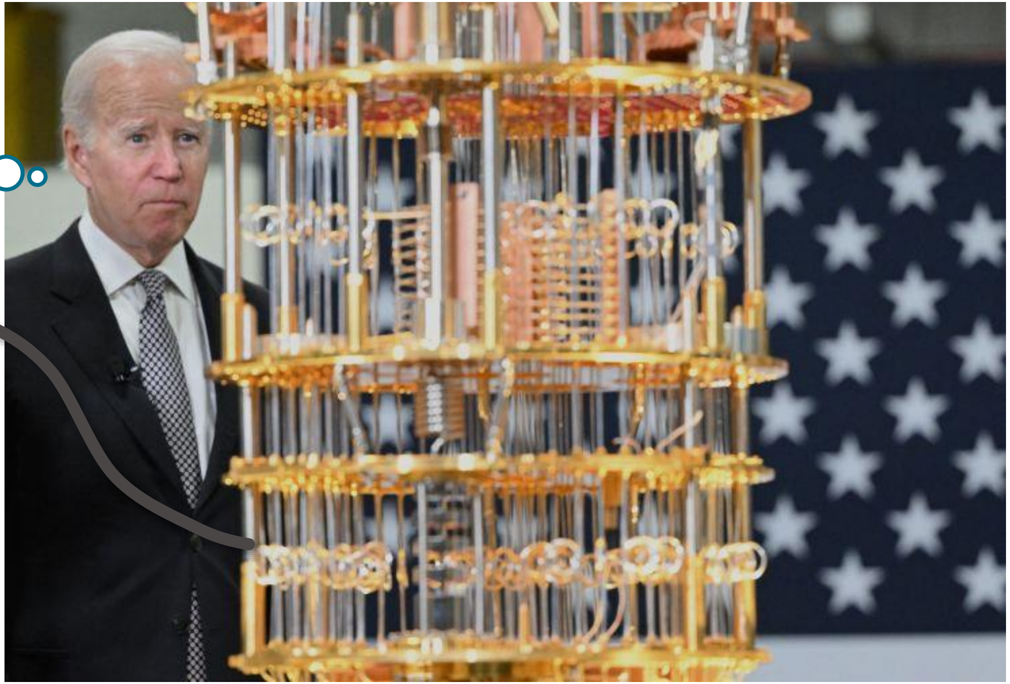
Jim Zou | Global Business Development

Tuesday October 15, 2024

How to use the quantum computer?

Can I install *Windows 10* and run *Zoom* calls?

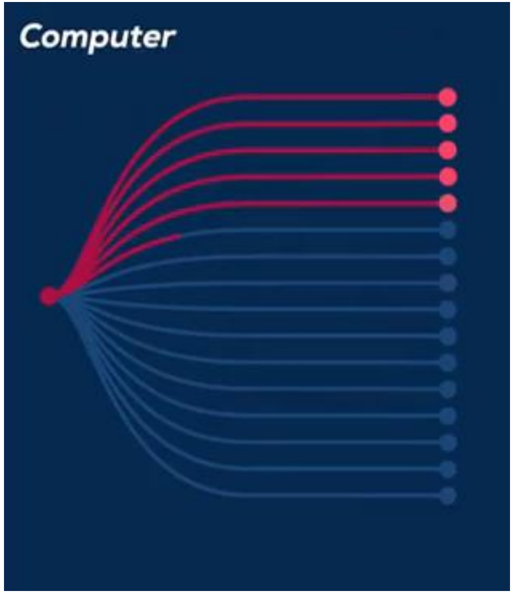
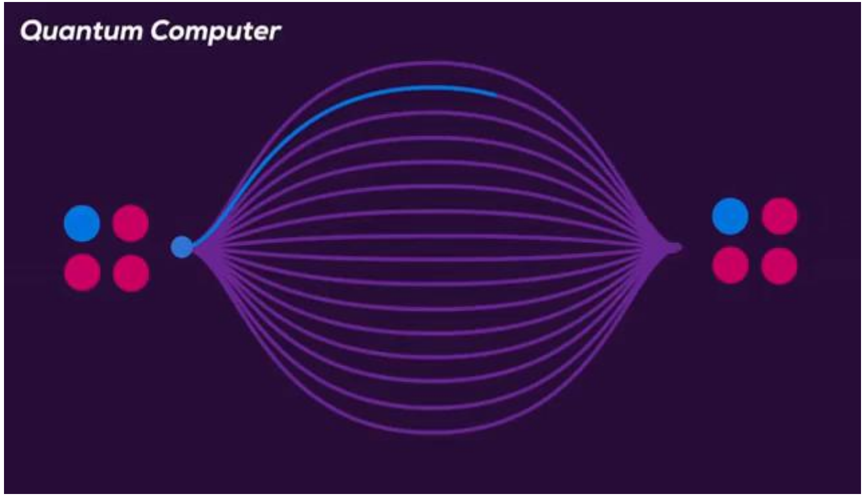
?



Unfortunately, and fortunately, the quantum computer is not a "normal computer"

Adtran

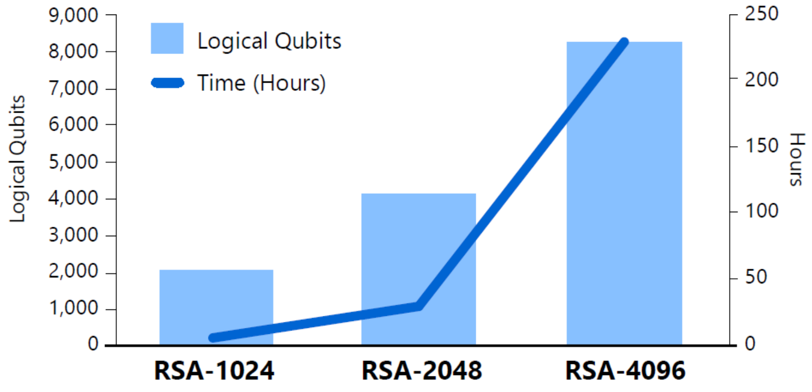
Quantum computer vs classical computer

Classical computing	Quantum computing
	

By “cleverly” manipulating Qubits, this can be exponentially more efficient!

