cisco Live!

# Let's go

The bridge to possible

# Getting ready for Quantum Security and API interaction for Post Quantum Cryptography

Vinay Saini, Principal Architect
Cisco CX

# Agenda

- Quantum Computing  Basics
- Quantum Security
- Quantum and Cisco

# What is Computing

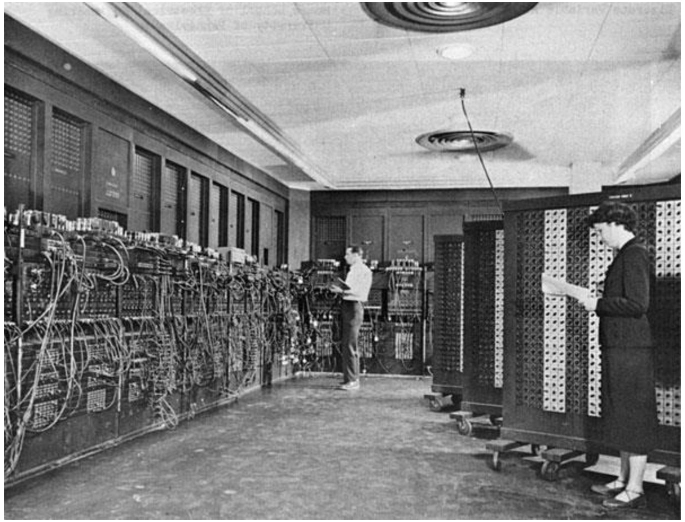
It is a procedure to calculate or determine something using mathematical or logical methods.

Turing Machine

*"Nature isn't classical. If you want to make a simulation of nature you'd better, make it quantum Mechanical"*

Richard Feynman

# Classical vs Quantum Computers



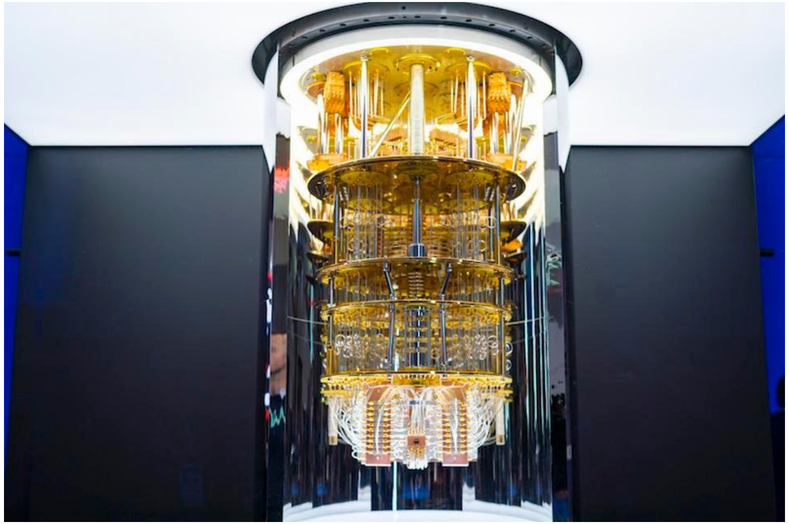
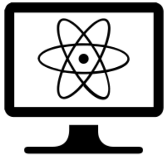


Image Source: IBM Q System One



Vacuum Tube-based early computer

Infancy Stage Quantum Computer

# What is Quantum Computing?

Studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data and solve problems too complex for classical computers

