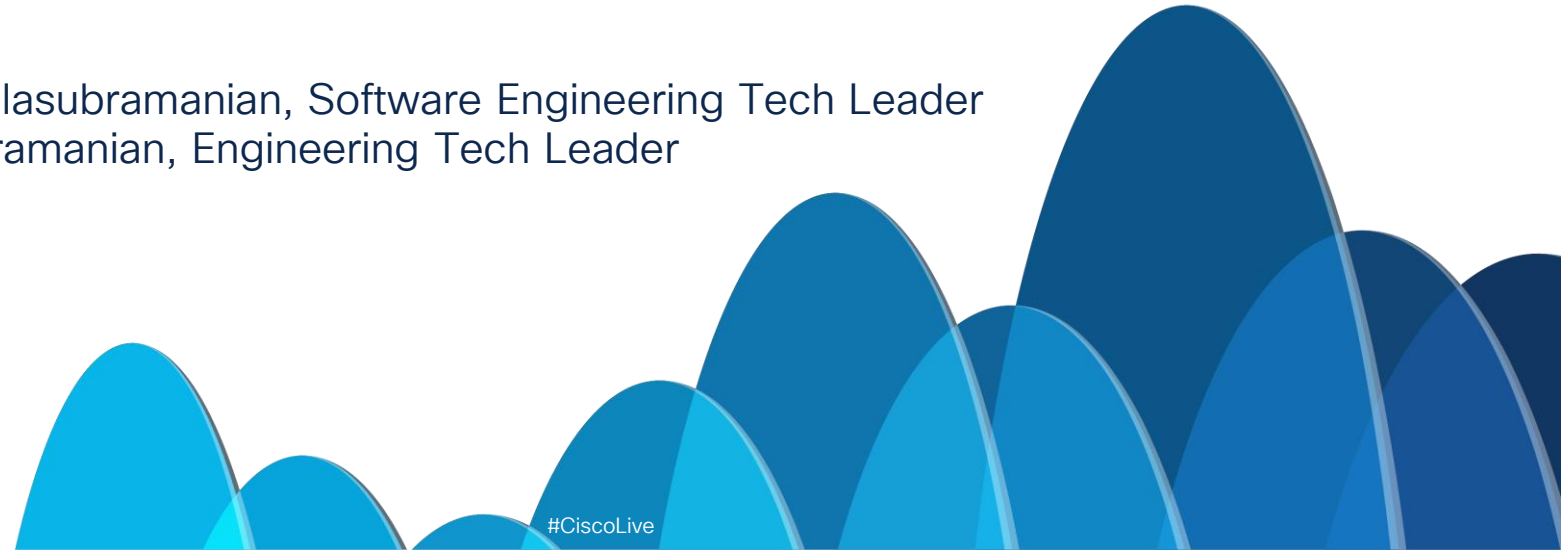
The bridge to possible

Quantum Ready Firewalls

Anupama Balasubramanian, Software Engineering Tech Leader
Vetrivel Subramanian, Engineering Tech Leader

BRKSEC-1036



cisco Live!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1036

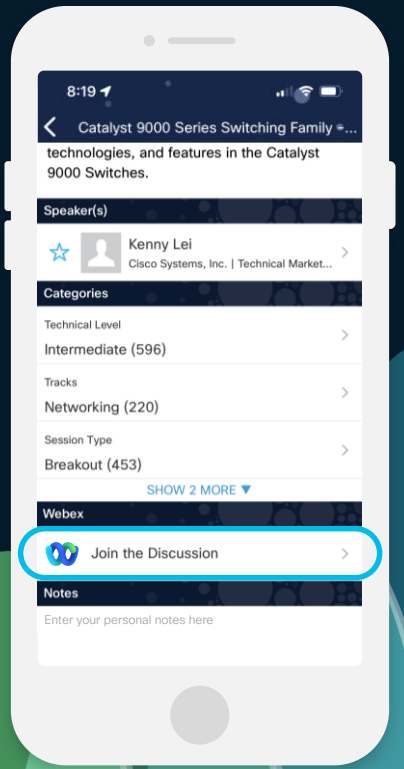
Questions?