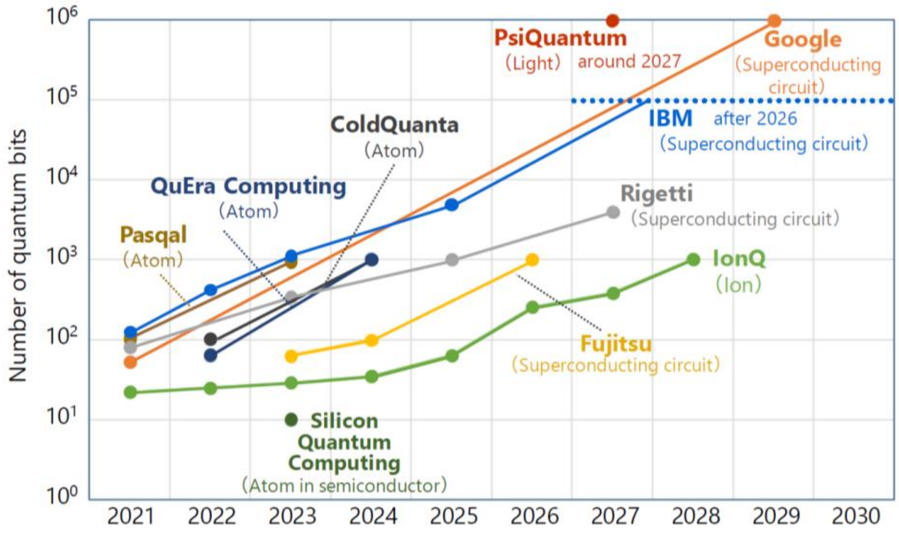
So, how quick or soon will quantum computer break RSA?

- Estimation of RSA quantum resilience by key length



Source: QED-C, data from National Academy of Sciences, Engineering and Medicine, 2019. "Quantum computing: progress and prospects. Washington DC: The national Academies Press. https://doi.org/10.17226/25196

