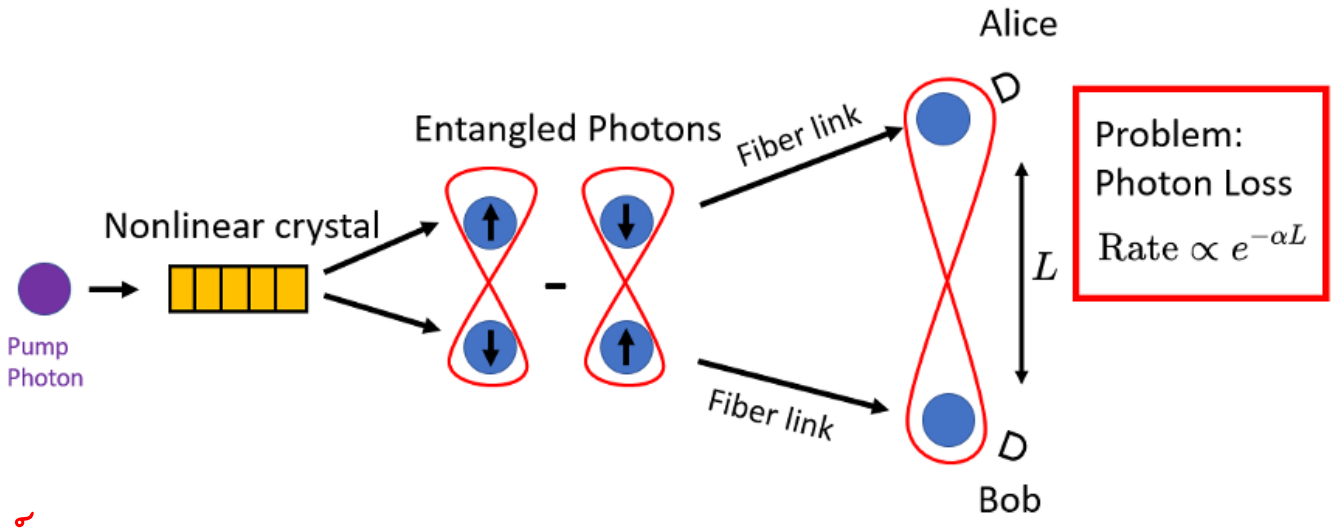
# บทที่ 5 IMPLICATIONS OF QUANTUM COMPUTING ON NETWORK SECURITY




ผู้ช่วยศาสตราจารย์จุฑาวุฒิ จันทรมาลี

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสวนดุสิต

# Security-Concerning Quantum Algorithms

- Shor's Algorithm:
  - factorizes large numbers
  - with quantum compute, Shor's algorithm threatens the security of classical Public Key Infrastructure (PKI) including:
    - Diffie-Hellman (DH)
    - Elliptic Curve Cryptography (ECC), and
    - Elliptic Curve Diffie Hellman (ECDH)
  - The key exchange is at greatest risk


- Grover's Algorithm
  - searches an unstructured database (or an unordered list) for a specific result
  - With quantum compute, Grover's algorithm will threaten the security of AES
  - Immediate recommendation is to increase key sizes

# Y2Q, CRQC and SNDL

- **Years to Quantum (Y2Q)** refers to the unknown number of years before there is are **Cryptographically Relevant Quantum Computers (CRQC)**
- A CRQC can compute prime factorizations and discrete logarithms in polynomial time by Shor's algorithm, thereby rendering public key algorithms all but obsolete
- However, an adversary can capture network traffic *today* in the hopes of decrypting it *later* with a CRQC; this is a **Store Now, Decrypt Later (SNDL)** type of attack, and means that sensitive data is vulnerable *right now* to future quantum threats
  - Sometimes this method is also referred to as **Harvest Now Decrypt Later** (HNDL)

# Grover's Algorithm: Classic vs. Quantum


Classic Search

$f("red\ ball")$ ▶ "Position 5"

Worst Case: $N$ *searches*

---

Quantum Search

$f("Pos\ 2?")$ ▶ "False"

