# QKD Impact on Optical System and PQC Solution

Maurizio Gazzola
Head of Optical Architecture Cisco

# Webex App

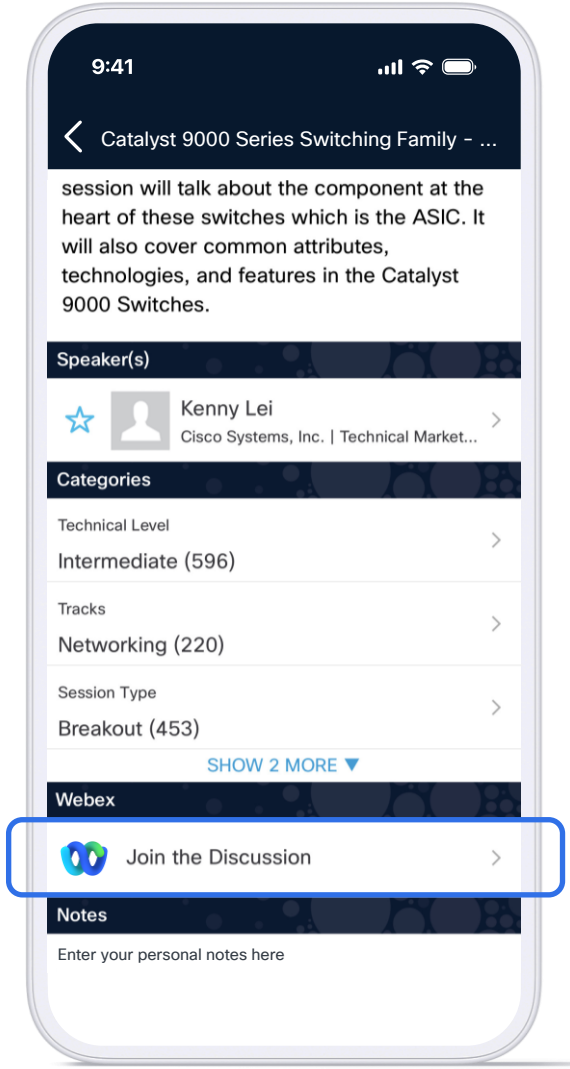
## Questions?

Use Webex App to chat with the speaker after the session

## How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

**Webex spaces will be moderated by the speaker until February 27, 2026.**



# Agenda

01 Security Threat by Quantum Computing

02 Is it a real Threat?

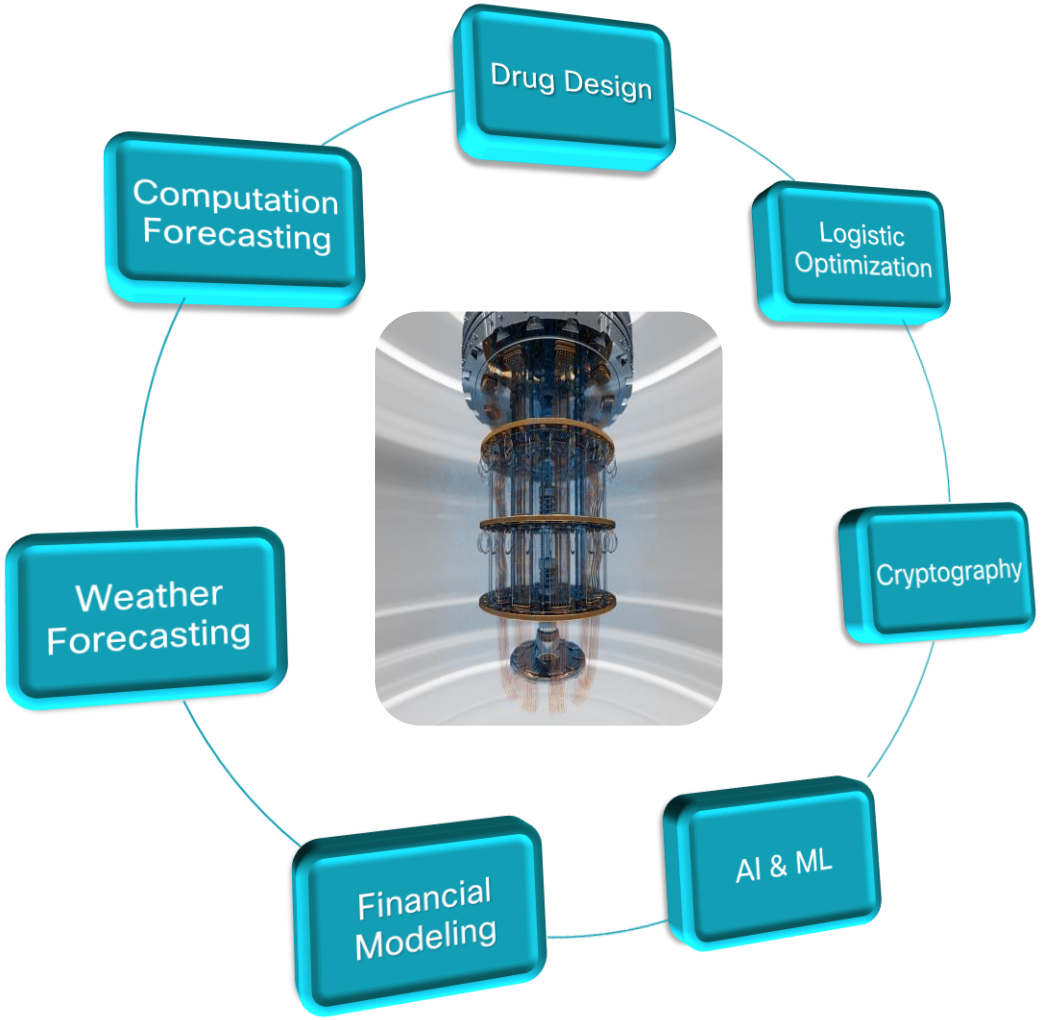
03 Possible Solutions

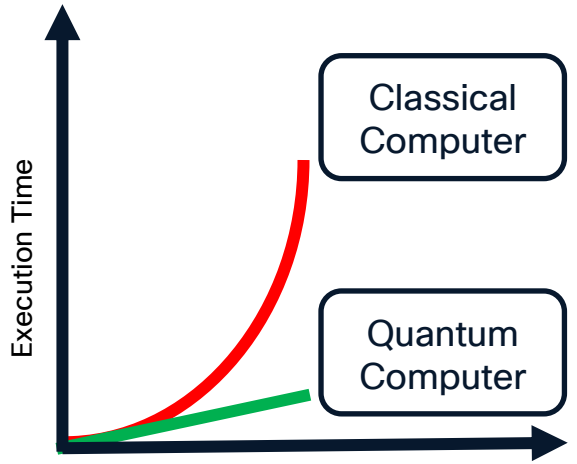
04 Cisco Strategy

05 Conclusion

# Security Threat by Quantum Computing

# Quantum computing power

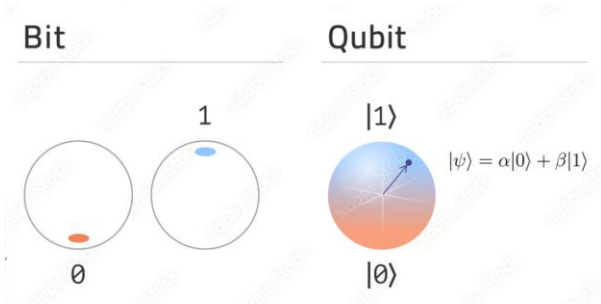


# Classic vs. Quantum Computer

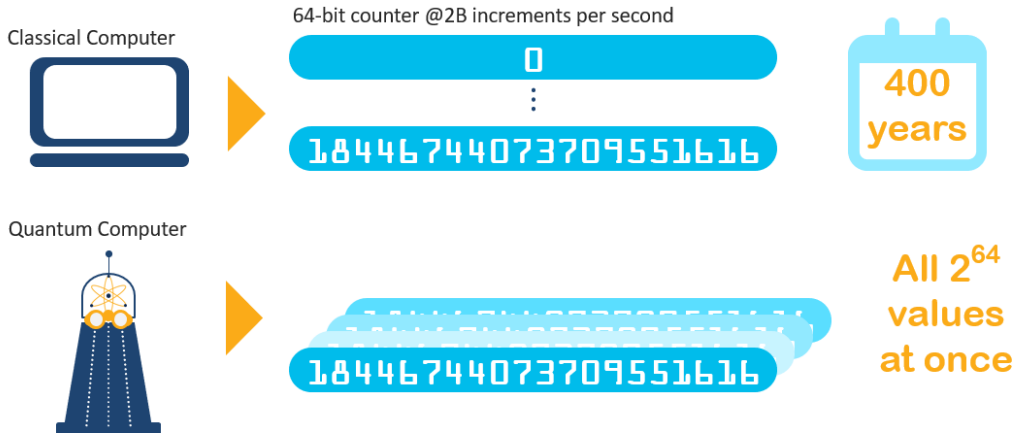
## Classic Computer

- Relies on classical bits: can assume one single value at a time
- Works in serial approach
- Very slow at solving certain types of problems (e.g. exploring a huge number of permutations)