Superposition

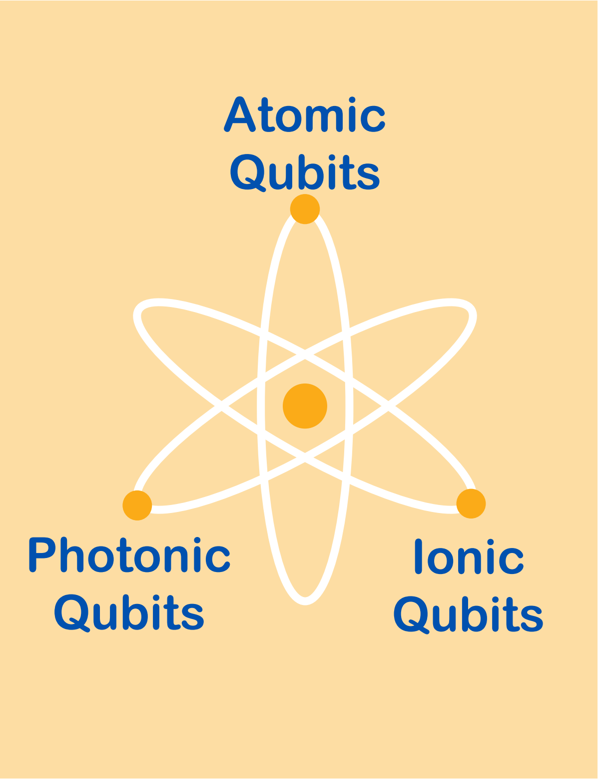
Entanglement

**New Breed of Information Processing**

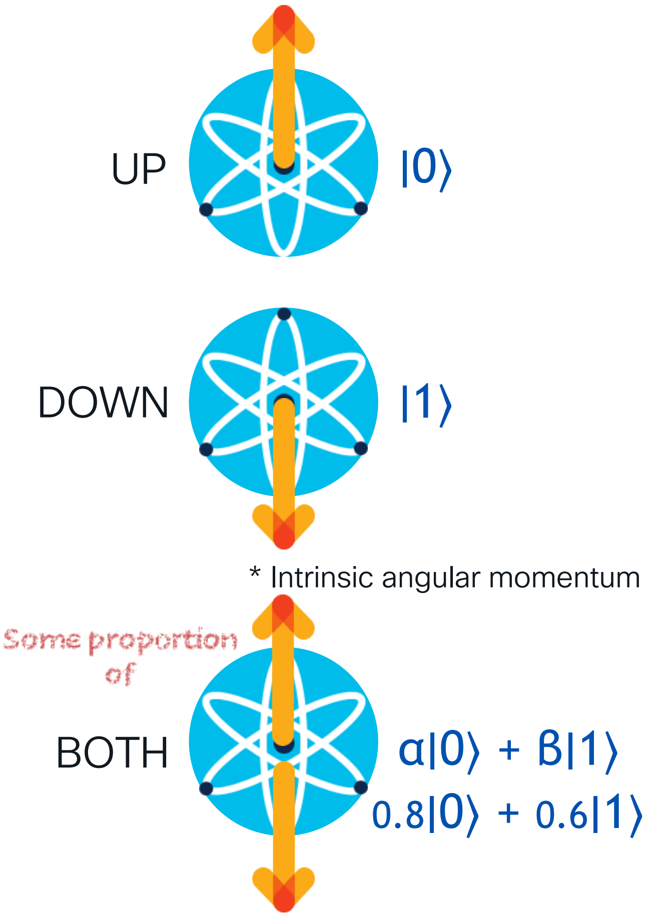
# Qubit

**Qubit**

Two-level quantum mechanical version of a classical data bit




## Electron Qubit "SPIN"*



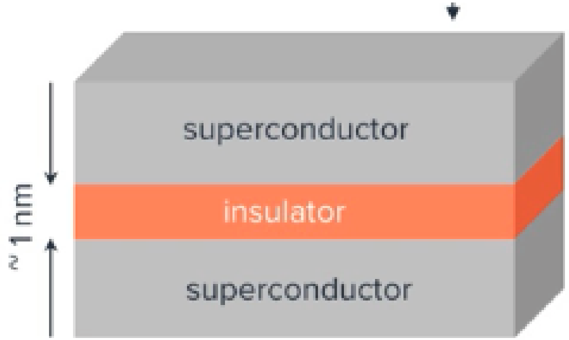

* Intrinsic angular momentum

# Qubit Modalities

Electron and Nuclear Spins based Qubits

Neutral atoms and Trapped Ions based Qubits

Superconducting Qubit





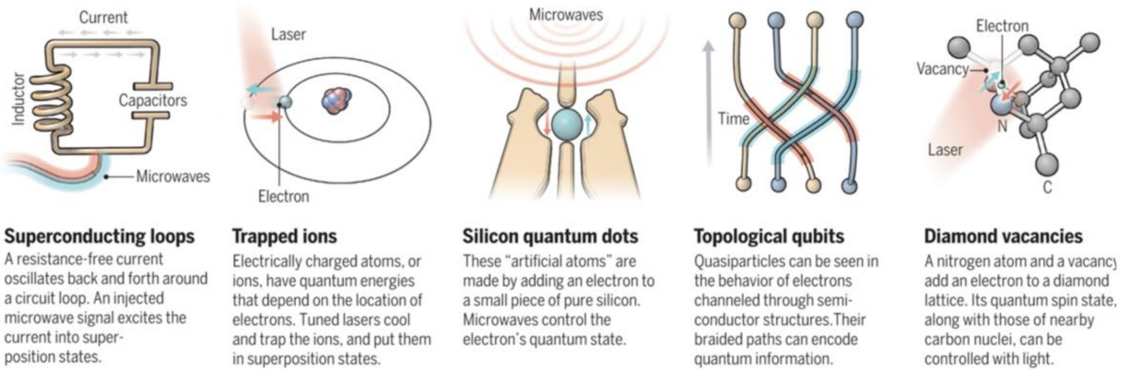



Image source - https://qc-at-davis.github.io/QCC/How-Quantum-Computing-Works/The-Qubit/The-Qubit.html

## Quantum state "Vector 0" or "Ket 0"

(~Like a classic 0 bit)

$$|0\rangle$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Vector 0

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Quantum state general formula

## Quantum state "Vector 1" or "Ket 1"

(~Like a classic 1 bit)

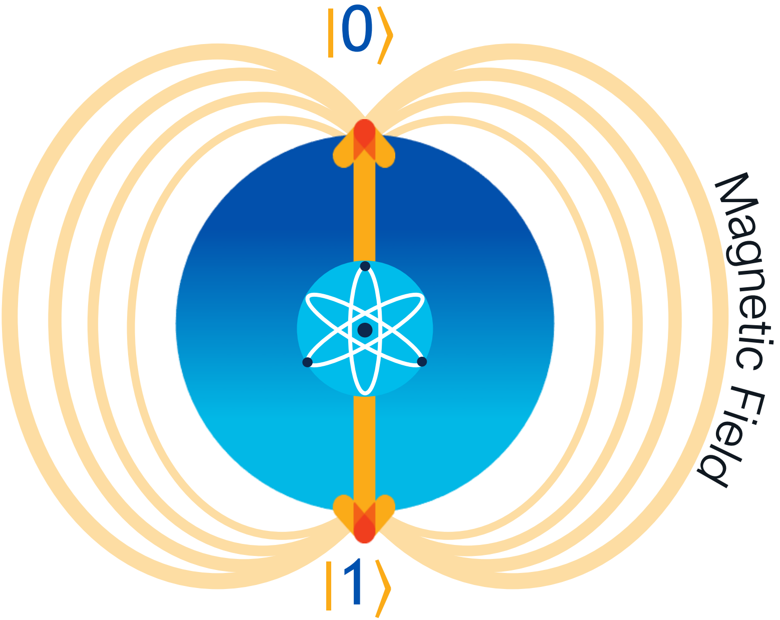
$$|1\rangle$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Vector 1

The state of a classical bit is a number, the state of a qubit is a vector

# Quantum Superposition




As long a QUBIT is unobserved (unmeasured) it is in a SUPERPOSITION of probabilities for Zero and One


The instant a QUBIT is measured, it will collapse into one of the discrete states

# The Power Of Quantum Superposition

Two classical bits

$B_1$ $B_2$

| $B_1$ | $B_2$ |
| --- | --- |
| 0 | 0 |
| 0 | 1 |
| 1 | 0 |
| 1 | 1 |

# states = n
(where n=2 above example)

FOUR independent states.
Only ONE of the combinations exists at any time.