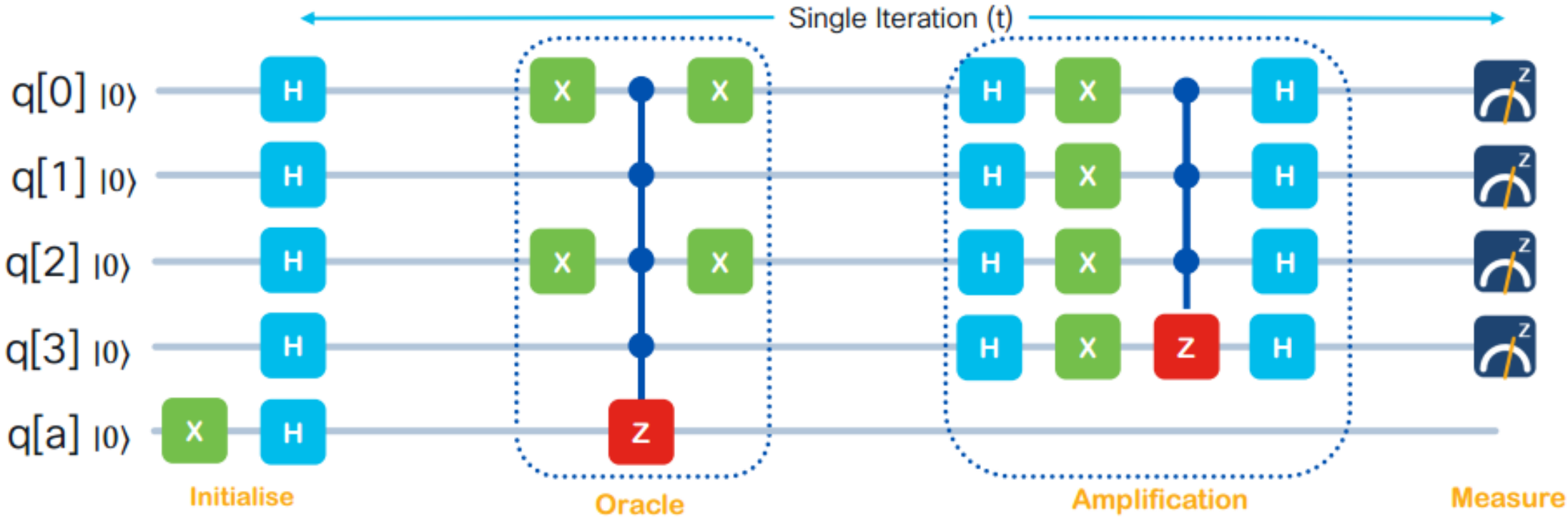
⋮

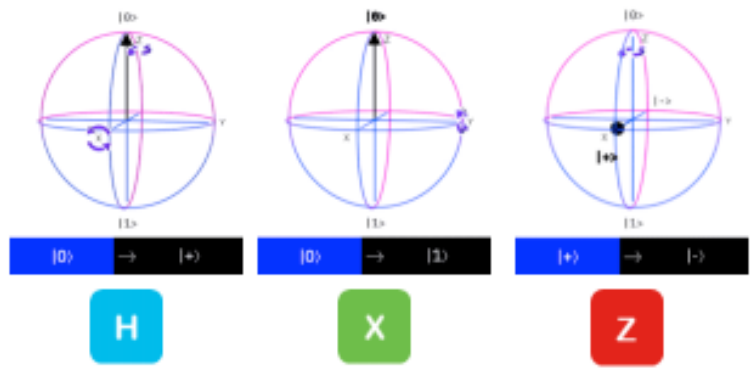
$f("Pos\ 5?")$ ▶ "True"

Worst Case: $\sqrt{N}$ *searches*

- Grover's algorithm uses amplitude amplification to return the correct result with high probability
- As such, with quantum parallelism and interference management, Grover's algorithm becomes quadratically faster than a classical algorithm