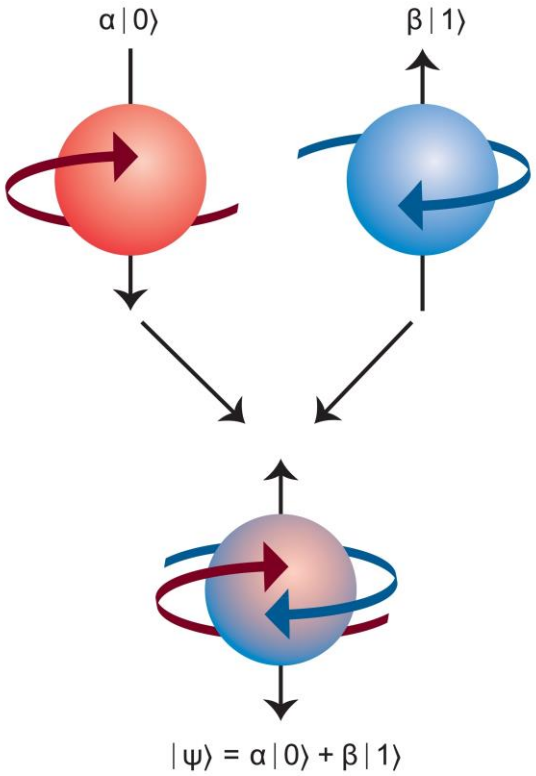

## Quantum Computer

- Relies on qubits: represent multiple states at a time with different probabilities
- Works in holistic approach
- High efficiency in the solution of problems thanks to its ability to probabilistic provide the outcome of a system in a single step



# Quantum physics power: superposition

- Classical bit : 1 or 0
- Quantum bit (qubit): $\alpha\,|1\rangle + \beta\,|0\rangle$ , $|\alpha|^2 + |\beta|^2 = 1$



# Quantum computing supremacy

classical

$0100110101$

quantum

$$p_0 0000000000$$
$$+p_1 0000000001$$
$$+p_2 0000000010$$
$$\vdots$$
$$+p_{2^N} 1111111111$$

- 2 qubits: superposition of 4 possible basis states
- 3 qubits: superposition of 8 possible basis states
- n qubits: superposition of $2^n$ possible basis states

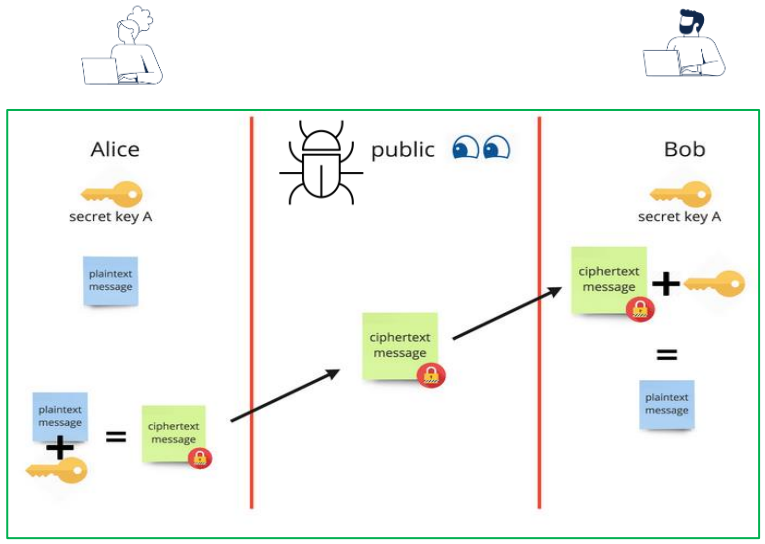
100 bits ➔ 100 0 or 1 coefficients

100 qubits ➔ **1,27 $10^{30}$** complex coefficients

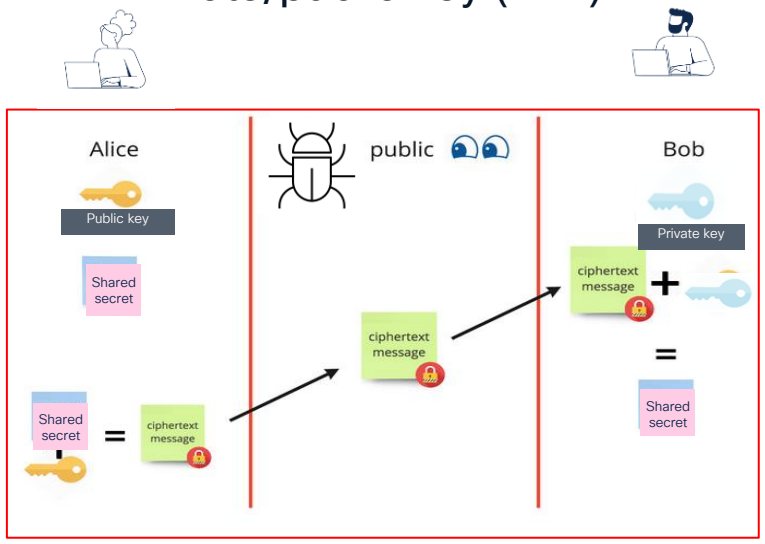
# Cryptography – Basic concepts

- Data is encrypted using symmetric key cipher by dedicated HW
- Key exchange and signatures are based on private/public keys (PPK) based asymmetric algorithms.

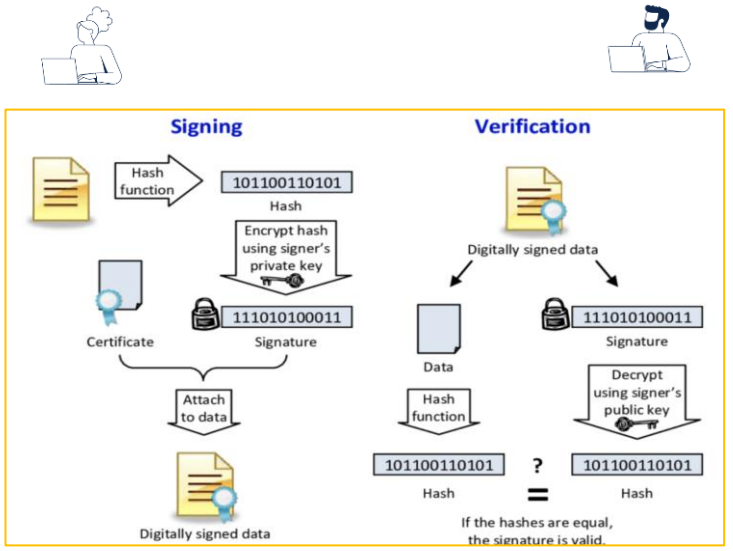
## Symmetric key cipher




## Asymmetric algorithm private/public key (PPK)




## Digital signature

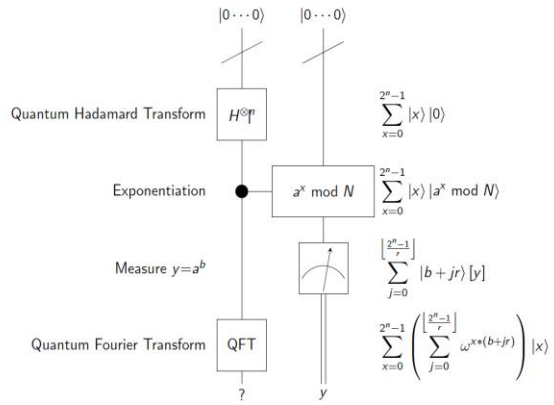


# The threat

Quantum computing expected to break current Public Key Exchange (PPK) used for “key exchange” and “authentication”

- *Shor’s algorithm enables to break RSA, DH, and ECDH impacting today asymmetric cryptography.*

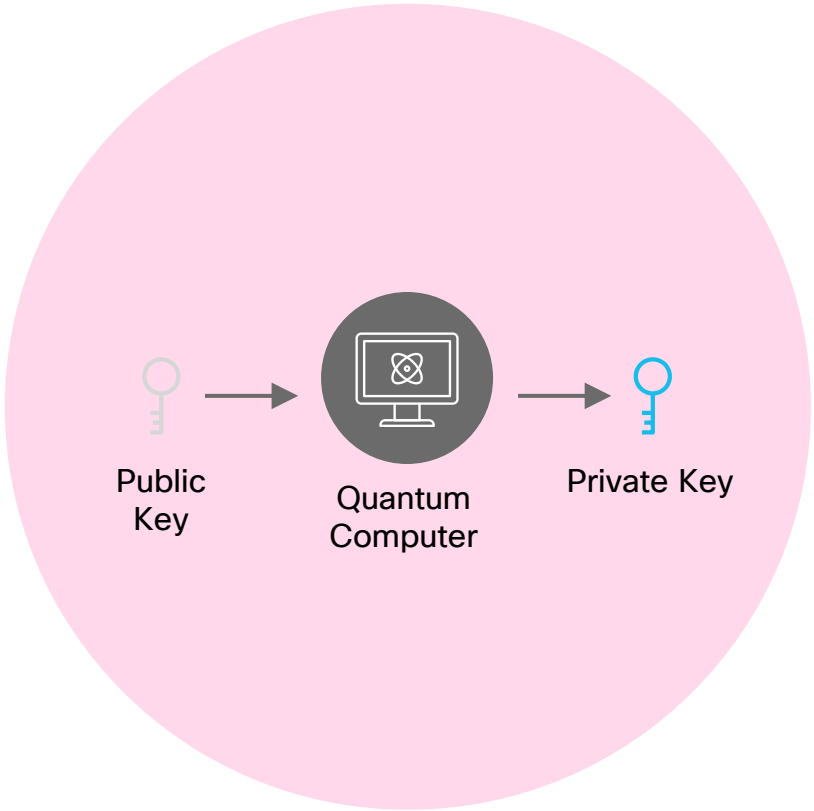
- *Symmetric ciphers (like AES-GCM-256) are not at risk, but to operate safely requires periodic key refresh*