**Quantum power grows exponentially with each extra Qubit**

Two quantum bits

ONE State simultaneously representing all FOUR combinations

( 0 0 ) + ( 0 1 ) + ( 1 0 ) + ( 1 1 )

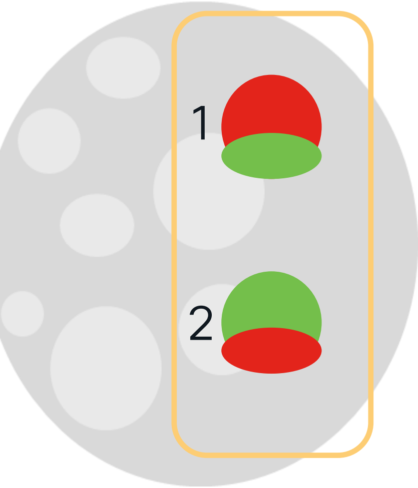
# states = $2^n$

$2^n$ vectors with various probabilities are input to create the single state

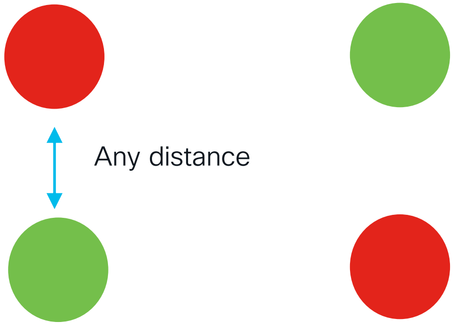
# Quantum Entanglement

## Entangled Qubits

Entangled qubits become a system with a single quantum state




If 1 is RED, then 2nd will be Green




If 1st is Green then 2nd will be red

Same or Different Entanglement is possible

Entanglement is a physical relationship between Qubits where they react to a change in the other(s) state instantaneously regardless of how far they are apart

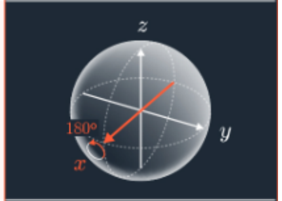
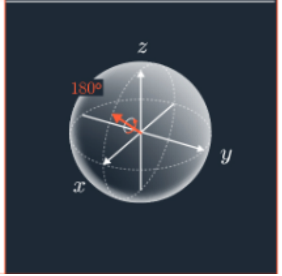
**https://research.ibm.com/blog/whole-device-entanglement

https://science.sciencemag.org/content/365/6453/570

# Classical Gate Operation

| GATE | | CIRCUIT REPRESENTATION | TRUTH TABLE |
|---|---|---|---|
| NOT | The output is 1 when the input is 0 and 0 when the input is 1. |  | Input \| Output<br>0 \| 1<br>1 \| 0 |
| AND | The output is 1 only when both inputs are 1, otherwise the output is 0. |  | Input \| Output<br>0 0 \| 0<br>0 1 \| 0<br>1 0 \| 0<br>1 1 \| 1 |
| OR | The output is 0 only when both inputs are 0, otherwise the output is 1. |  | Input \| Output<br>0 0 \| 0<br>0 1 \| 1<br>1 0 \| 1<br>1 1 \| 1 |

# Quantum Gates

| GATE | CIRCUIT REPRESENTATION | MATRIX REPRESENTATION | TRUTH TABLE | BLOCH SPHERE |
|---|---|---|---|---|
| $I$ Identity-gate: no rotation is performed. | $-\boxed{I}-$ | $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | Input / Output<br>$\|0\rangle$ → $\|0\rangle$<br>$\|1\rangle$ → $\|1\rangle$ |  |
| $X$ gate: rotates the qubit state by $\pi$ radians (180º) about the x-axis. | $-\boxed{X}-$ | $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | Input / Output<br>$\|0\rangle$ → $\|1\rangle$<br>$\|1\rangle$ → $\|0\rangle$ |  |
| $H$ gate: rotates the qubit state by $\pi$ radians (180º) about an axis diagonal in the x-z plane. This is equivalent to an X-gate followed by a $\frac{\pi}{2}$ rotation about the y-axis. | $-\boxed{H}-$ | $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ | Input / Output<br>$\|0\rangle$ → $\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$<br>$\|1\rangle$ → $\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$ |  |

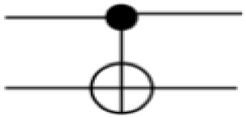
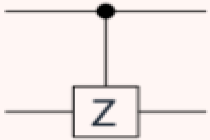
## Matric Multiplication for I gate

$$I|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$I|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Commonly used – creates a superposition state.