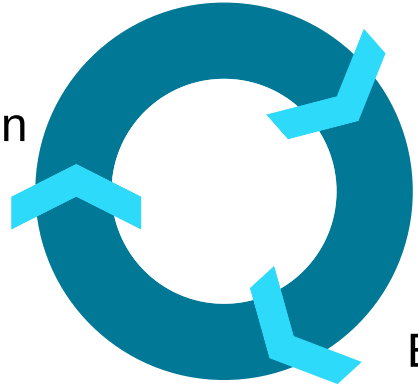
- Roadmap for physical Qubit count



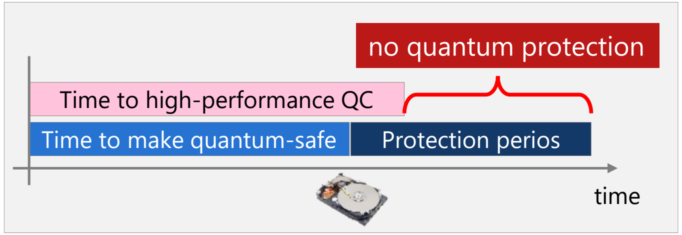
The quantum security migration circle

Quantum-safe algorithms
and deployment strategy

Start: Identify quantum
risk and initiate mitigation

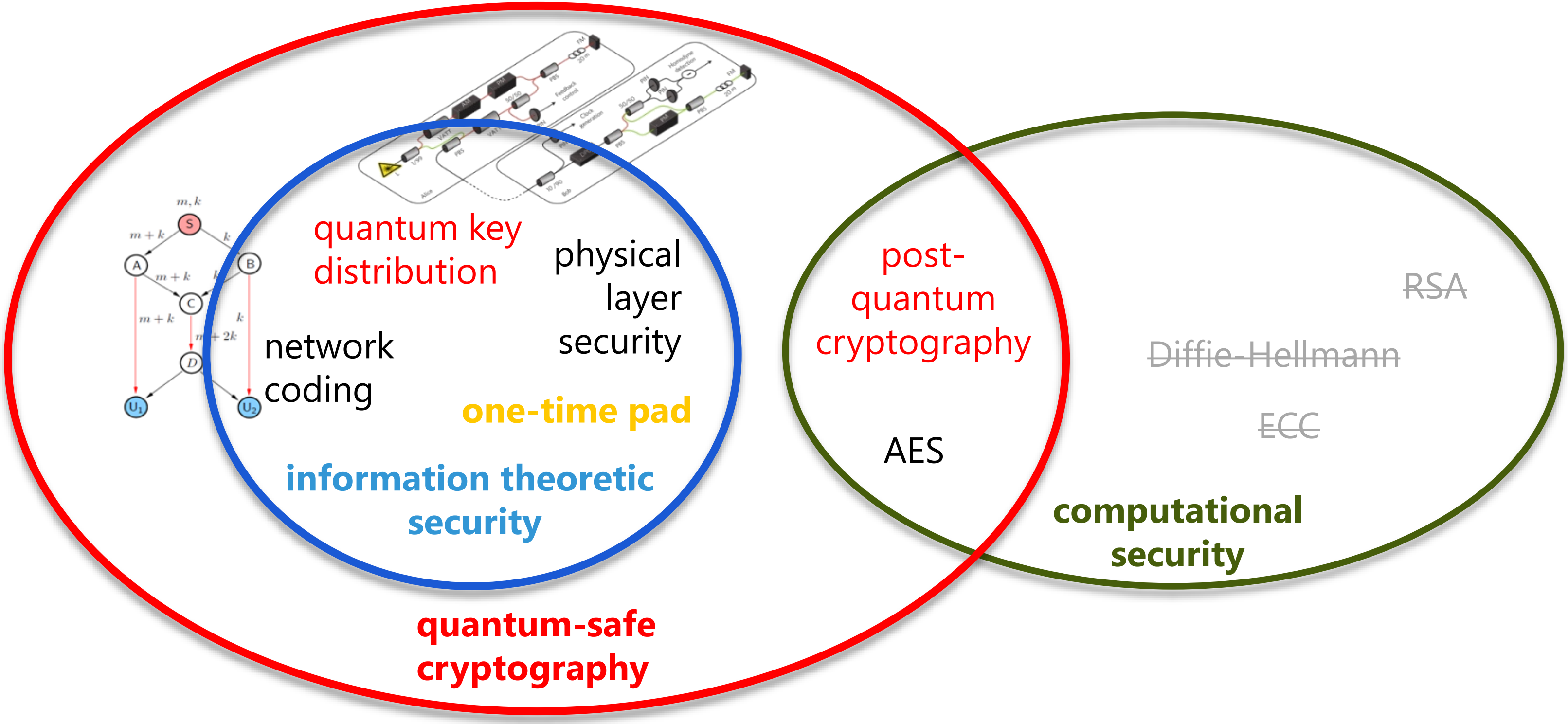


Execution, restoring
information security



Urgent. Complex. Time-consuming.

Classification of cryptographic implementations



QKD and PQC are most promising concepts

What is communication security all about?

Confidentiality	“Ensures that only authorized users…	Encryption, identity management
Integrity	…have access to accurate and complete information…	Digital signatures, authentication
Availability	…when required.”	Access management, redundancy/failover

Protection against sabotage and espionage of threat actors

Protection against application and human errors

General Business

Adtran

Is QKD ready?

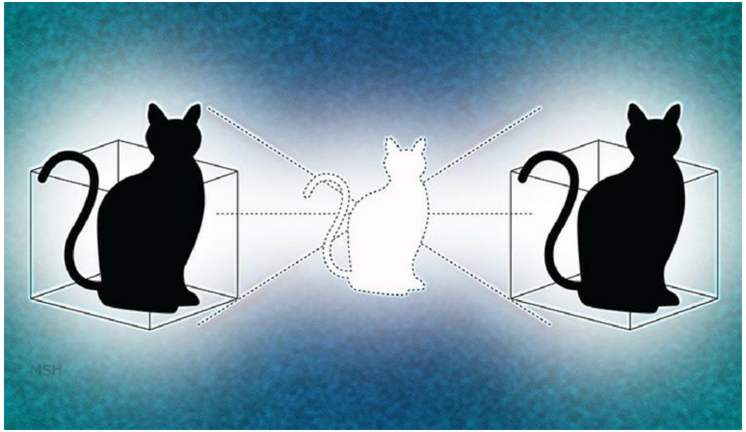
No-Cloning Theorem

Can you copy a Qubit (or photon) in superposition?

- No!

Measurement or observation “destroys” a superposition state

- Known as no-cloning theorem



(Illustration by Michael S. Helfenbein)

QKD = very low-speed photon communication that can’t be “copied”

QKD alone is NOT “fundamentally secure”

Today’s digital communication

Security = **Secure Key** + **Secure Encryption + Authentication + Protection**

- QKD is provably secure against unbounded attacks
- With one time pad encryption (OTP) it is information theoretic secure
  - True only for the concept, not an implementation
  - Almost all use cases do not allow OTP but rely on symmetric encryption
- Practical QKD provides the keys, but lacks security quantification and measurable metrics
- Trusted nodes: need to trust the QKD network provider
- Digital security can’t substitute physical protection

It is not about information theoretic security but rather a different attack surface!

Current EU government position statement on QKD

Why is QKD not mature?

- No standardized QKD protocols
- No comprehensive security proofs under realistic conditions
- Evaluation methodology (e.g. to evaluate resistance against implementation attacks) missing


RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office
for Information Security

General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on
Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

26 Jan 2024

QKD is not yet sufficiently mature from a security perspective

WHAT SECURTY BODYS SAID ABOUT QKD

QKD is controversial

Bundesamt für Sicherheit in der Informationstechnik

security must be quantified for specific protocols
Limited distance, no end-to-end security
Side channels endanger product security

QKD could be seen as complementary rather than competitive as soon as the QKD ...

National Cyber Security Centre
a part of GCHQ

GCHQ white paper on quantum security technologies:
QKD protocols address only the problem of agreeing keys for encrypting data, (but not authentication, data integrity, software updates).

- **Partial solution (only key agreement)**
- **No end-to-end security (trusted nodes)**
- **Dedicated equipment on the physical layer**
- **Securing/validating against side channels is hard**
- **Can provide complementary physical security**

National Security Agency/Central Security Service:
does not recommend QKD for National Security Systems
- only a partial solution
- requires special purpose equipment.
- increases infrastructure costs & insider threat risks.
- securing/validating QKD is a significant challenge.
- increases the risk of denial of service.