*P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” IEEE FOCS 1994. doi.org/10.1109/SFCS.1994.365700*

# Quantum computing impacts

## Asymmetric cryptography




### Public / Private Key Pairs

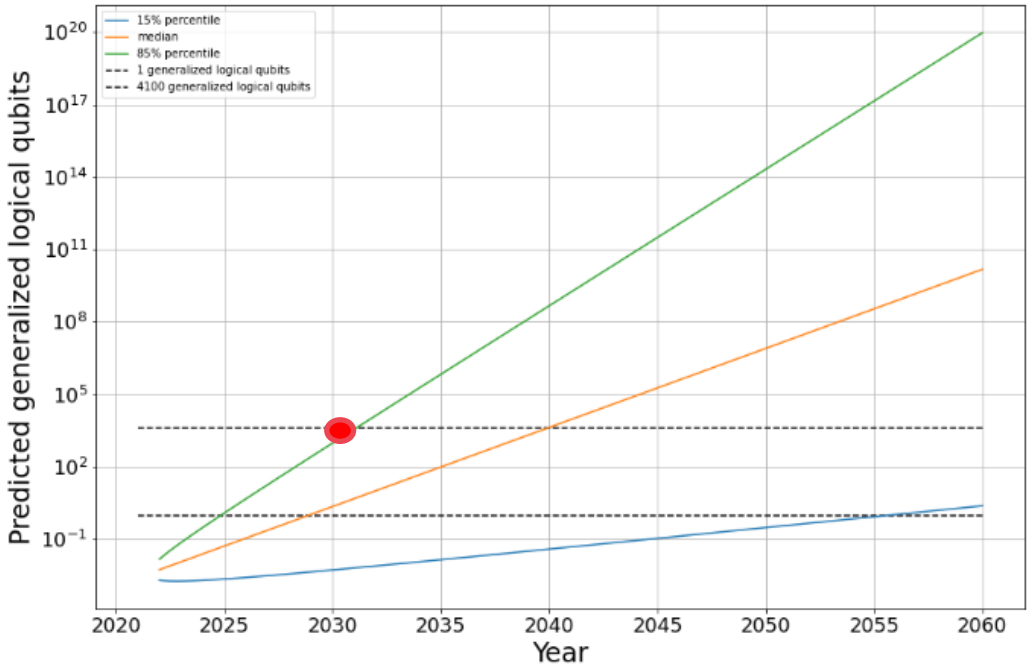
- Identity (e.g., HW SUDI, TLS certificates, S/MIME certificates, Root CA certificate)
- Software signing & verification,
- Key exchange

### Threats

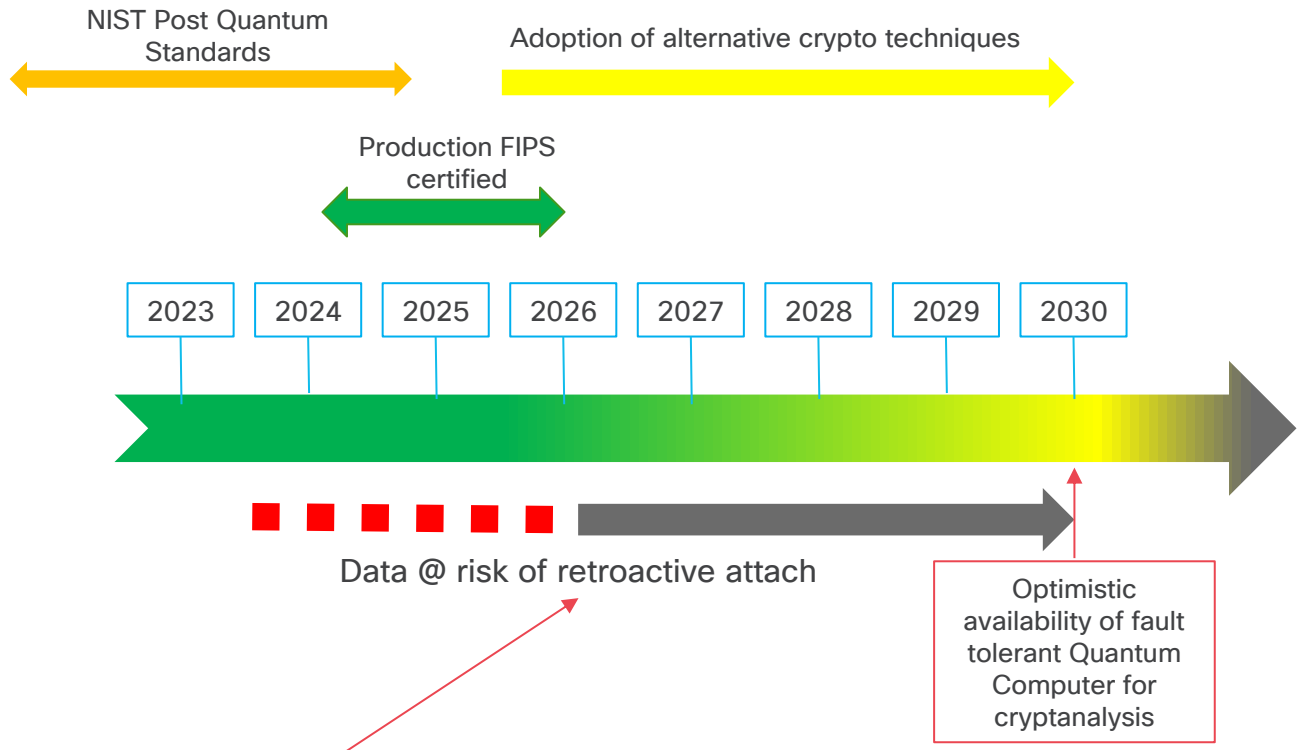
- Capture data encryption keys -> decrypt secured data
- Break secure boot – “sign” altered images -> malware
- Spoof endpoints – I can become you -> man-in-the-middle attacks & data extraction
- Break remote attestation -> Void anti-counterfeit checks (such as HW ID verification)

# Is It a Real Threat?

# Quantum race




Forecasting timelines of quantum computing, Dec. 2020
https://arxiv.org/pdf/2009.05045.pdf

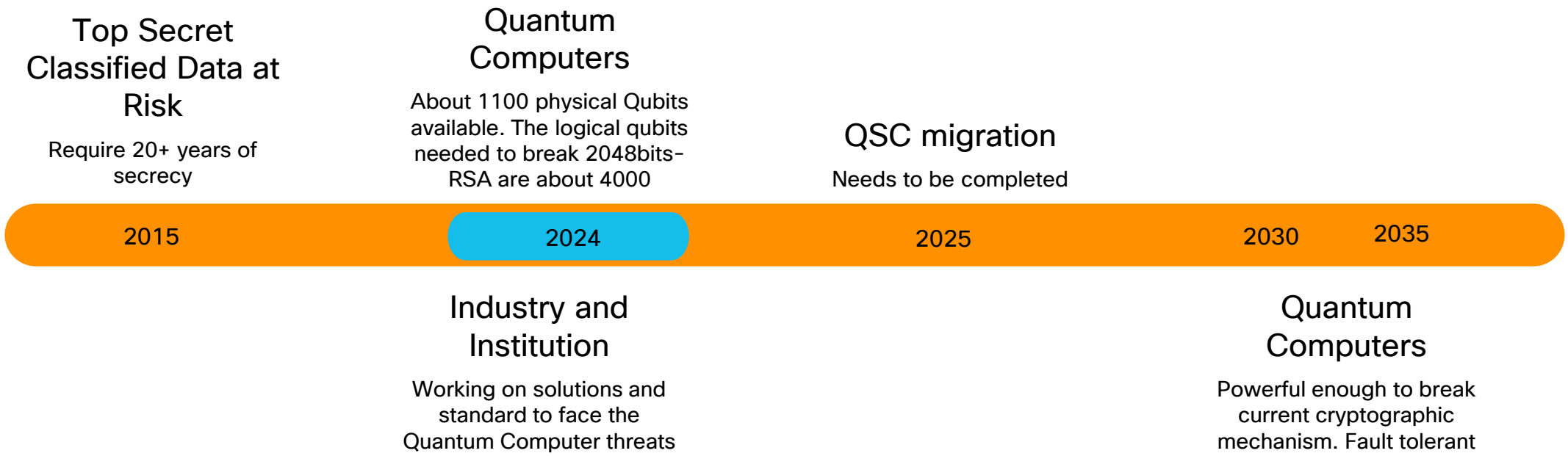



Some customers requires data protection for more than 10 years

# Asymmetric cryptography threat: harvest now, decrypt later

Asymmetric cryptogrphy relies on the generation of mathematically related **public/private** key pairs. Quantum Computers may be able to compute private keys starting from the public one. As a consequence:

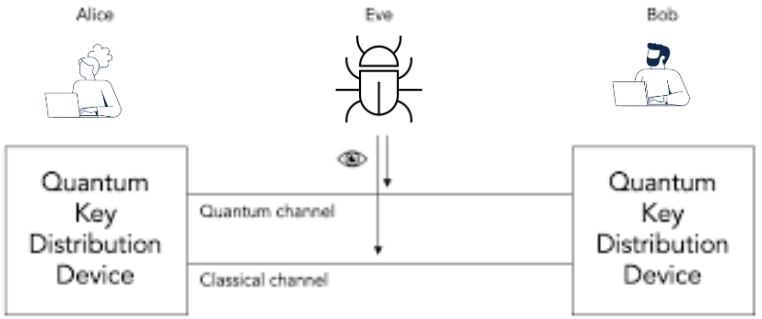
**RSA, DH, ECC are harmed by this technology.**



# Possible Solutions

# Post quantum security remediation

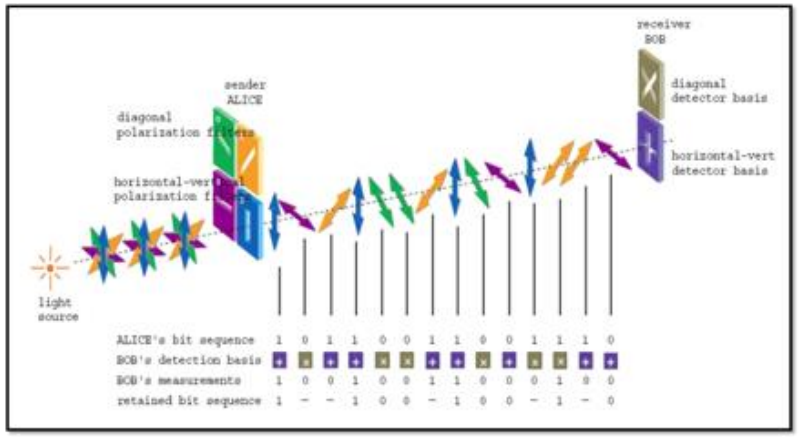
- Quantum key exchange (QKD)
  - *Rely on quantum physics to generate and distribute a shared secret (secure keys)*

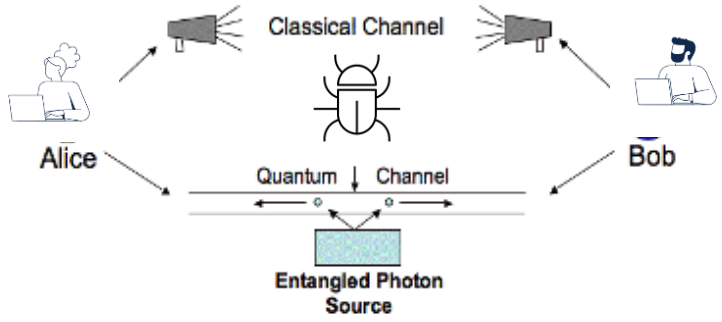



- Post Quantum Cryptography
  - PQ secure key exchange and signature alghos

# Quantum Key Distribution

- A large number of QKD implementations and protocols (10+) have been proposed.
- Commercial implementations have till now focused on:
  - Discrete Variable Direct transmission (BB84 and B92)
  - DV-QKD is discrete, as it's encoded in a discrete property of the single photon, for example polarization; it's a light switch, it can be ON (1) or OFF (0).
- But now also appearing examples of :
  - Entanglement based Discrete Variable Measurement Device Independent (MDI)-QKD (E91)
  - Continuous Variable  with Gaussian modulation
  - CV-QKD is continuous, as it's encoded in a continuos property of the light field, specifically it's amplitude and phase; it's a smart dimmer switch that can be set at different amplitudes




Practical implementation rely on an untrusted intermediate node for entanglement detection (Time Reversed Measurement Device Independent)

# Discrete Variable Quantum Key Distribution: How does it work?

BB84 Example

- Photon polarization is used to transfer information.
- The receiver uses beam splitters to determine the polarization of each photon but must guess which beam splitter to use for each one.
- Afterward, the receiver informs the sender which beam splitter was used for each photon in the sequence. The sender then compares this information with the sequence of polarizers used to send the photons.
- Photons read with the incorrect beam splitter are discarded, and the remaining sequence of bits forms a unique optical key.
- To check for eavesdropping, Alice and Bob compare a predetermined subset of their remaining bit strings. If an eavesdropper like Eve has gained information about the photons' polarization, it introduces errors in Bob's measurements.
  - A principle of quantum mechanics is that measuring a particle's property alters that property.
- Error rate measurements are used to determine the security of Quantum Key Distribution (QKD).

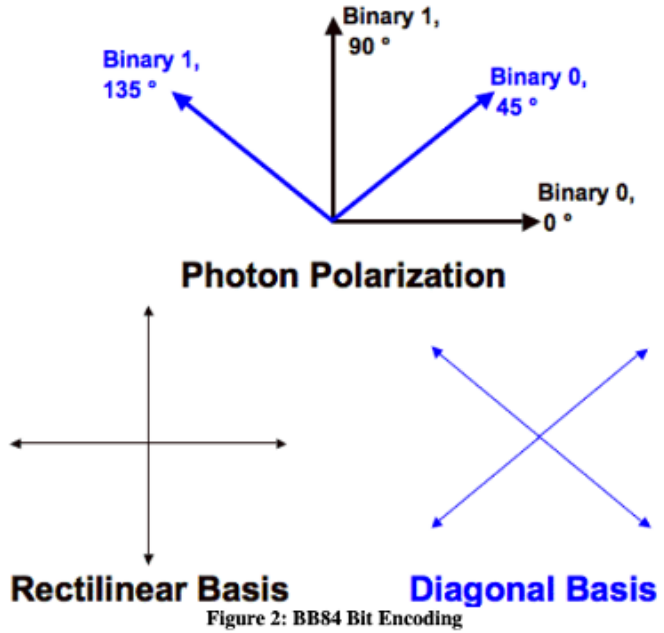


Figure 2: BB84 Bit Encoding

| Alice's bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| Alice's basis | + | + | X | + | X | X | X | + |
| Alice's polarization | ↑ | → | ↖ | ↑ | ↖ | ↗ | ↗ | → |
| Bob's basis | + | X | X | X | + | X | + | + |
| Bob's measurement | ↑ | ↗ | ↖ | ↗ | → | ↗ | → | → |
| Public discussion | | | | | | | | |
| Shared Secret key | 0 | | 1 | | | 0 | | 1 |

# Continuous Variable Quantum Key Distribution: How does it work?

- The fundamental protocol for QKD using CV-QKD architectures is the **GG02 protocol**:
  - Alice **preparation**: for each signal she wants to send, Alice sends a map to Bob of random numbers Q ( amplitude) and X (phase)
  - **Transmission** (Quantum Channel): Alice sends very weak signals (to be in quantic regime) . The signal gets also weaker during the propagation; thus, the map gets blurry.
  - Bob **Measurement** (Decoding): Bob randomly chooses to decode either the X or the Q, he, differently from DV-QKD, does not get either 1 or 0 but a number, for instance X=3.14.
  - Basis **reconciliation** and shifting: Now both Alice and Bob have a random set of numbers (Xa,Qa) and (Xb,Qb), similarly to what happens in BB84,Bob tells Alice, over a classical channel, which quadrature (X or Q) he had measured, and Alice tells him which ones to keep. Now they have a smaller subset of data, that is very similar but not identical.
  - **Parameter Estimation**: they sacrifice a portion of their data and calculate the noise between their numbers, if it' higher than expected, there was an eavesdropper, they can thus decide to either abort the protocol or to keep it and now they have a precise estimate of how much information Eve could have.
  - Information reconciliation: the problem is that due to normal noise, the parameters are similar but not identical, they need to fix this through **Reverse reconciliation**
- Error rate measurements are used to determine the security of Quantum Key Distribution (QKD).