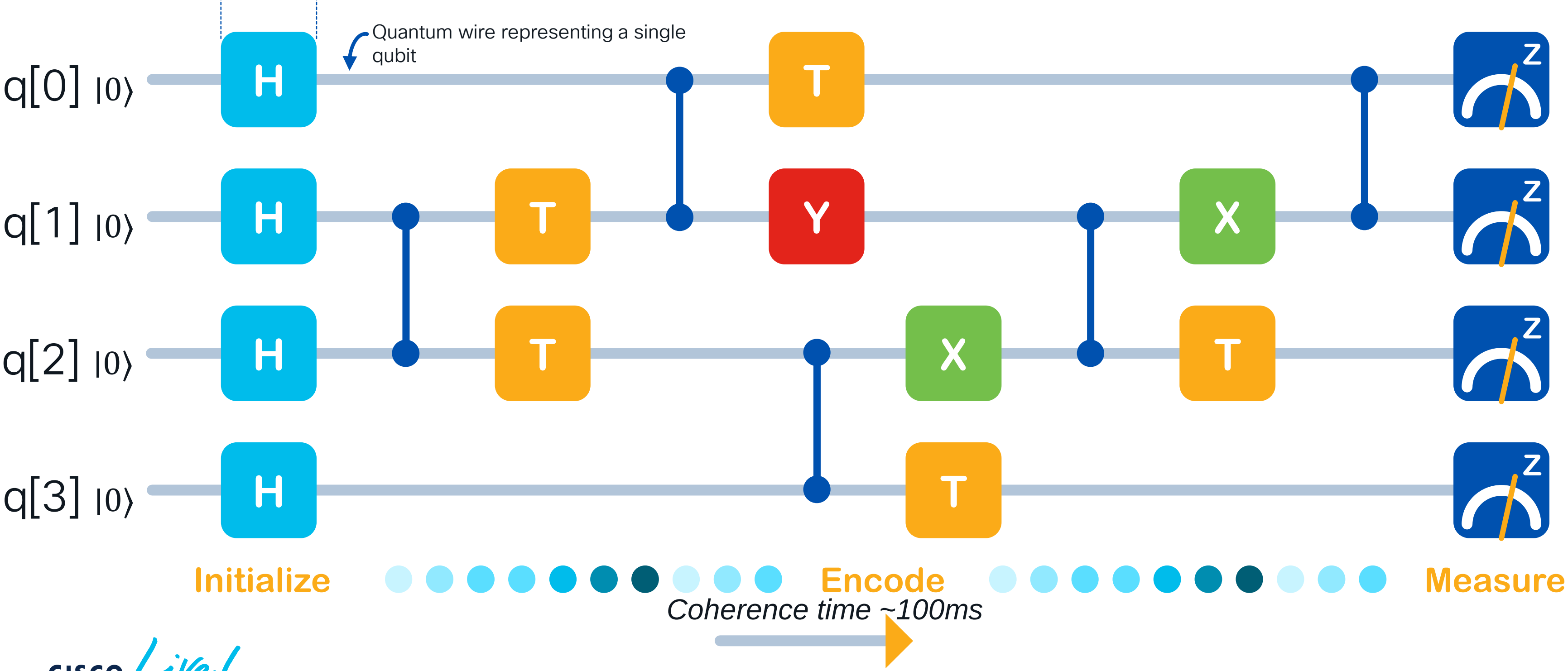
# Quantum Gates – Two Qubit Operation

| GATE | CIRCUIT REPRESENTATION | MATRIX REPRESENTATION | TRUTH TABLE |
|---|---|---|---|
| Controlled-NOT gate: causes an effective X-gate on the target qubit if the control qubit is in state $\lvert 1\rangle$ |  | $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ | Input / Output<br>$\lvert 00\rangle$ / $\lvert 00\rangle$<br>$\lvert 01\rangle$ / $\lvert 01\rangle$<br>$\lvert 10\rangle$ / $\lvert 11\rangle$<br>$\lvert 11\rangle$ / $\lvert 10\rangle$ |
| Controlled-phase gate: causes an effective Z-gate on the target qubit if the control qubit is in state $\lvert 1\rangle$ |  | $cZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ | Input / Output<br>$\lvert 00\rangle$ / $\lvert 00\rangle$<br>$\lvert 01\rangle$ / $\lvert 01\rangle$<br>$\lvert 10\rangle$ / $\lvert 10\rangle$<br>$\lvert 11\rangle$ / $-\lvert 11\rangle$ |

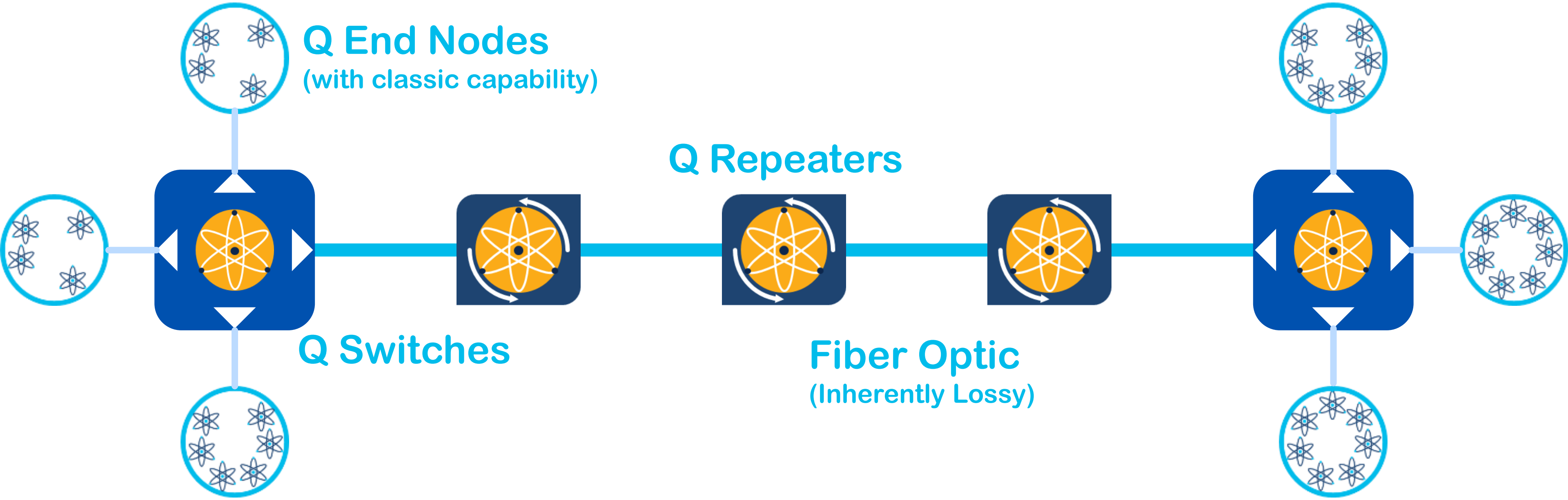
The CNOT is used to entangle two qubits together (Bell State) and is essential in quantum computing/algorithms

# Quantum Circuit = Quantum Operations + Classical Computing

Number of Qubits input must match number of Qubits output



# Components of the Quantum Internet



# Quantum Security

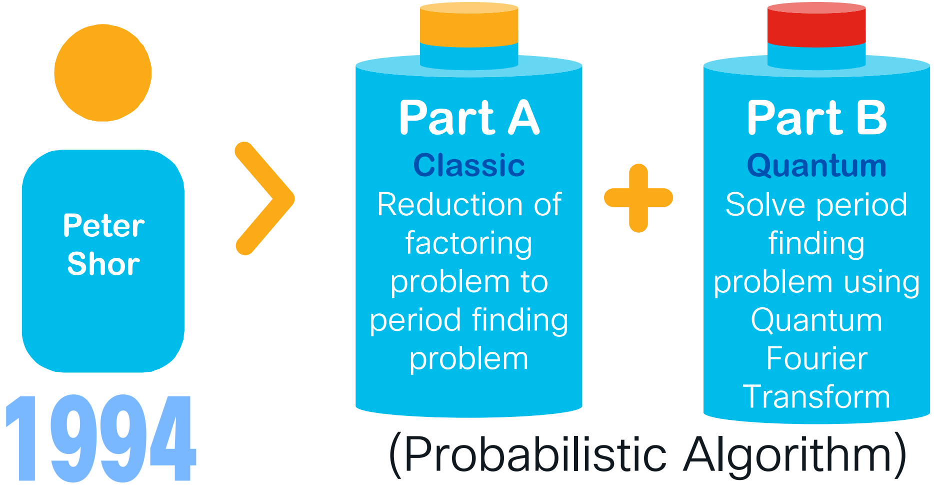
# Today's Cryptography Temporal Defense

TIME PROTECTS PUBLIC KEYS UNTIL Y2Q

# Shor's Factoring Algorithm

$N = p_1 * p_2$

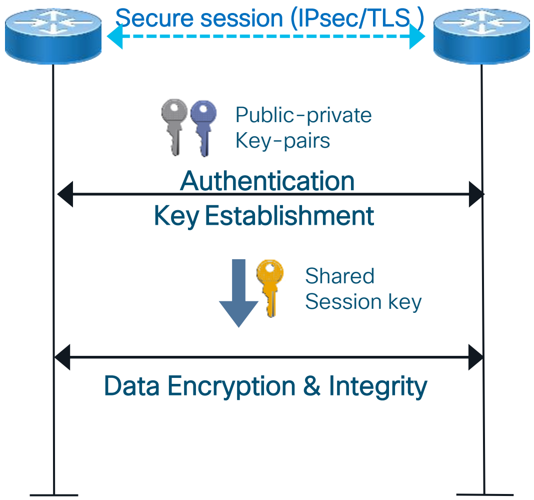
Problem: For a given "N" find a "p" between "1" and "N" that divides "N"