Agence nationale de la sécurité des systèmes d'information

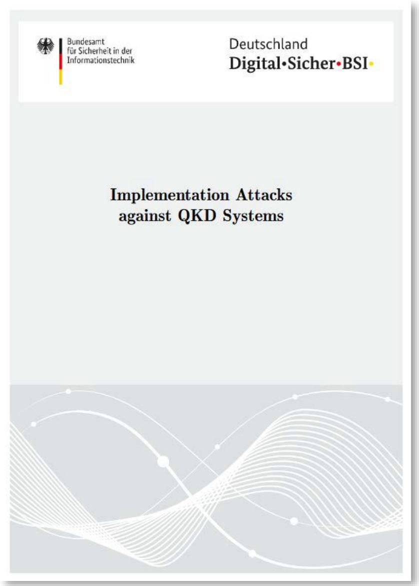
... functional equivalent to public key cryptography and offers limited applications due to the need of a dedicated communication infrastructure and without real routing capabilities. QKD could be used for niche applications providing some extra physical security on top of algorithmic cryptography

BSI report on implementation attacks

What's that about?

- Structured overview of known QKD-specific implementation attacks on QKD systems according to the present literatures

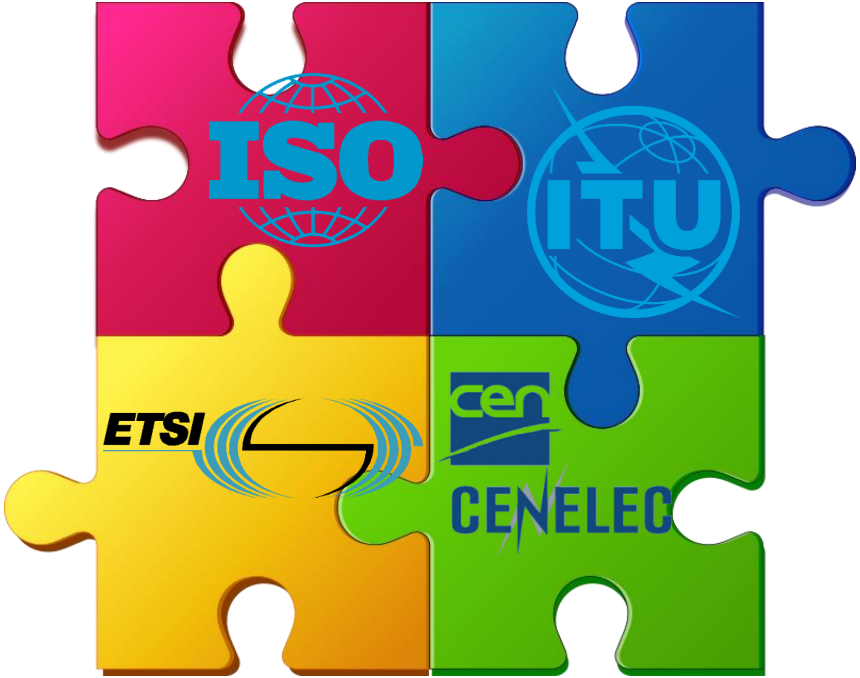
- Research on further attacks?
- Effectiveness of countermeasures?
- More practical attack experience?
- Classical IT security of QKD devices?



21 Nov 2023

Standardization and certification

ISO/IEC JTC 1/SC 27
Framework for QKD evaluation according to common criteria



ITU-T Y.38xx
QKD networks
ITU-T X.17xx
Security aspects

ETSI ISG QKD Industrial QKD standards for ICT networks
(Interfaces, use cases, security, CC protection profile, …)

CEN/CLC/JTC 22 Quantum Technologies
including Quantum communication and cryptography

Standardization is a first step for certification

15 YEARS OF DEVELOPMENT

Cost, Size, Power

Optical transceivers

2008
40G (Nortel)

15 years

2023
400G QSFP-DD
(OIF 400ZR)

QKD Tx/Rx

2008
Clavis² (IDQ)

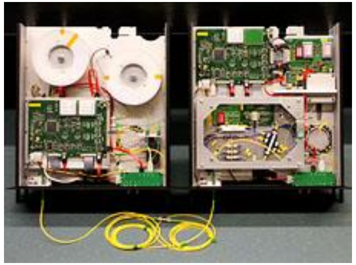


Foto ©2008 Vadim Makarov

15 years

2023
BB84 / CV-QKD / BBM92

Adtran

Is PQC ready?

Updated!

NIST

NIST Post-quantum Cryptography Project

2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024

Aug 2016
Draft submission requirements & evaluation criteria

Dec 2016
Final requirements and criteria

Nov 2017
DL for submissions

April 2018
1st NIST PQC workshop

Jan 2019
2nd round started

Aug 2019
2nd NIST PQC workshop

July 2020
Selected finalists and alternate candidates

2020-2021
Round 3 seminars (virtual)

July 2022
Announced finalists to be standardized and candidates for 4th round

2023
Standards drafts released

8/13/2024
Final standards

Adtran

HARMONIZING QUANTUM-SAFE TRANSITION

EU Recommendation on PQC


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

Statement and Goal

To encourage Member States to develop and implement a harmonized approach as the EU transitions to post-quantum cryptography.

As a software-based solution, PQC is compatible with our existing infrastructures in several sectors, and so can be deployed relatively swiftly.

Existing cryptographic approaches or QKD may be combined with PQC via hybrid schemes to address existing public administration systems and critical infrastructures.