# Continuous Variable Quantum Key Distribution issue

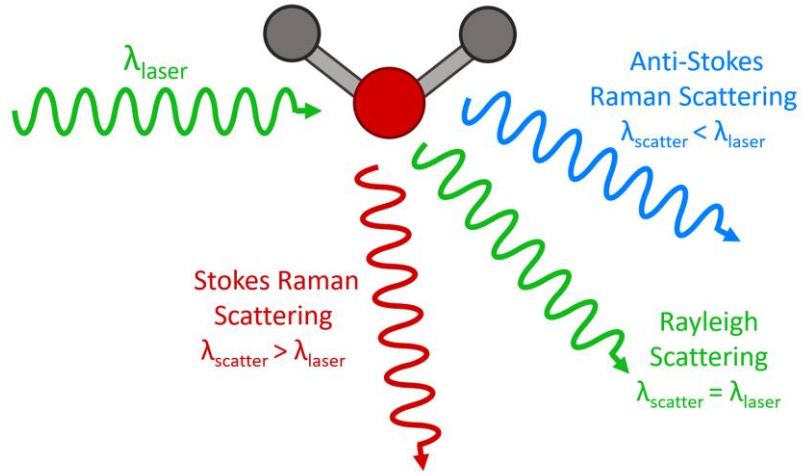
- Eve can perform what is called a **Photon Number Splitting (PNS)** attack.
- Basically, Eve intercepts a **relatively small number of photons** from a light beam that Alice sends (10 out of 10000), from Bob prospective that is normal (light loses power throughout the propagation in a fiber) but now **Eve has a perfect copy** of the photons that Alice sent, she can do this multiple times as much as Alice continues to send light beams to Bob and recreate the secret key, **remaining completely invisible**.
- However, they can use powerful error correction algorithms; Alice sends a ‘parity check’ to Bob over public channel, so Bob can fix his data to match Alice’s. However now Eve has access to that small amount of information.
- Alice and Bob now share a long, identical string of numbers, they know how much information Eve has, because they already calculated noise difference between the two datasets and they know about the ‘parity check’ they leaked earlier.
- They then ‘shrink’ their string into a shorter one using a cryptographic hash function, this function is designed to ‘distill’ the randomness, and they choose that this new string has to be the length of the original string minus the information that Eve might have from the knowledge of the ‘parity check’.
- The mathematical properties of the hash function makes Eve partial knowledge useless; this process is called **Privacy Amplification**.

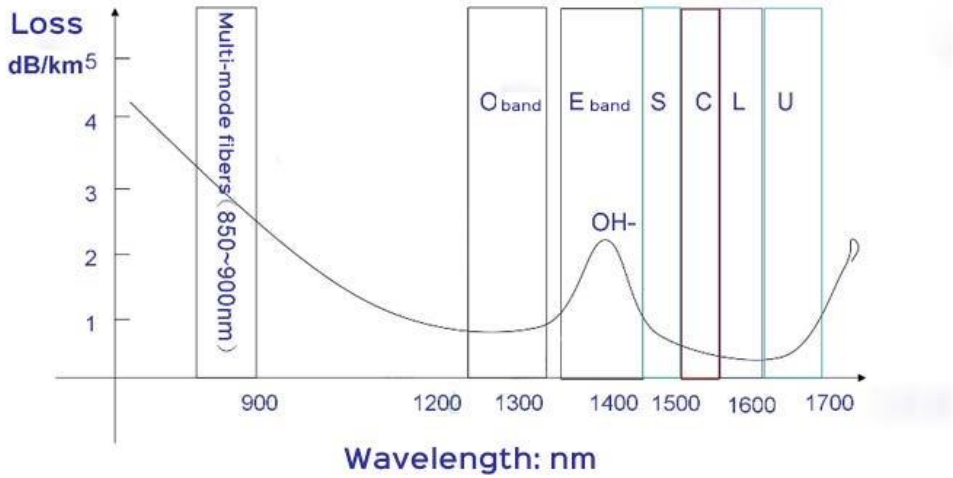
# Drawbacks on QKD

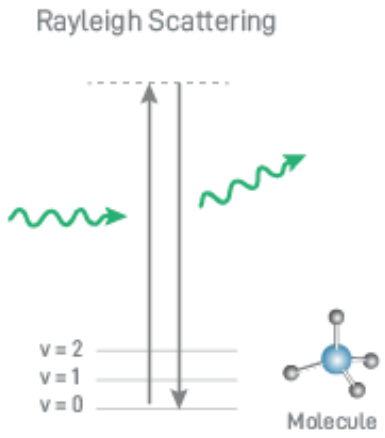
- No interop nor standard
- Requires dedicated HW at each secure endpoint.
  - Single photon emitter and receiver (DV-QKD)
  - Gaussian Source (CV-QKD)
- Required a noiseless dedicated quantum optical channel.
- Key generation rate drop “exponentially” with distance
  - Commercial QKD implementation requires to regen at about 100km on dark fiber.
  - New implementation using aka “twin-field” QKD is promising longer distances up to 600km
- Same implementations showed weakness to counter detector side-channel attacks.
- Address only key exchange

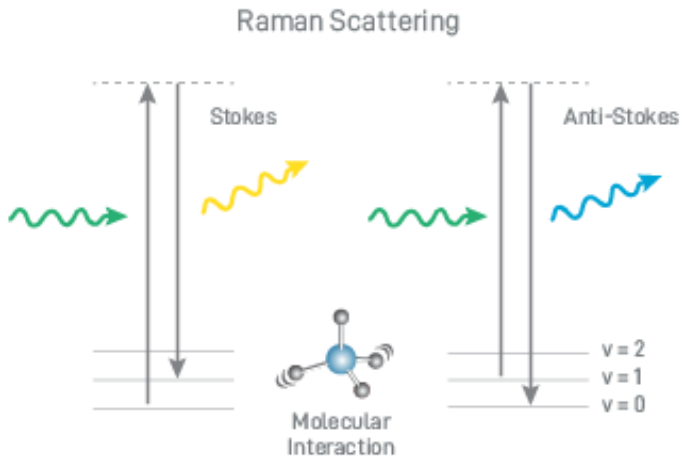
# Challenges in mixing quantum and classical channels

- Scattering effects on classical channels generates spurious photon across the spectrum
- Classical channels traditionally use C Band (1530–1565 nm) and L Band (1565–1625 nm)
- Quantum channel need to be moved to O Band (1260–1360 nm) where injected noise is limited
  - Fiber loss higher (about .5dB/km)



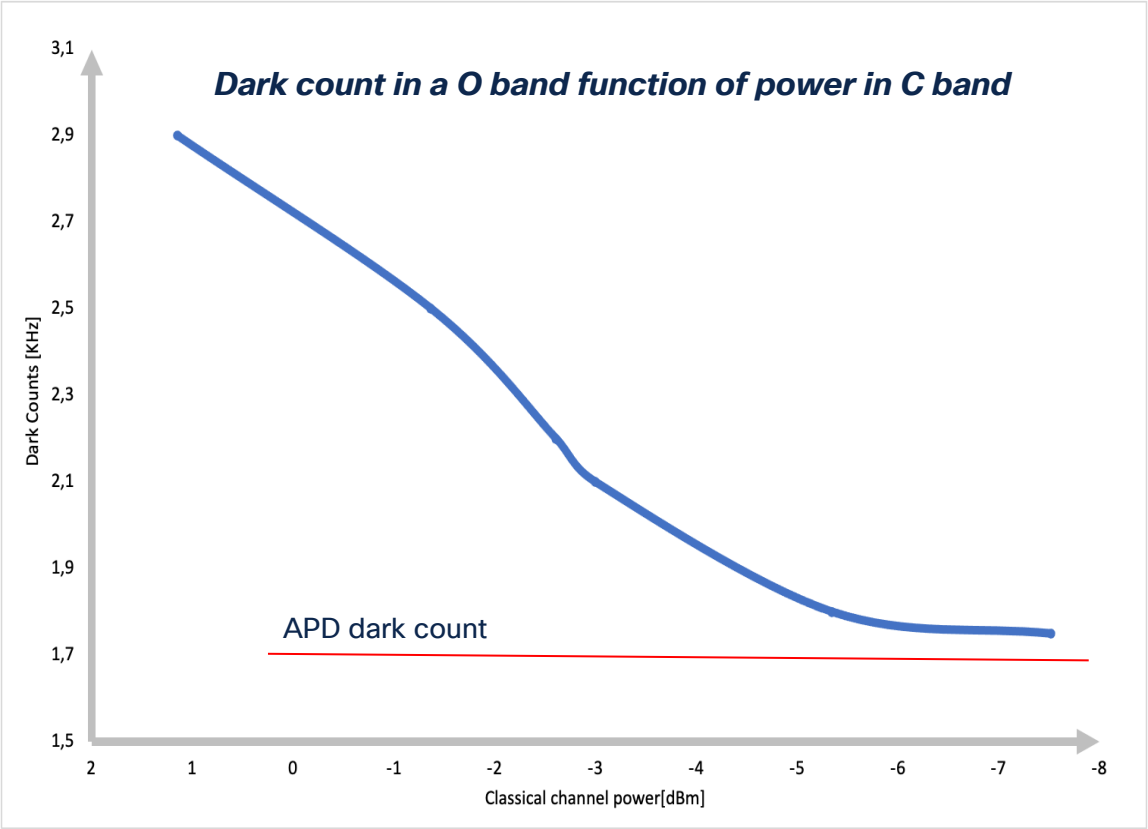



# Mixing quantum and classical channels

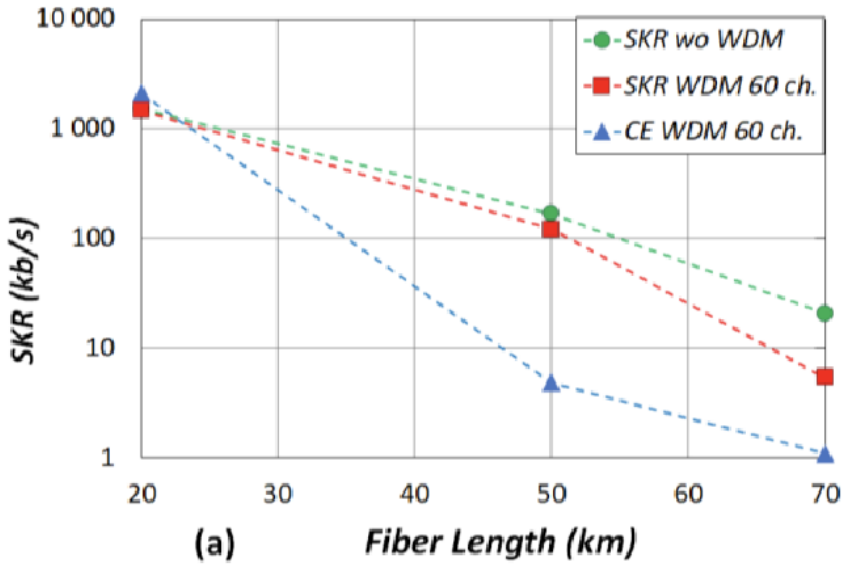
- QKD successfully operated in O band up to 70km with single classical channel in C band
- To reduce the injected noise in the quantum channel, the classical channels power must be reduced below -4 dBm
- Such limit impacts the SNR and the classical bandwidth capacity/reach is heavily affected (4.8T vs 76Tb over 100km distance)