# Grover Quantum Circuit


https://www.techscience.com/jqc/v3n4/46224/pdf

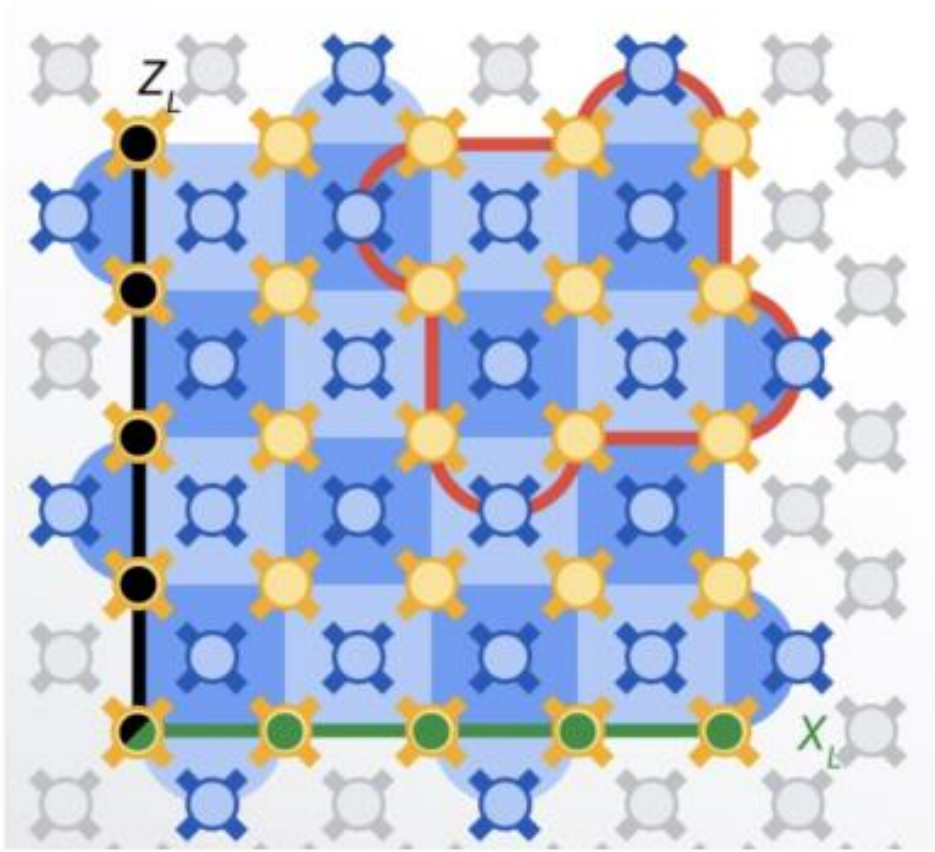
# How many Qubits are required to Break RSA and AES?

- Experts estimate that:
  - RSA-2048 requires a quantum computer with 4,096 **logically-corrected qubits** to be broken
  - AES-256 requires a quantum computer with 6,681 **logically-corrected qubits** to be broken

https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

# How Many Physical Qubits are Required to Produce a Logically-Corrected Qubit?

- Qubits are notoriously fragile and extremely sensitive to the environment and can easily lose coherence (state)
- The logical state of a qubit can be spread over many physical qubits to achieve **Quantum Error Correction**
- In March 2023, Google realized a logically-corrected qubit with just 49 physical qubits
- In December 2023, Harvard scientists achieved the same with just 48 qubits