Help EU develop a consistent migration strategy to protect digital infrastructures

Post-quantum key exchange – status

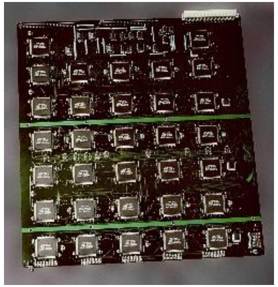
Approach	Advantages	Disadvantages
Code-based encryption (using Goppa codes)	High confidence in security Very fast encryption Short ciphertexts	Large public keys
Lattice-based encryption (using NTRU or related)	Short ciphertexts and keys Very fast encryption	Relatively young algorithm
Supersingular elliptic-curve isogeny (SIDH) key exchange	Short messages	Broken – require more security analysis

Adapted from: D. J. Bernstein and T. Lange, Post-quantum cryptography, *Nature, Nature Publishing Group,* **2017**, *549*, 188

Large public keys can be acceptable in optical transmission with high data rates

Learning from the crypto-past

Brute-force attacks



“Deep Crack”
breaks DES (1998)

Mathematical attacks


ars TECHNICA

Post-quantum encryption contender is taken out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.


Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

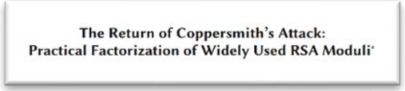
IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Two hot PQC contenders
broken in 2022

Implementation attacks

2016


CacheBleed: A Timing Attack on OpenSSL Constant Time RSA


The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli

2017

2017

Meltdown Spectre

Dec 2023(!)

KyberSlash

Never-ending
side-channel attacks

Highly complex and dynamic environment

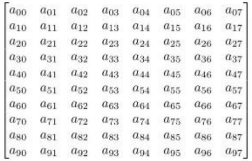
General Business
Adtran

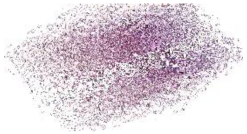
LONG BUT RIGHT WAY!

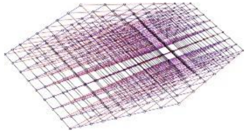
BSI vs NIST to PQC standardization

Bundesamt
für Sicherheit in der
Informationstechnik

BSI TR-02102-1
(Version: 2024-01)



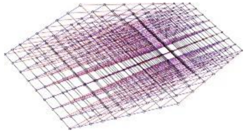




Classic McEliece	FrodoKEM	ML-KEM (To be added)
longest history	unstructured lattice	structured lattice

NIST

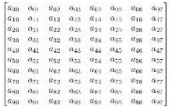
Just standardized!

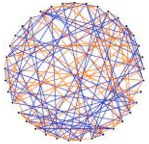


CRYSTALS-KYBER
(ML-KEM [3])

general-purpose algorithm
(ML-KEM is royalty-free [2])

round 4 submissions



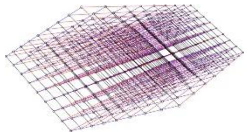


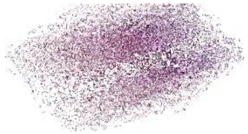
Classic McEliece
BIKE
HQC

[2] https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/selected-algos-2022/nist-pqc-license-summary-and-excerpts.pdf
[3] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

ANSSI vs NIST to PQC standardization

ANSSI
(2023-09)





CRYSTALS-KYBER

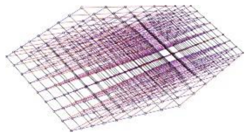
FrodoKEM

structured lattice

unstructured lattice

NIST

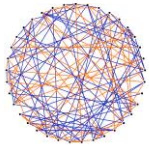
Just standardized!



CRYSTALS-KYBER
(ML-KEM [3])

general-purpose algorithm
(ML-KEM is royalty-free [2])

round 4 submissions

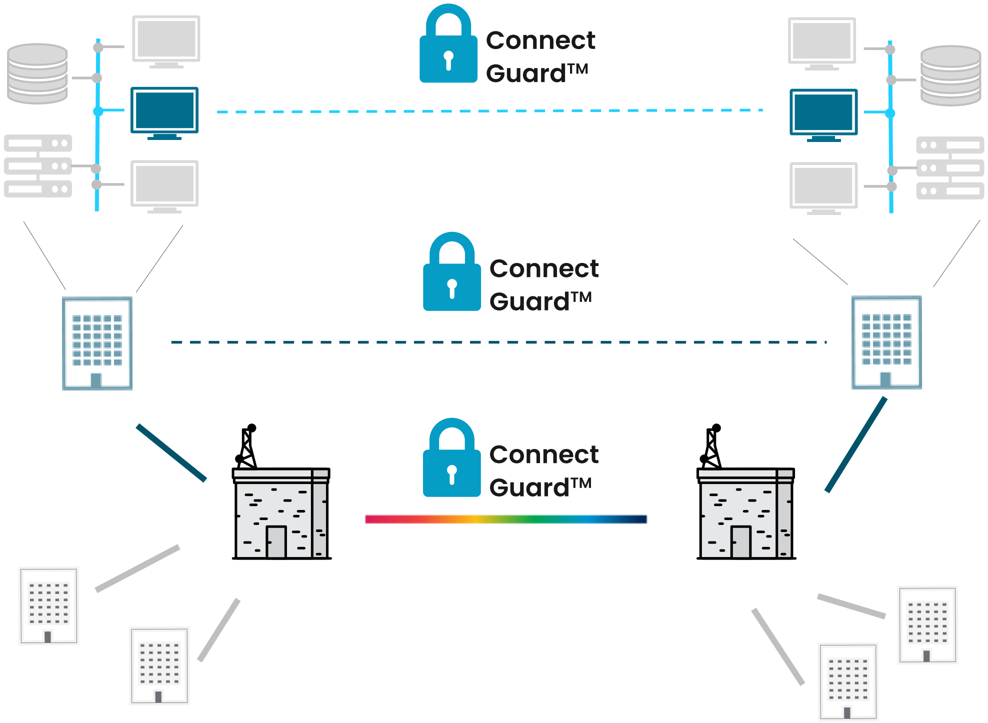


Classic McEliece
BIKE
HQC

[2] https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/selected-algos-2022/nist-pqc-license-summary-and-excerpts.pdf
[3] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

How would the practical deployment look like?