**Shor's algorithm converts exponential complexity to polynomial complexity**

$x^N \rightarrow N^x$ **where N is the number of bits**

# Quantum Computing Impact on Cryptography




**Asymmetric Cryptography**

- Based on mathematically related public-private key-pairs
- Used for control plane operations
  - Authentication, Key establishment
- Example: RSA, DH, ECC

Large reliable Quantum computers can break RSA, DH, ECC!

**Symmetric Cryptography**

- Based on shared key
- Used for bulk data encryption & integrity
- Protection level based on key strength
  - Key size & entropy
- Example: AES-GCM

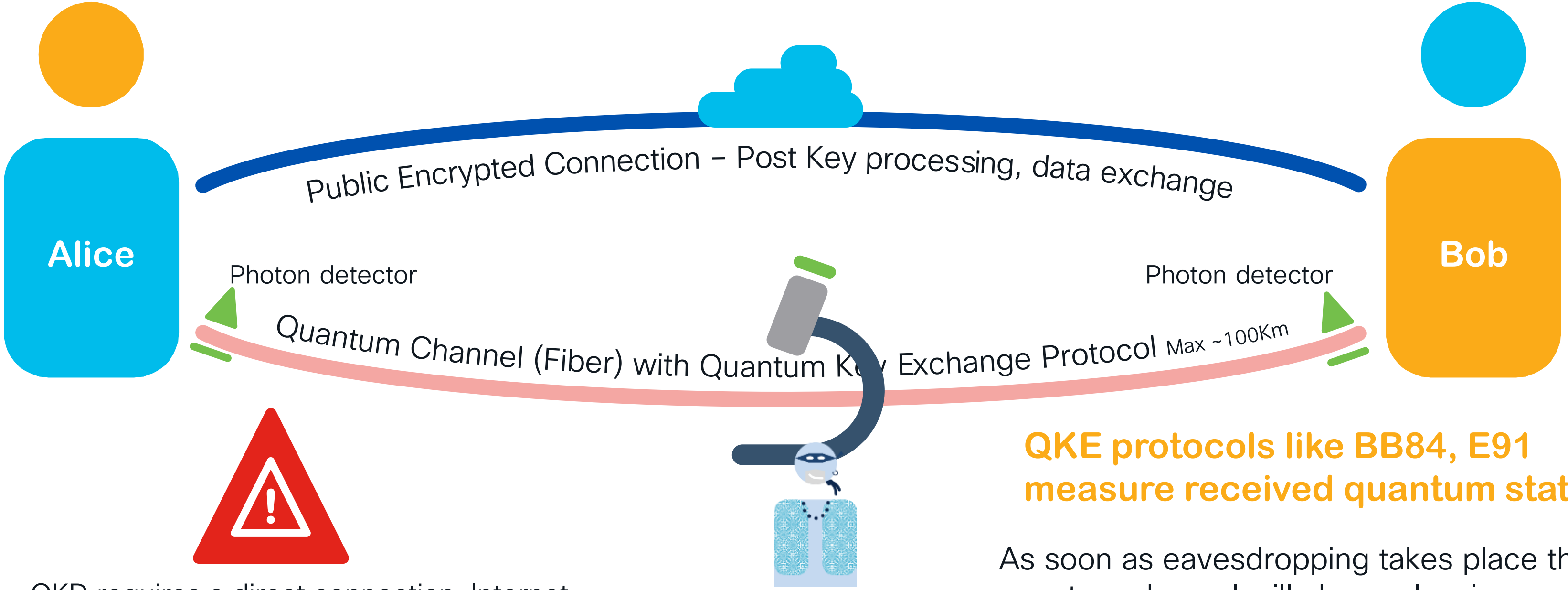
Symmetric crypto with large and high-entropy keys is resistant to Quantum computer attacks

Asymmetric crypto with RSA/DH/ECC based session keys is NOT Quantum-resistant

Symmetric crypto with pre-shared-key based session keys is Quantum-resistant

# Quantum Key Distribution

QKD is a scheme for distributing secure symmetric keys over a communication channel