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

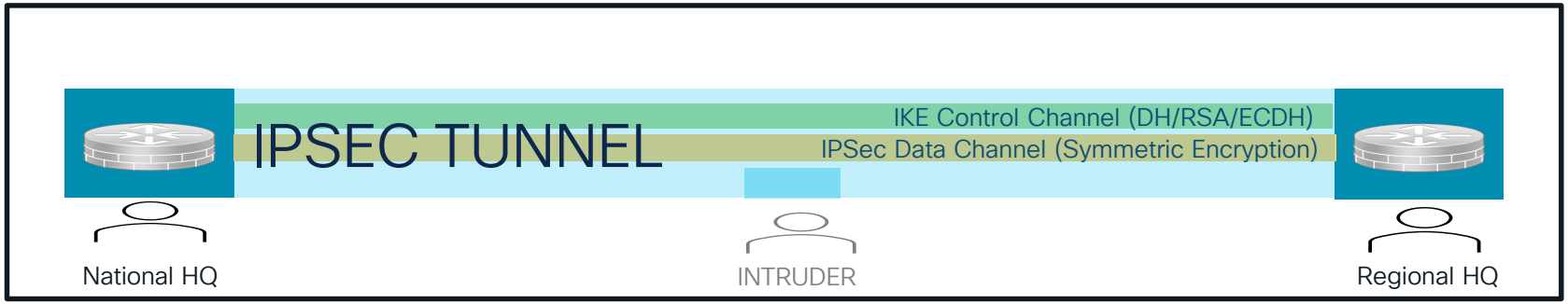
How

1. Find this session in the Cisco Live 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

Webex spaces will be moderated by the speaker until June 7, 2024.



Why Be Quantum Ready?



	Existing Public Key Infrastructure	Quantum Safe	
		Hardware Based Solution	Software Based Solution
Is the communication safe today?	Yes		
Can it withstand today's SNDL attacks?	No	Yes (QKD)	Yes (RFC 8784)
Will it be safe after Q-Day?	No	Yes (QKD)	Yes (PQC Algorithms)

Agenda

- How can Quantum Computers break Cryptography?
  - Principles of Quantum Computing
  - Impact of Quantum computing on cybersecurity
- Quantum Safe Cryptography
- Quantum Readiness of Cisco firewall VPNs

Vetri !

- 18 years with Cisco
- CCIE – Wireless
- Married; One daughter.

Loves

- Bike riding
- Travelling
- Adventure sports

Anupama !

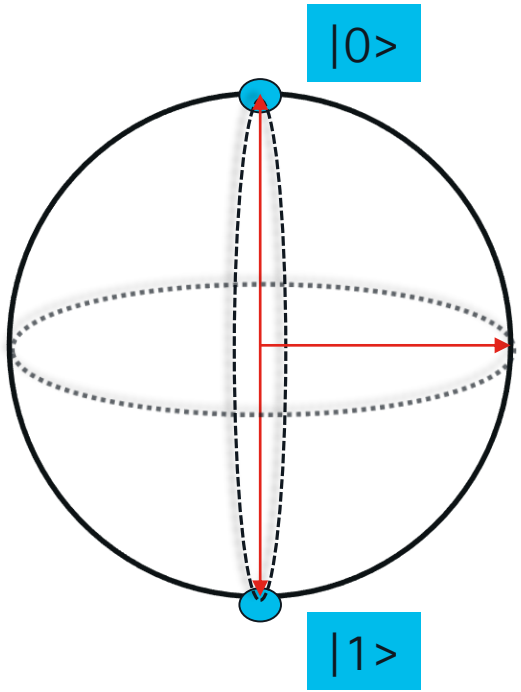
- 20 years of Industry Experience
- 3 years with Cisco