Holistic network security



IP Layer 3 protection

Interconnecting users, applications and resources in a secure way

Ethernet Layer 2 encryption

End-to-end encrypted connectivity services

Optical Layer 1 encryption

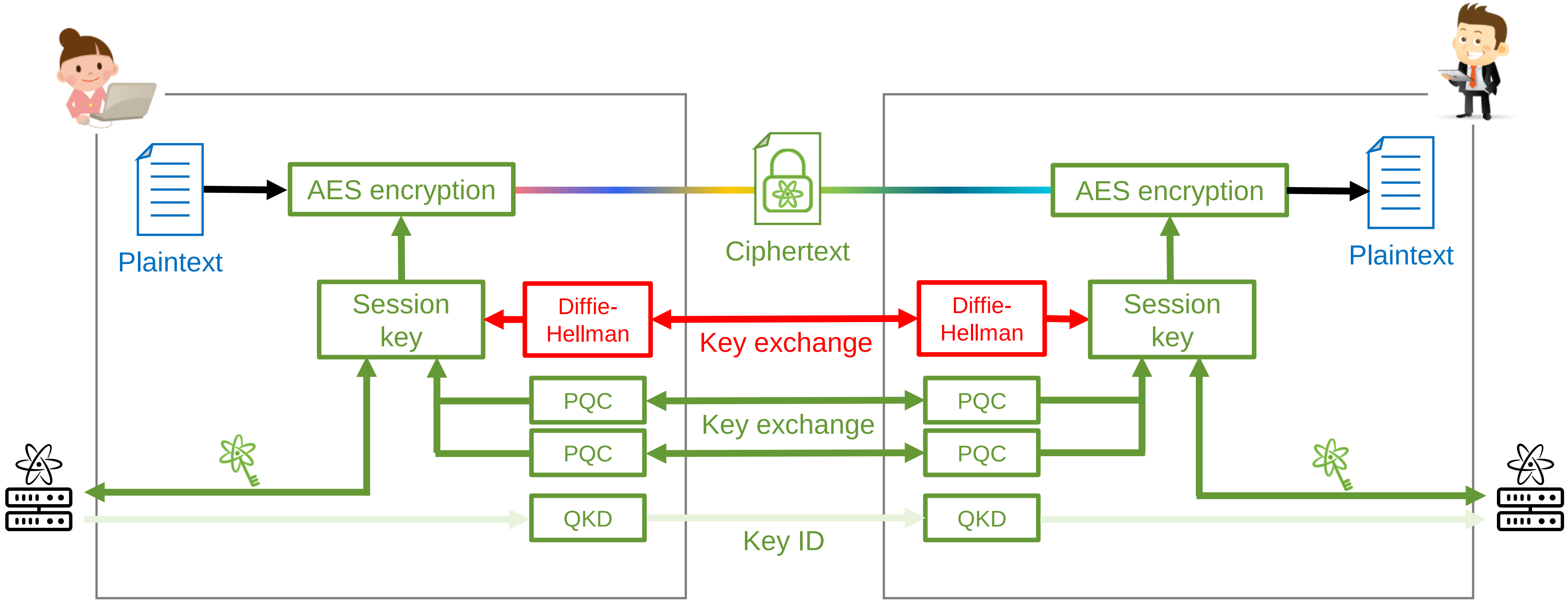
Protecting terabit optical connections with lowest latency