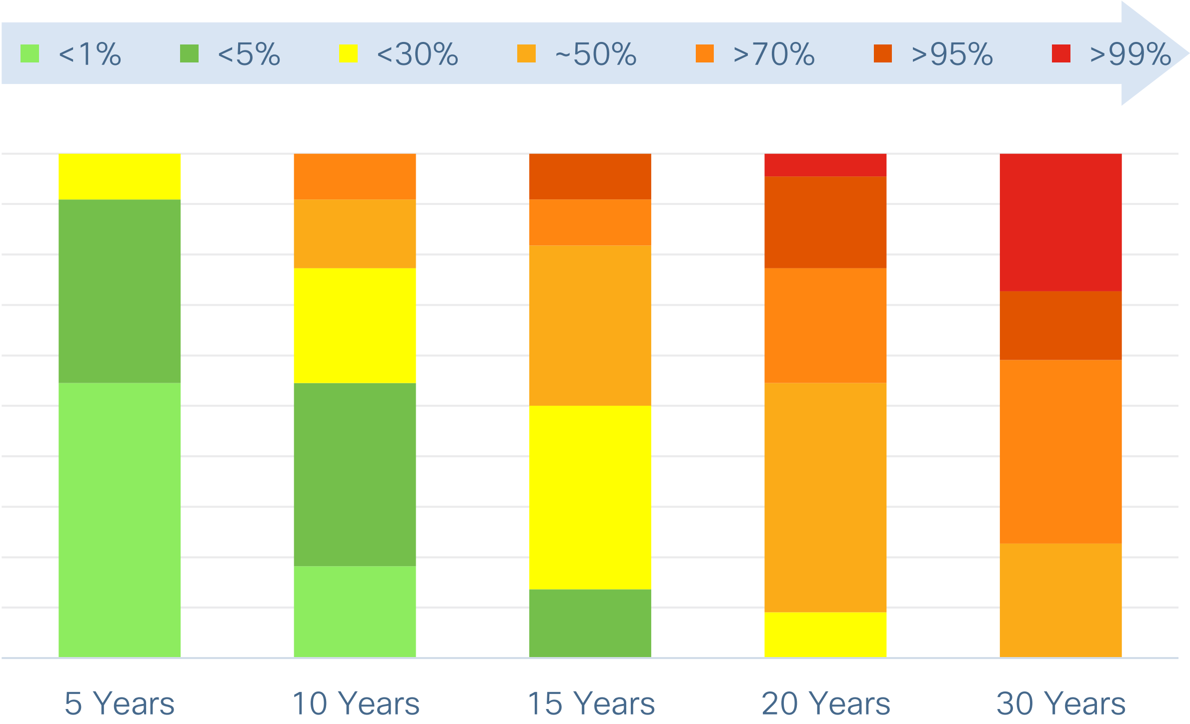

QKD requires a direct connection. Internet optical switches would destroy the quantum effect. Hence we need to a Quantum Internet

**QKE protocols like BB84, E91 measure received quantum states**

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

# Quantum Threat Risk (Likelihood) Over Time

Expert opinions on the likelihood of a significant Quantum Threat to Public-Key Cybersecurity as a function of time




Source: 2021-01-Quantum-Threat-Timeline-Report-2020-v2-revised-in-2022.pdf

# Quantum Security with Cisco

# Two Ways to Secure

Quantum Safe Cryptography: Any Technique that seems to be secure against adversaries with Quantum Computer

QKD – Quantum Key Distribution + NIST encryption schemes

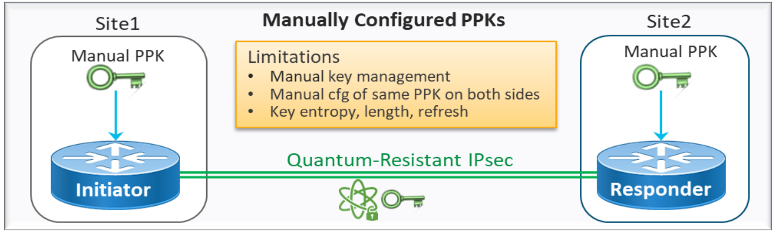
Post Quantum Cryptography (PQC) : Making Existing algorithms stronger against the adversaries of a quantum computer

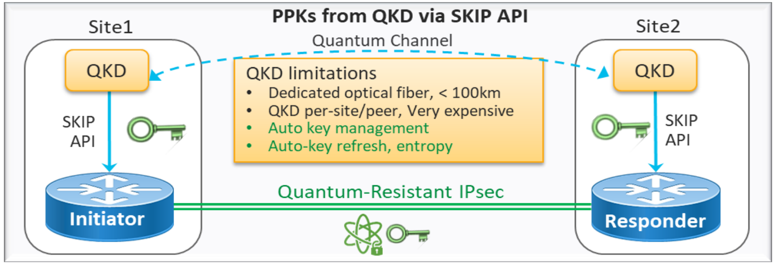
Pre-Shared Keys or PSK Mixing keys RFC 8784

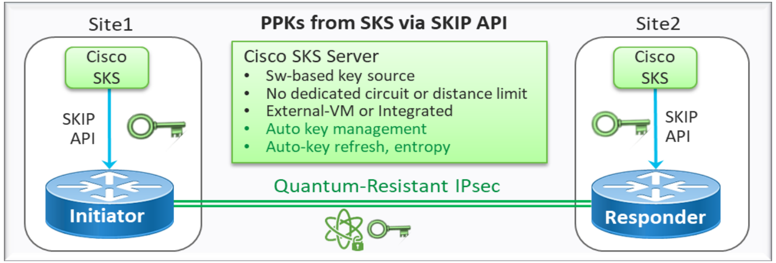
# Approach for Securing Transport

| Symmetric cryptography | Quantum key distribution | Post-quantum cryptography |
|---|---|---|
| ✓ Long symmetric keys are quantum-safe | ✓ Use quantum mechanics to protect the data | ✓ Replace current public key algorithms with new ones |
| ⚠ Issues with distributing keys and trust | ⚠ Technology limitations | ⚠ Still need to vet the algorithms and update the protocols |
| | Software Based / QKD Based | |
| Immediate | Mid Term | Long Term |

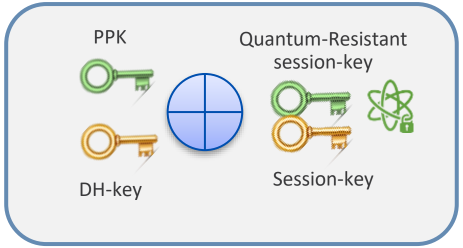
# Quantum Security Approach – IOS XE , IPSEC



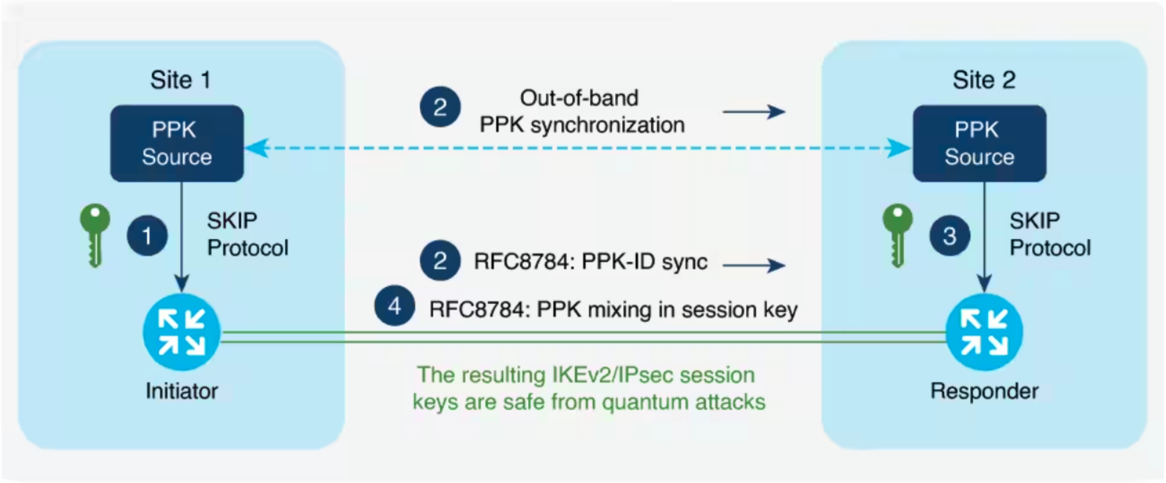

**RFC-8784 - PPK based IPsec encryption keys**




| Deployment Model | Availability |
|---|---|
| Manually configured PPK | IOS-XE: IPSEC |
| PPKs from QKD via SKIP | IOS-XE: IPSEC |
| PPKs from Cisco SKS Server | IOS-XE: IPSEC: (VM) |