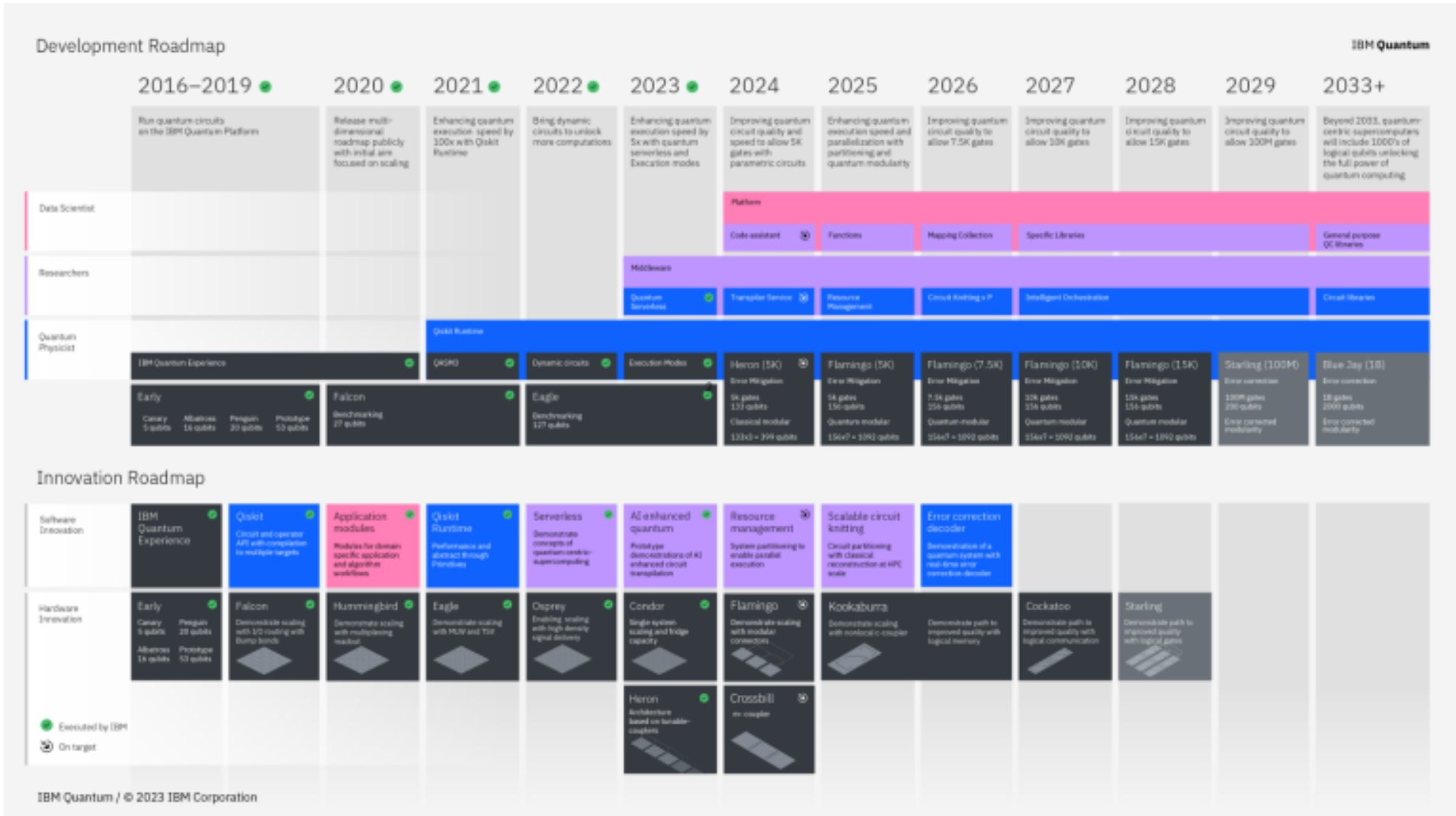

https://blog.google/inside-google/message-ceo/our-progress-toward-quantum-error-correction/
https://thequantumrecord.com/quantum-computing/breakthrough-in-quantum-error-correction/

# So, really...
# How many Qubits are required to Break RSA and AES?

- Let's assume 50 physical qubits for one logically-corrected qubit
- Experts estimate that:
  - RSA-2048 requires a quantum computer with 4,096 logically-corrected qubits to be broken
    - (4096 * ~50) 200,800 physical qubits
  - AES-256 requires a quantum computer with 6,681 logically-corrected qubits to be broken
    - (6681 * 334,050) 334,050 physical qubits
- But remember:
  - Quantum computers are ***increasing*** in size, while
  - Quantum Error Correction circuits are ***decreasing*** in size