*Quantum channel at 1310 nm filtered @ 50GHz*

# Solution to reduce noise in mixed configurations

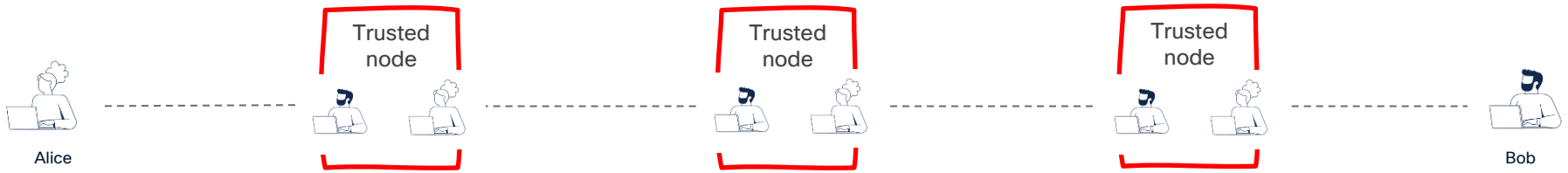
- A time gated filtering on quantum channel is a proposed alternative approaches to reduce noise
- The bandwidth capacity for classical channels decreases by half.
- The QKD distance (secure key rate vs. distance) remains heavily reduced.



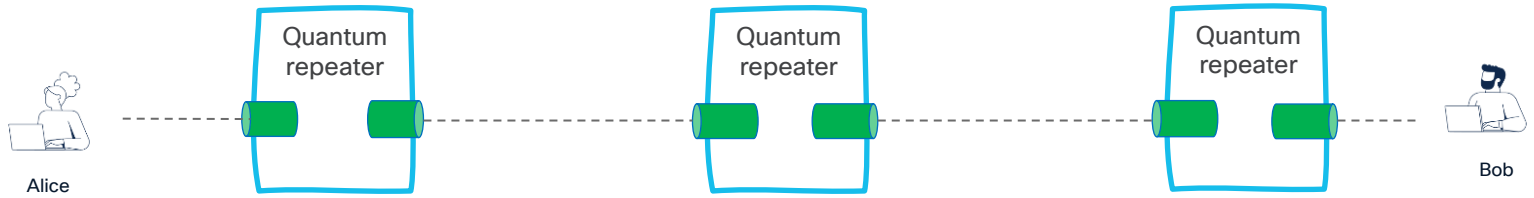

* Co-propagation of 6 Tb/s (60*100Gb/s) DWDM & QKD channels with ~17 dBm aggregated WDM power over 50 km Standard Single Mode Fiber
P. Gavignet (1), F. Mondain (1), E. Pincemin (1), A. J. Grant (2), L. Johnson (2), R. I. Woodward (2), J. F. Dynes (2) and A. J. Shields (2)

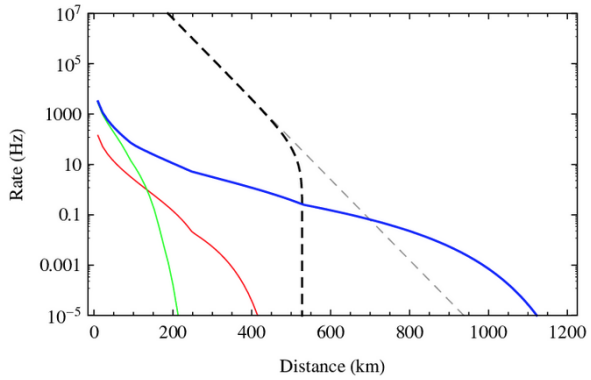
# Addressing QKD Distance Limitations on Fiber

- Chain of trusted repeater
  - Key distribution channel or data traffic re-encrypted in each segment




- Chain of Quantum Repeater
  - Requires either quantum error correction or quantum memory




An efficient quantum light-matter interface with sub-second lifetime

Entanglement distribution rate for quantum repeater versus single-photon distribution rate through direct transmission.

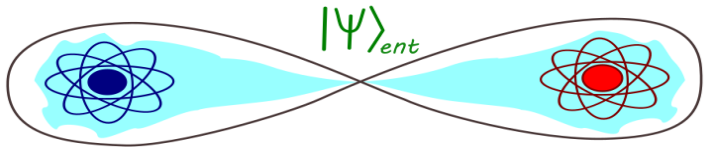
- Dashed lines correspond direct transmission (Gray: no dark count, Black: dark count probability of 10−9 considered).
- Solid lines correspond to quantum repeater with different memory parameters (lifetime + efficiency). Red: 0.2 s + 16% (Radnaev el al. in 2010 [12]), Green: 3.2 ms + 73% (Bao et al. in 2012 [16]), Blue: 0.22 s + 76% (result of this paper).

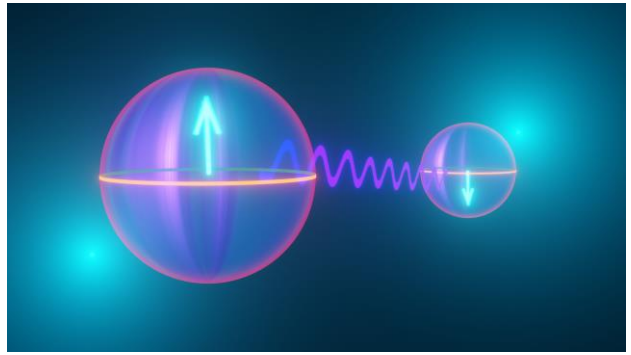
https://arxiv.org/abs/1511.00407

# Quantum repeater: let's use the power of quantum technology

Entanglement (strange correlation)

- A term to describe the quantum state of two or more particle that cannot be described independently from each other.



- Qubits can be entangled
- A measurement of one qubit will affect instantaneously the state of other qubit independently from the distance without direct interaction





cisco

# Quantum repeater: how it (will) works

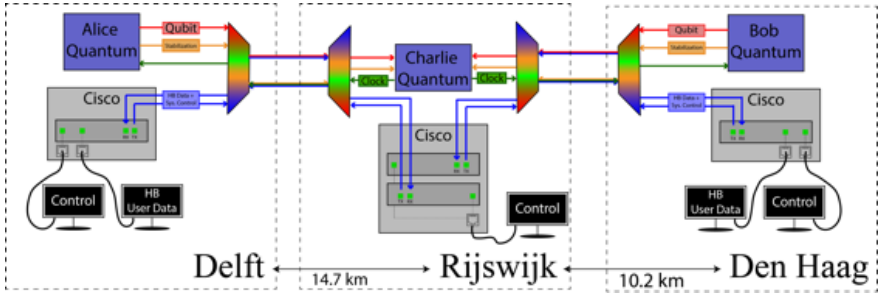
- It is based on concept like Quantum state Teleporting:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Assuming we can generate two remote entangled particles in particular state called “Maximally entangled Bell state” (EPR pairs), quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and trasmissions of 2 classical bits

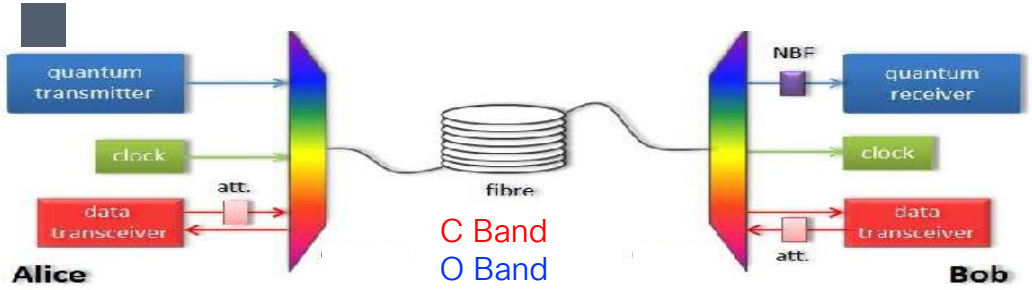
# Cisco activities on QKD

- Field demo with time-bin MDI-QKD w/Qutech
  Quantum channel and classical channel on same fiber