Platforms Catalyst 8000v, 8300 & ASR 1000
Software version 17.11 onwards

# Secure Key Integration Protocol (SKIP)



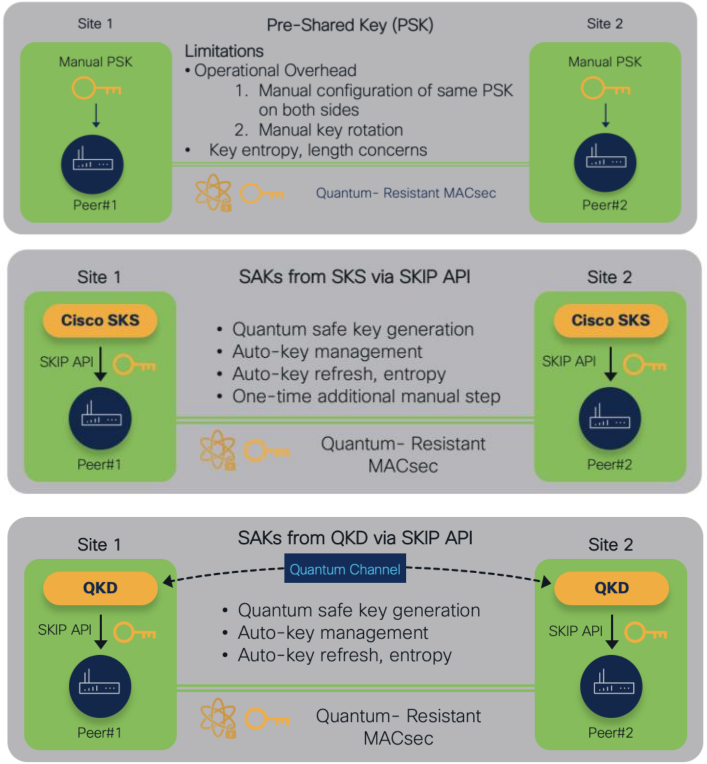

- HTTPS based protocol
- Allows integration with QKD or other entropy generators

```
8k-1-EFT#show crypto ikev2 sa de
8k-1-EFT#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
4         192.168.102.53/500    192.168.102.54/500    none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK, QR
      Life/Active Time: 86400/3626 sec
      CE id: 0, Session-id: 1
      Local spi: 57B6CBD926A008FA       Remote spi: 9364CE992C113974
      Status Description: Negotiation done
      Local id: 192.168.102.53
      Remote id: 192.168.102.54
      Local req msg id:  10             Remote req msg id:  0
      Local next msg id: 10             Remote next msg id: 0
      Local req queued:  10             Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
      Quantum Resistance Enabled
      PEER TYPE: Other

 IPv6 Crypto IKEv2  SA
```

# Quantum Security on IOS XR, MACsec




| Deployment Model | Availability + Current plans |
|---|---|
| Manually configured PPK | IOS-XR: MACSEC: PSK (Not RFC 8784) |
| PPKs from QKD via SKIP | IOS-XR: MACSEC: Available from 7.9.1 |
| PPKs from Cisco SKS Server | IOS-XR: MACSEC: Available from 7.9.1 |

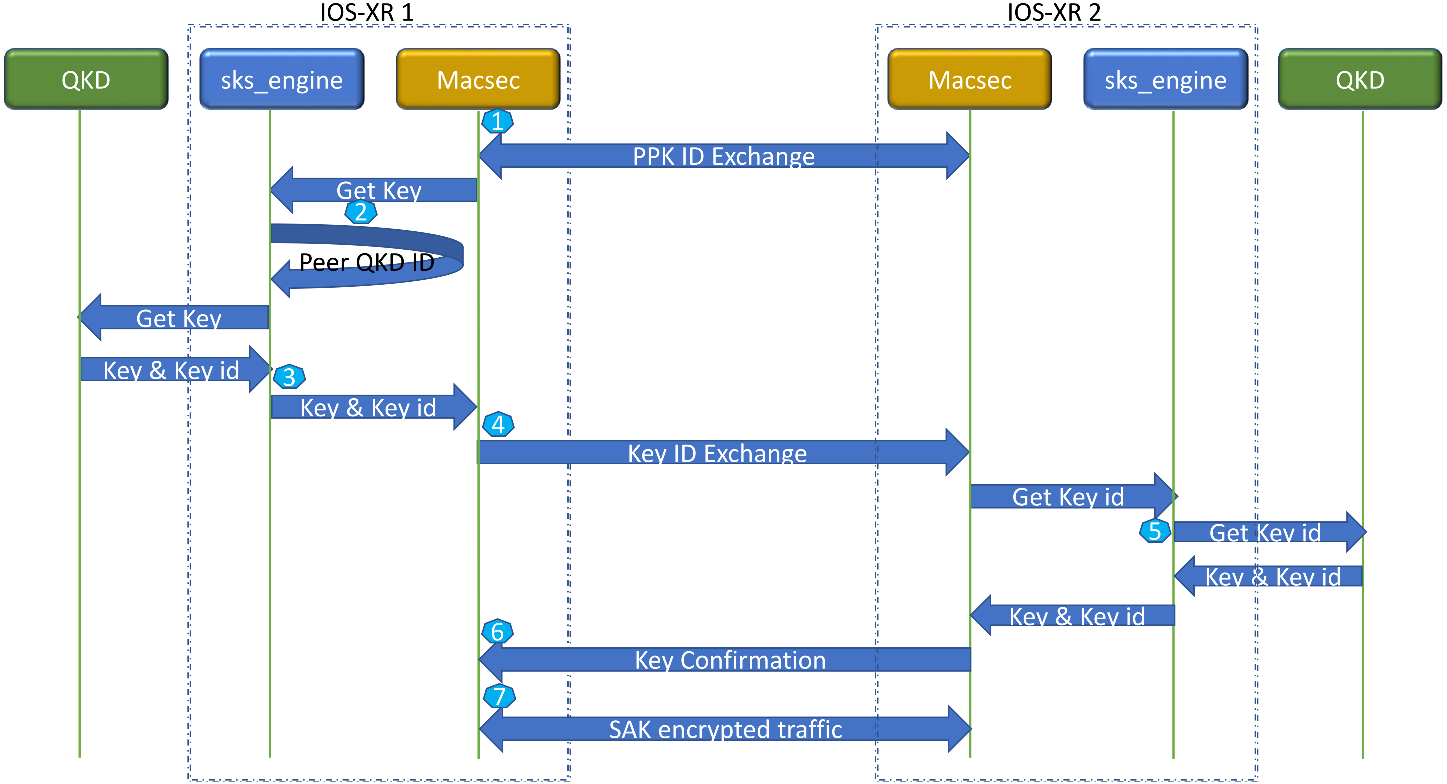
*SKS Server is inbuilt within IOS XR Code