https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

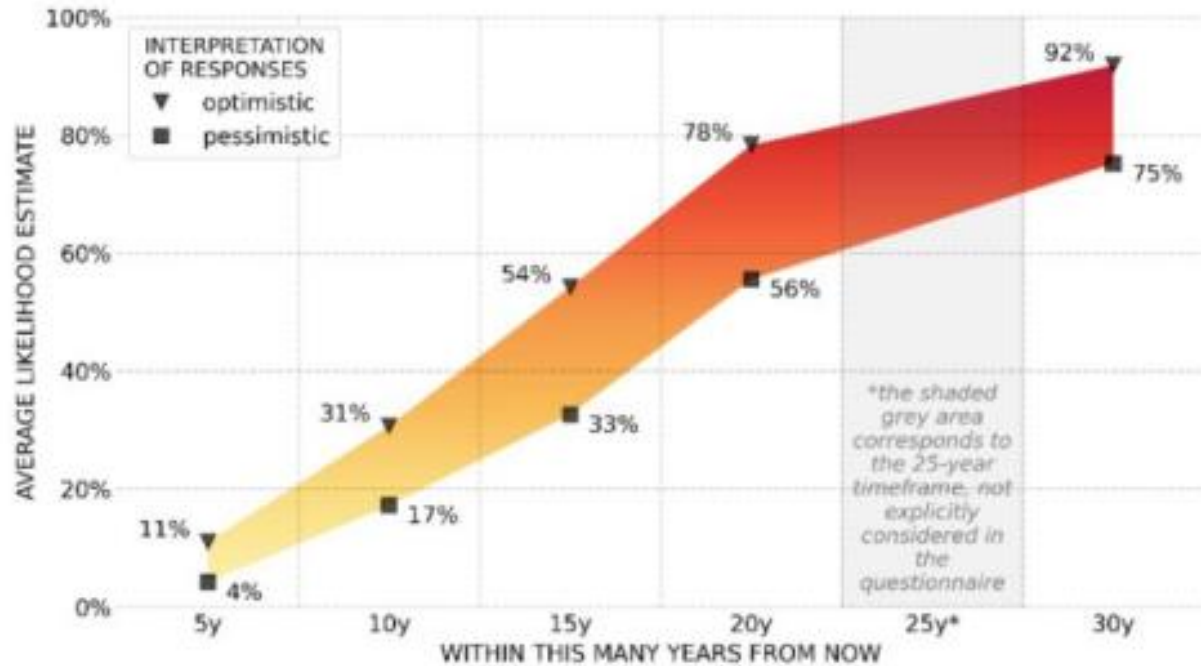
# How Far Off Is That?




https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

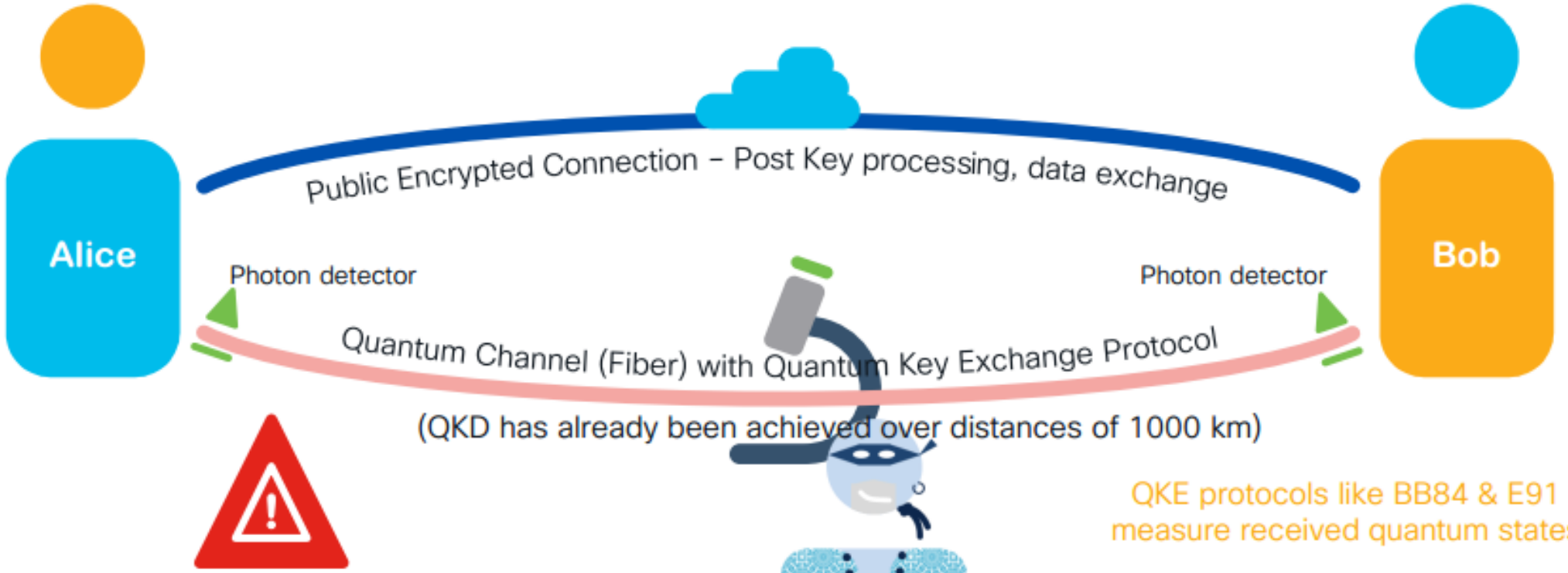
# How Many Y2Q?