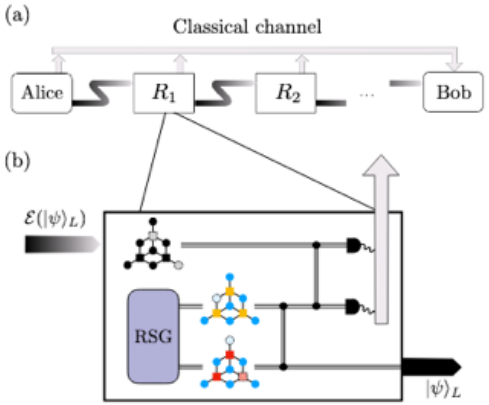



Deployed MDI-QKD and Bell-State Measurements Coexisting with Standard InternetData and Networking Equipment

- Interop test on Cat8k and NCS platform
  - IDQuantique, TQ , QTI, Qbird
- Quantum and classical channel mix
  - Up to 70km successfully tested with a single classical channel
  - Kicked off a university collaboration for modeling




- Study on CV-QKD and “all photonics one way quantum repeater”
  - Based on cluster state quantum error correction
- Two new demos with latest QKD technology under development for next Cisco Live




https://arxiv.org/pdf/2210.10071.pdf

# Cisco Strategy

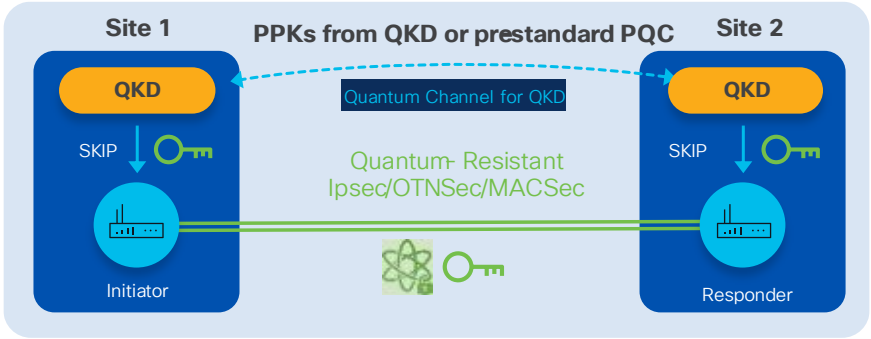
# Getting ready to post quantum security

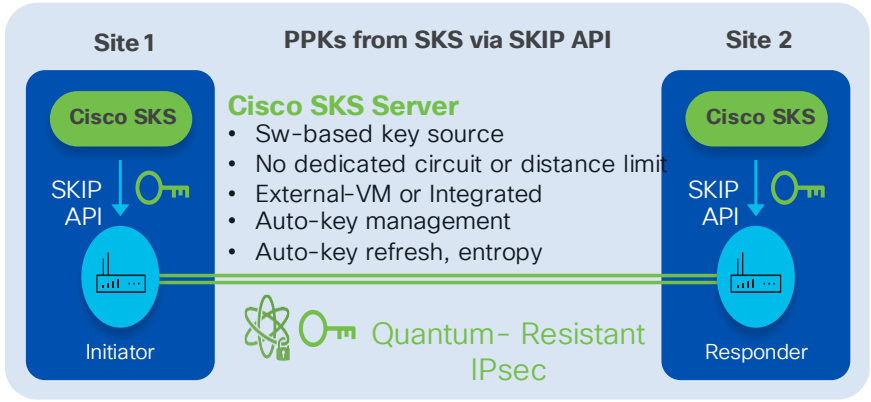
Short term (Today):

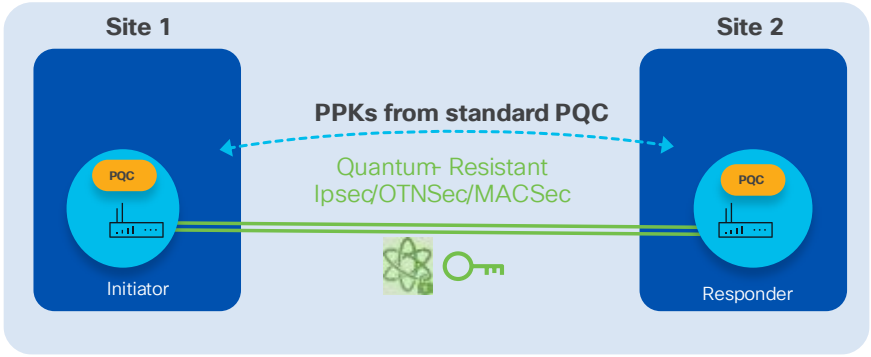
- RFC 8784 – Mixing Preshared Keys in IKEv2
- Cisco Security Service engine with seed transferred using McElice PQ algho
- SKIP (Secure Key Import Protocol) – Enable third party Secure Key Service (QKD or pre standard PQC)

Long term (CY25/26):

- Enable NIST approved PQC alghorithm to enable secure PQ
  - Key exchange and Digital signature