# API Interaction b/w QKD device & IOS XR

| API | Method | URL |
| --- | --- | --- |
| Get capabilities | GET | https://{server_ip}/capabilities |
| Get key | GET | https://{server_ip}/key?remoteSystemID={remote_id} |
| Get key via key-id | GET | https://{server_ip}/key{key_id}?remoteSystemID={local_id} |
| Get entropy | GET | https://{server_ip}/entropy |

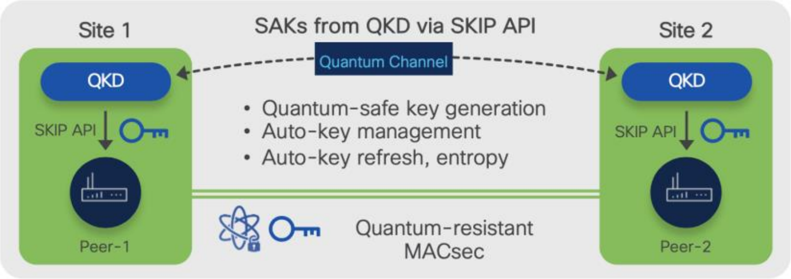
The interface between the IOS-XR device and QKD device is a web server REST API interface. The communication between the XR device and QKD uses HTTPS(TLS) with JSON encoded query requests and responses.

# QKD Key Fetching Flow



# SKS vs OKD

### *External QKD hardware*




1. Hardware-based key source
2. Dedicated optical fiber (up to 100 km supported)
3. QKD hardware per-site/peer
4. Very expensive
5. Supported from IOS-XR 7.9.1 release

### *Cisco SKS server*

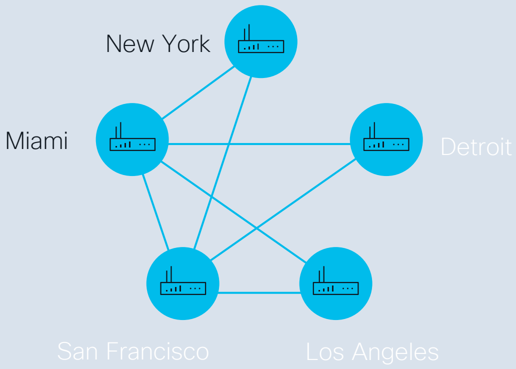

1. Software-based key source
2. No dedicated circuit or distance limitations
3. No additional hardware requirement
4. No additional cost
5. Supported from IOS-XR 7.4.1 release

Cisco Supports both Options for its IOS XE/XR devices

# • Quantum Crypto Scope

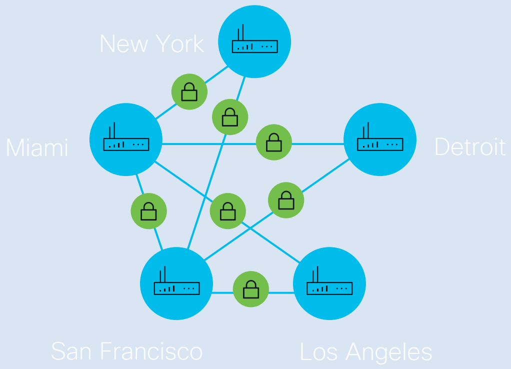
## Today

Legacy Networks




## Near-Term Solutions

Quantum Safe Cryptography




Protecting existing networks and information against quantum computer attacks.

## Expected End-State

Using quantum computing and technologies to create new networks.

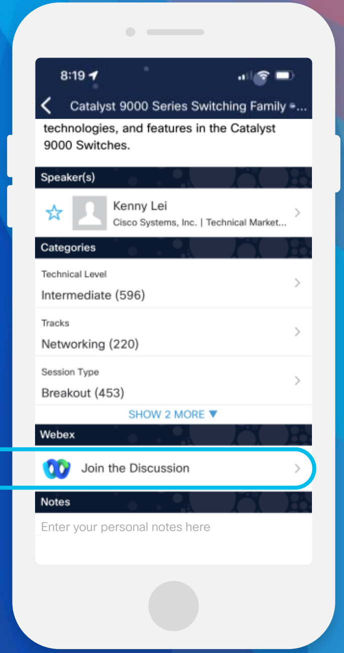
# Webex App

## Questions?

Use the Webex App to chat with the speaker after the session

## How

1. Find this session in the Cisco Events Mobile 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




https://ciscolive.ciscoevents.com/ciscolivebot/#DEVLIT-1054

## Webex spaces will be moderated by the speaker until February 23, 2024.

# Fill out your session surveys!

Participants who fill out a minimum of **four session surveys and the overall event survey** will get a Cisco Live t-shirt (from 11:30 on Thursday, while supplies last)!


All surveys can be taken in the Cisco Events Mobile App or by logging into the Session Catalog and clicking the ‘Participant Resource Center’ link at https://www.ciscolive.com/emea/learn/session-catalog.html.

# 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 ciscolive.com/on-demand. Sessions from this event will be available from February 23.

# Thank you

cisco Live!

# Let's go