- Cloud Security Alliance:
  - April 14, 2030
- Global Risk Institute:
  - ~50% of experts predict 15 years
- White House / NIST
  - “in the not-too-distant future”




https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum/
https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

# Quantum Key Distribution (QKD)



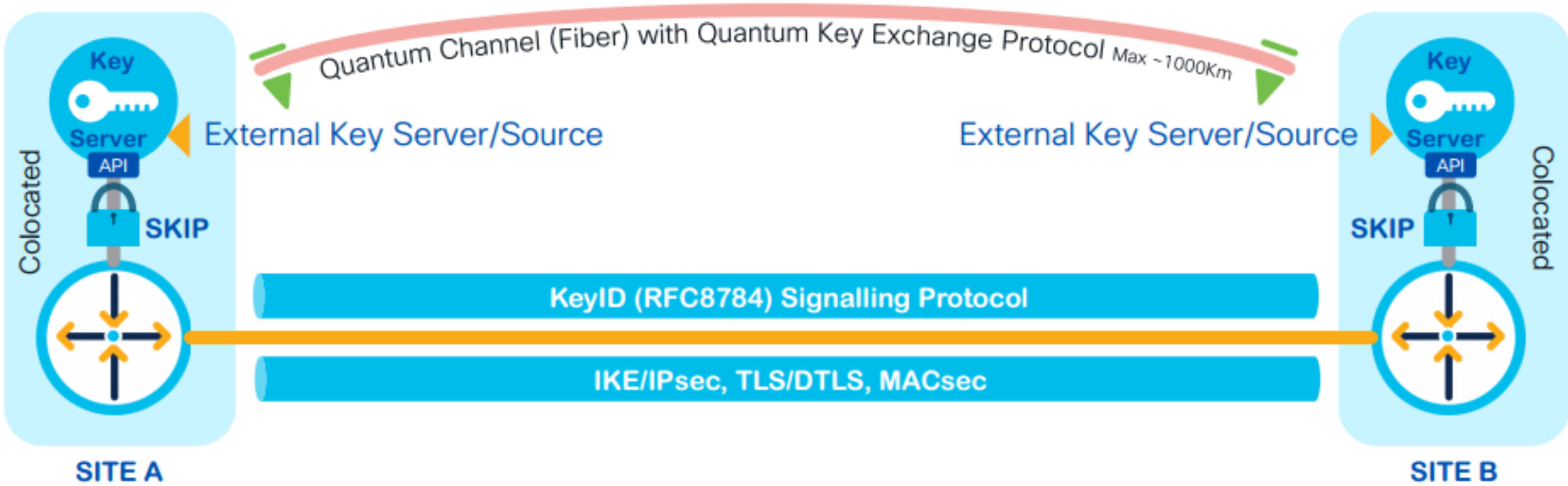

QKD requires a direct connection because current optical switches would destroy the quantum effect. Hence, we need to a Quantum Internet

QKE protocols like BB84 & E91 measure received quantum states

As soon as eavesdropping takes place the quantum channel will change leaving evidence of tampering

https://phys.org/news/2023-06-scientists-km-quantum-key.html

# Secure Key Import Protocol (SKIP)




QUESTIONS
ANSWERS