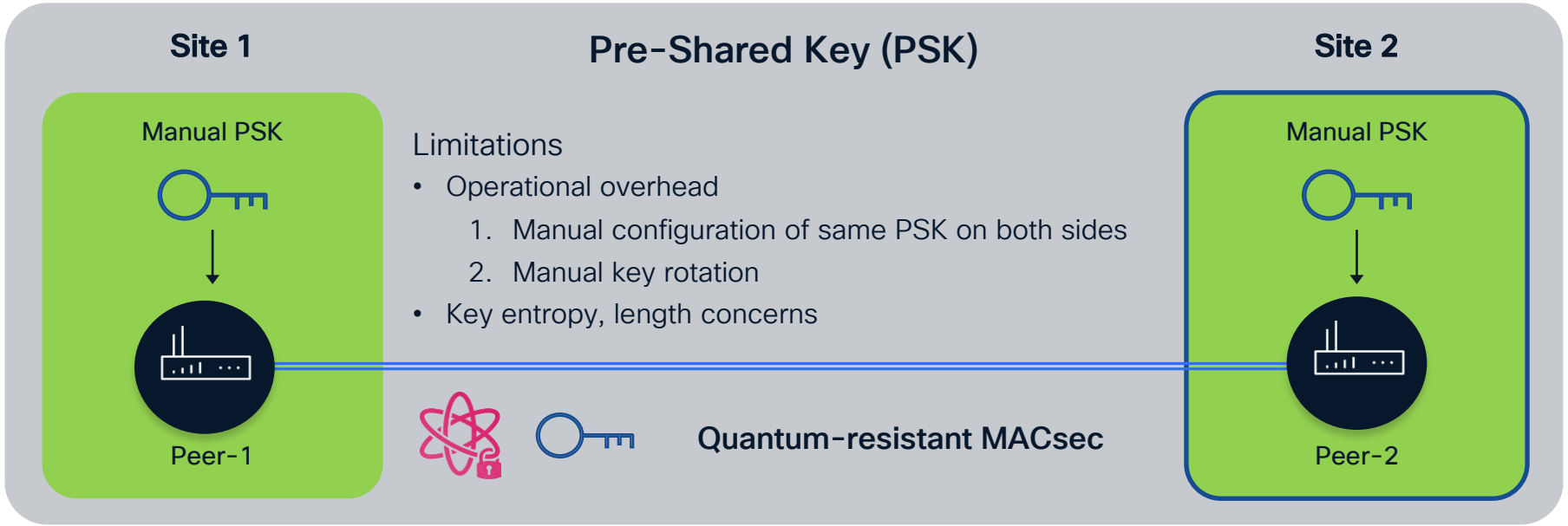


# Quantum-safe MACsec

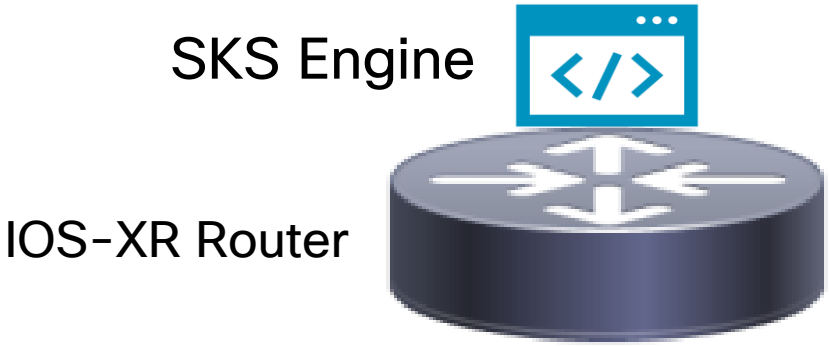
Pre-shared key (PSK) option

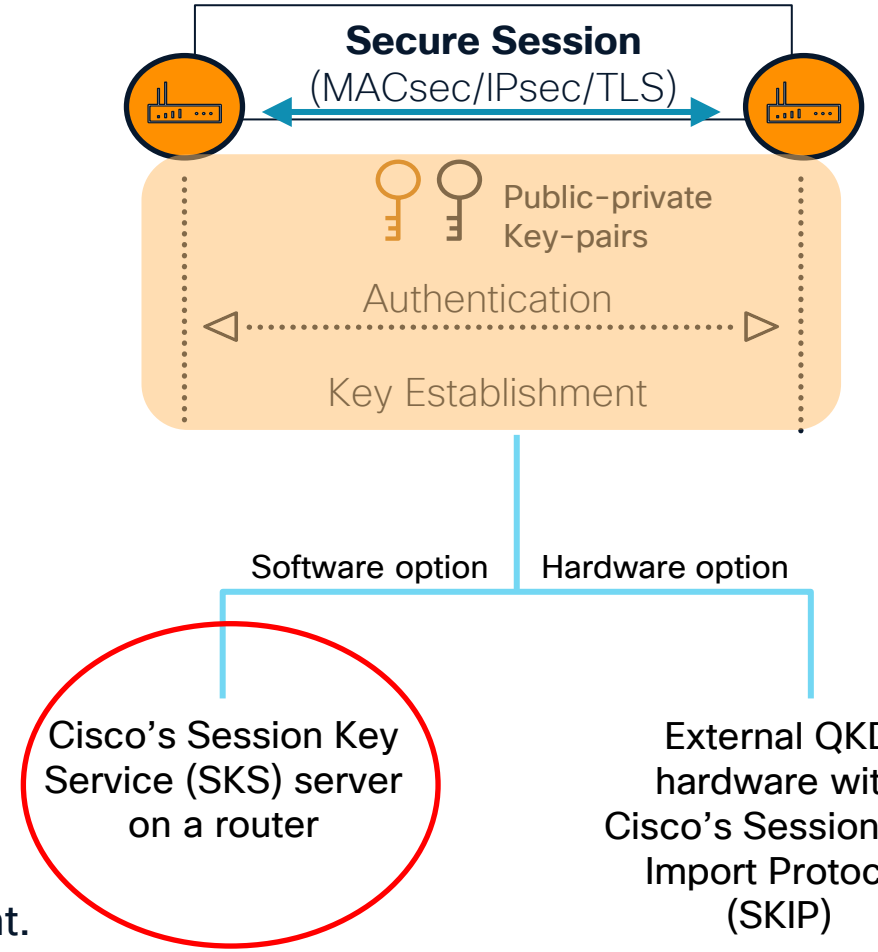



1. MACsec with PSK option is already supported and used by customers.
2. There is no need for additional hardware (like QKD*) or software upgrade.
3. Quantum-safe as this is based on symmetric cryptography which is quantum-resistant.

*Quantum Key Distribution

# Cisco Session Key Service overview

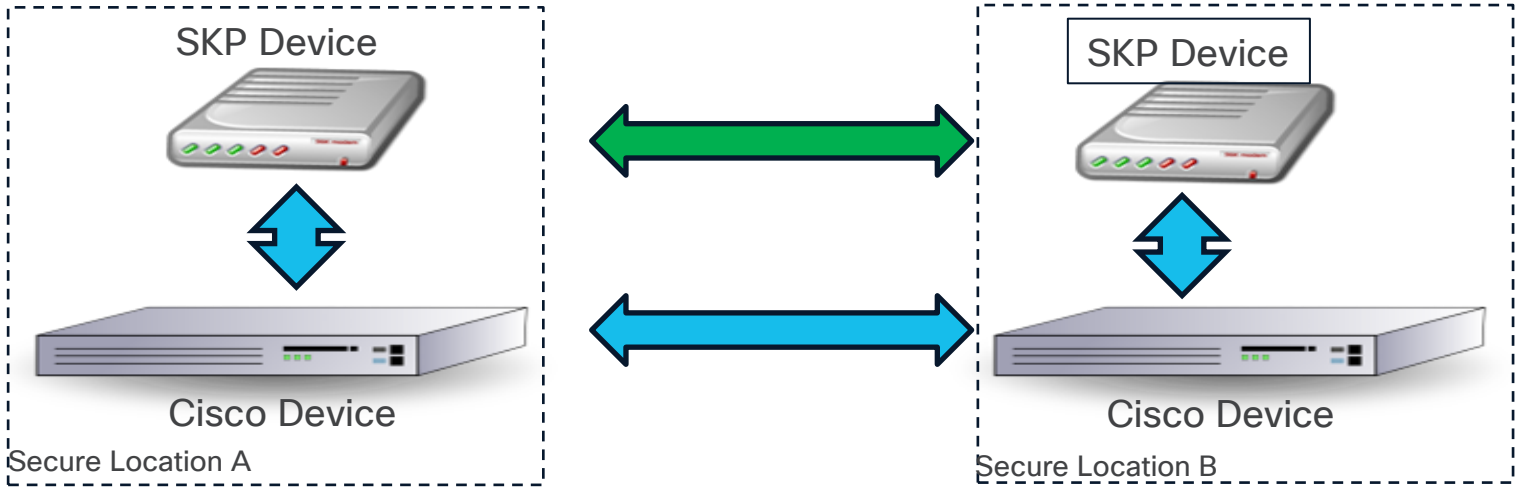



- SKS engine on the router generates the keys.
- No additional hardware required.
- The SKS engine must be seeded with the same seed on both the peers.
- The seed is protected by McEliece cryptosystem which is quantum-resistant.
- Only key-id is sent on the wire, and the peer derives the key from its local SKS engine.

# Cisco SKIP protocol

- Secure Key Integration Protocol (SKIP) enables Quantum-Safeness to Cisco equipment




*Quantum-Safe keys are provided to Cisco device by Security key provider (SKP) devices*

- Already shipping on XE, NX-OS and XR platforms

# Post Quantum Cryptography algho status

Government and Industry Actions

**February 24, 2016:**

Announcement and outline of NIST's call to submissions of PQC algorithms

[...]

**August 24, 2023:**

NIST issued draft standards with request for comments for Kyber, Dilithium and SPHINCS+

**August 13, 2024:**

NIST issued the first finalized Post Quantum Encryption standards ML-KEM, ML-DSA, SLH-DSA

(FIPS 203-205)

**March 11, 2025:**

HQC Announced by NIST as a 4th Round Selection as backup to the standard ML-KEM





**Table 4.** Algorithms to be Standardized

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| CRYSTALS–KYBER | CRYSTALS–Dilithium |
| | FALCON |
| | SPHINCS+ |

**Table 5.** Candidates advancing to the Fourth Round

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| ~~BIKE~~ | |
| ~~Classic McEliece~~ | |
| HQC | |
| ~~SIKE~~ | |

FIPS available

FIPS coming soon

# Conclusions

# QKD vs. PQC

QKD challenges:

- *Requires dedicated HW at each secure endpoint*
- *Mandate a noiseless optical quantum channel*
- *Distances are limited. Beyond trusted regen/channels are needed*
- *No interop, nor standard so far*
- *Address only key exchange, not authentication*
- *Weakness to counter detector side-channel attacks due to (non ideal) implementations*

PQC pros:

- *Enable e2e protection without dedicated HW*
- *Simple upgrade of today for crypto model w/o distance/medium limitations*
- *Mandatory to fix also digital signature*

# Walkaway message on PQ security

- Quantum computing might break key exchange and authentication by CY30
  - AES 256 symmetric cipher implemented in HW is not at risk.
- QKD might enable secure key generation/exchange, but
  - Requires dedicated hardware
  - Key generation rate drop “exponential” with distance
- Post Quantum security will be enabled by a SW PQ key exchange and digital signature alghos. The new alghorithms and standard will become deployable by CY25/26.
- Immediate action is reccomended only to secure against retroactive attack threats
  - Cisco already support RFC 8784 and SKIP protocol

# Quantum Learning Map

Explore the bizarre and mind-blowing world of quantum technologies and learn about the ground-breaking research & development advances Cisco is making to become the industry-leader in quantum networking

**START**

Monday, Feb 9 | 3:45 PM - 4:15 PM | Center Stage
**A Quantum Leap in Networking: Cisco's Blueprint for Tomorrow's Infrastructure**
CENETI-1290

Tuesday, Feb 10 | 12:00 PM - 1:00 PM | Session Room A11
**Strategies for a Quantum-Safe Security Transition**
BRKETI-1007

Wednesday, Feb 11 | 5:00 PM - 6:30 PM | Session Room A1
**What is Cisco Doing in Quantum?**
**An Introduction to Quantum Mechanics, Computing, and Networking**
BRKETI-1401

Thursday, Feb 12 | 8:45 AM - 9:45 AM | Session Room A16
**QKD Impact on Optical System and PQC Solution**
BRKETI-3086

Thursday, Feb 12 | 10:15 AM - 11:15 AM | Session Room A16
**Post-Quantum Hybrid PQC+QKD for Crypto Agility**
BRKETI-2667

**FINISH**

Thursday, Feb 12 | 3:00 PM - 4:00 PM | Session Room D508
**Are You Quantum-Ready?**
IBOETI-1061

# Complete your session evaluations

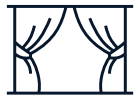
**Complete** a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2025.

**Earn** 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

**Level up** and earn exclusive prizes!

**Complete your surveys** in the Cisco Live mobile app.

# Continue your education



**Visit** the Cisco Showcase for related demos.

**Book** your one-on-one Meet the Engineer meeting.

**Attend** the interactive education with DevNet, Capture the Flag, and Walk-in Labs.

**Visit** the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

**Contact me at**: https://www.linkedin.com/in/mauriziogazzola/

# Thank you

cisco Live !


CISCO