USP: Encryption solutions for any customer need and services scenario

General Business

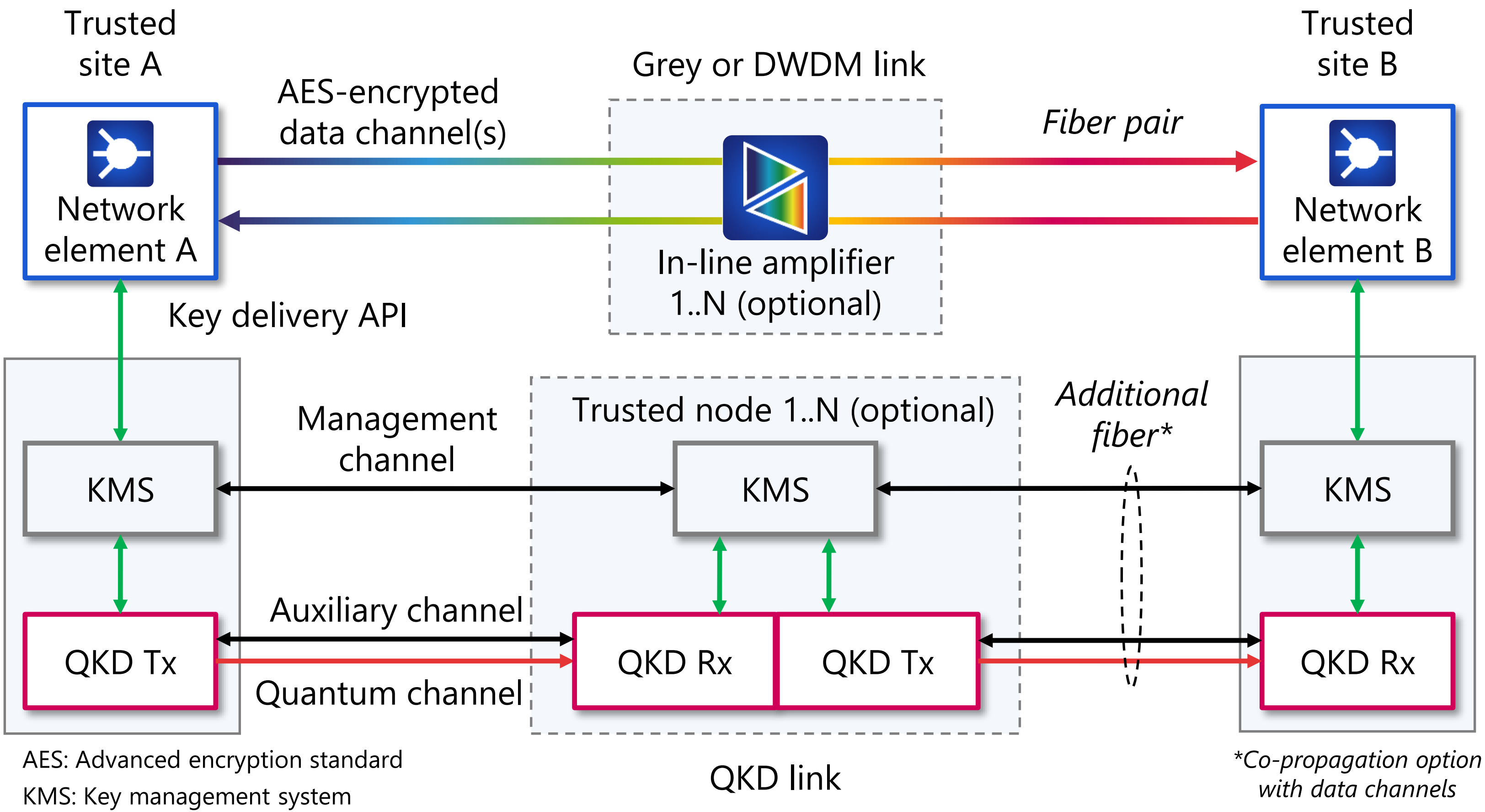
Adtran

Hybrid key exchange is key ☺



Combining the best and most secure of both worlds

Limited reach of QKD requires trusted nodes



AES: Advanced encryption standard
KMS: Key management system

Co-propagation option with data channels

How we support your compliance requirements

Security certifications

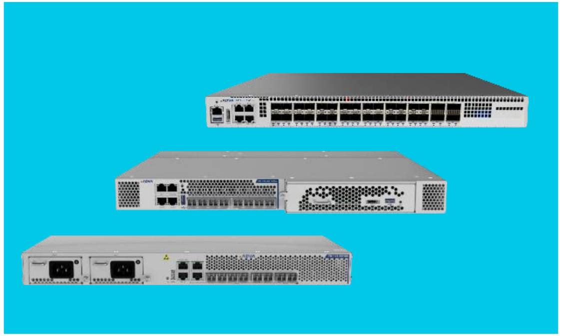
- Common Criteria EAL2
- Common Criteria NIAP
- US CsFC. DOD

Approved encryption

- NIST - FIPS certified
- BSI approval for restricted data of DE, EU, NATO

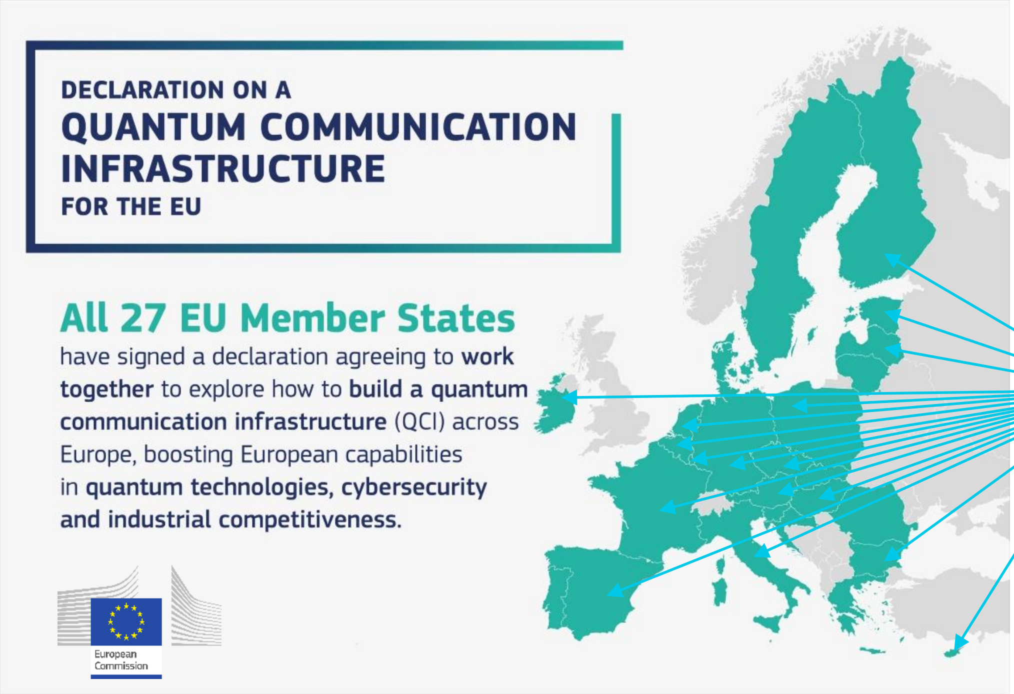
Future certifications

- BSI TR-03163 (aka EU-CC)
- EU Cyber Resilience Act (CRA)



Adtran

EuroQCI as stepping stone to the Quantum Internet



EuroQCI Phase-1 (**154M€)**

- European Industrial Ecosystem **(44M€)**
- National QCI deployment **(108M€)**
- Testing and validation for certification **(2M€)**

Adtran and Adva Network Security are engaged with most of the state consortia, offering QKD-ready L1/2 encryption transport solutions

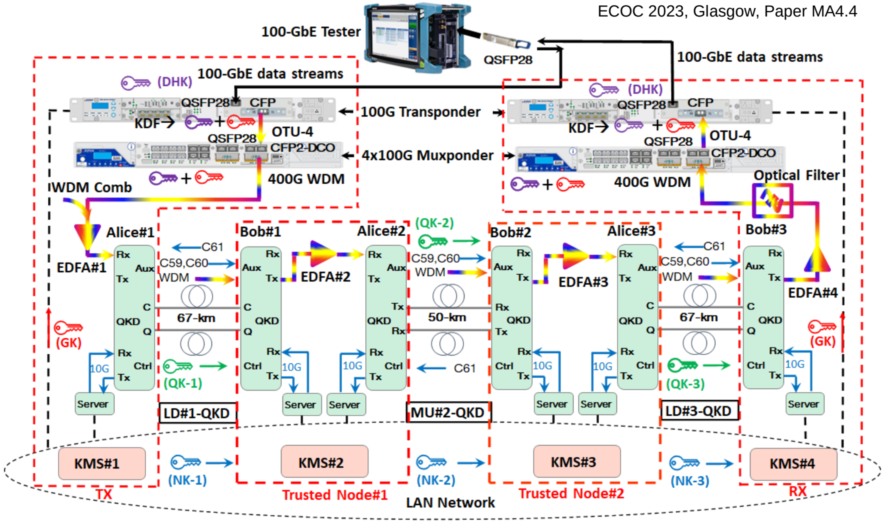
EuroQCI is planned to be fully operational by 2027

General Business
Adtran

Feasibility studies by the EU incumbent operators

Orange

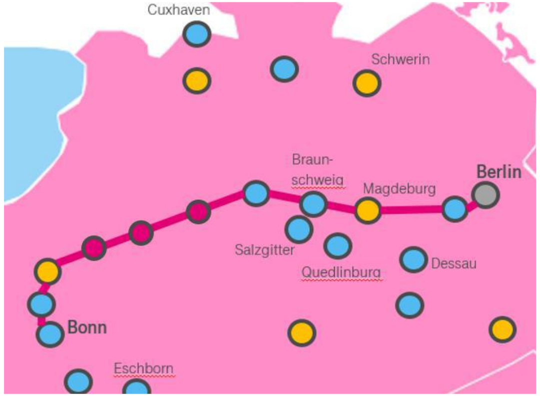
- 400G transmission of QKD-secured data stream over 184 km SSMF through three QKD links and two trusted nodes



ECOC 2023, Glasgow, Paper MA4.4

Deutsche Telekom

- **DemoQuanDT:** Application-oriented **demo**nstration of **quan**tum communication in **D**eu**t**schland



- Carrier grade
- Minimum intervention
- Layered architecture

- Up to 18 trusted nodes
- Field deployable trial

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt

Gaining experiences and shaping deployment strategies

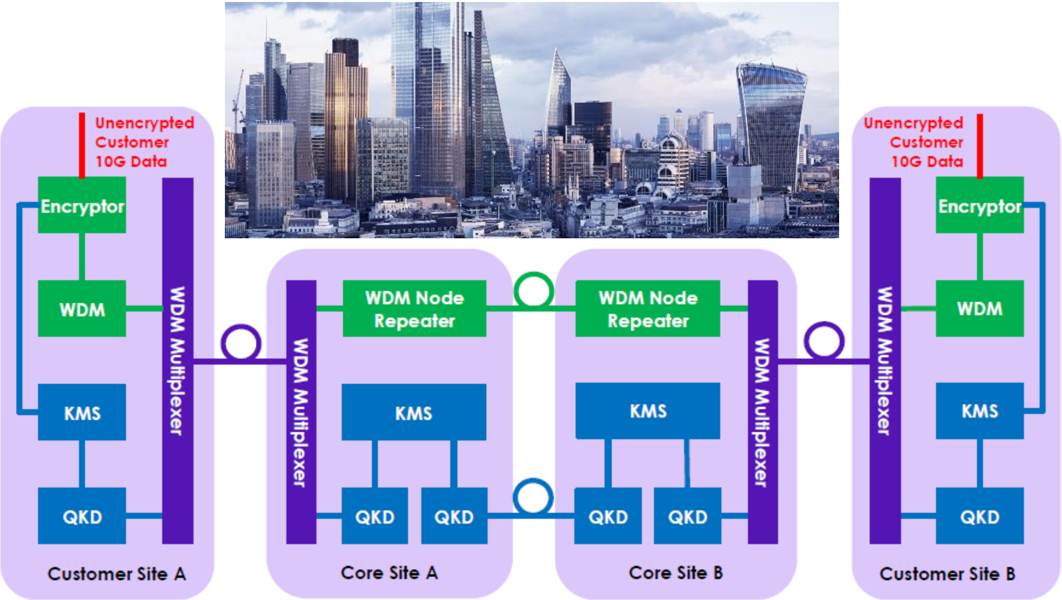
COMMERCIAL PILOT FOR ENTERPRISES

London quantum-secured metro network services trial

Connecting sites in London's Docklands, the City, and the M4 Corridor

- End-to-end encryption between sites
- Hybrid encryption keys (+PQC in dev.)
- Dedicated high bandwidth with low latency
- ITS-authentication of QKD
- Backbone of both core and access
- Flexibility to co-research with customers

Customers today:



Summary

1 **Securing optical networks is getting more important**
PQC will be the standard way while QKD is a research complement

2 **Operators won’t be happy to fiddle with transport networks**
PQC is relatively easier to be migrated while QKD adds extra confidence

3 **Hybrid key exchange and crypto-agility**
Best practice to maximize security level

4 **Research advances, standardization, commercialization**
Regulatory mandate? To be monetized? A long and winding road!

Thank you / Vielen Dank

jim.zou@adtran.com