Loves

- Classical Music and Dance
- Books
- Movies

Principles of Quantum Computing

Qubit



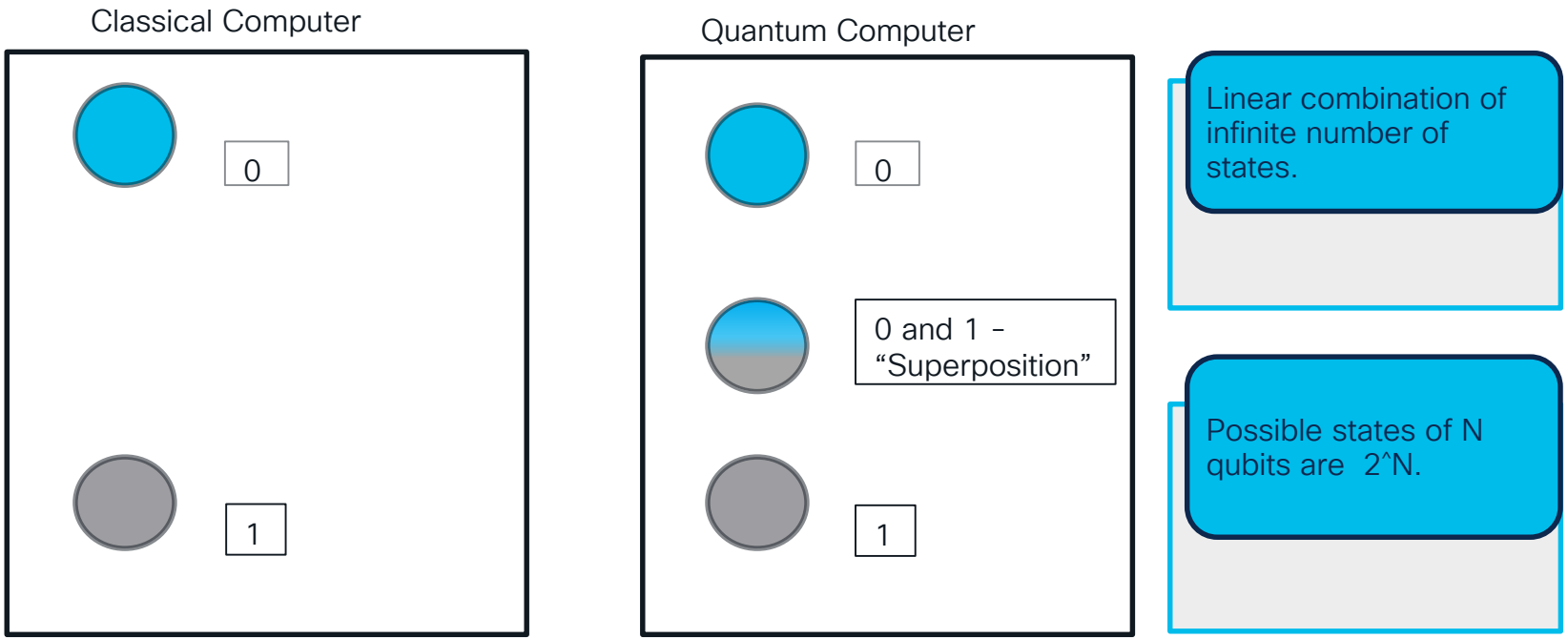
(|0> + |1>)/(sqrt(2))

The Basic Unit of Information in Quantum Computing

A qubit represents 0, 1, or any quantum superposition of these classical states.

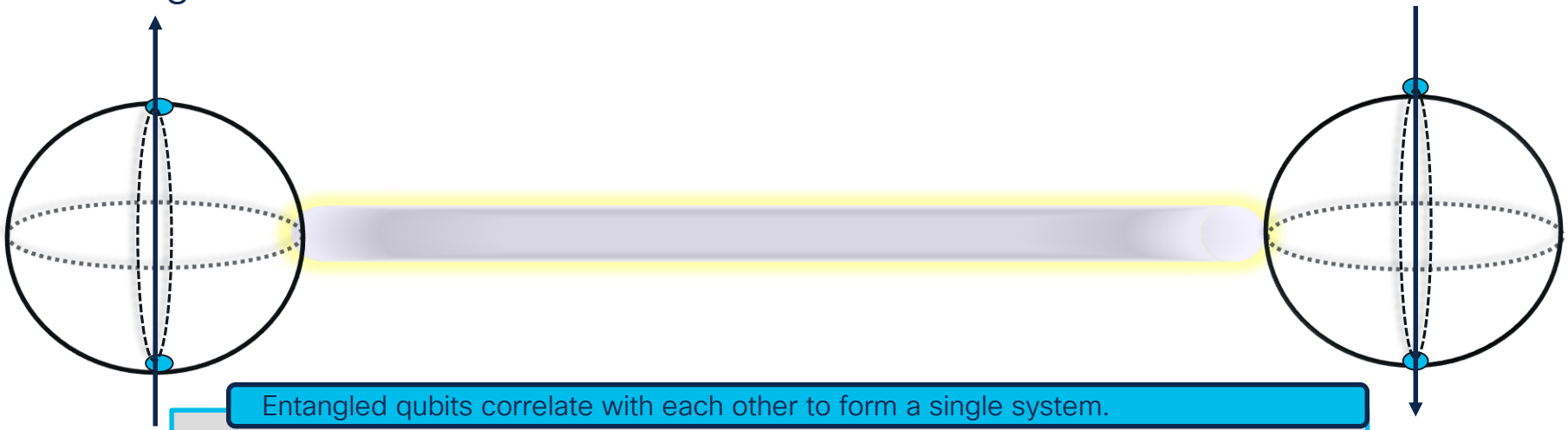
Principles of Quantum Computing

Superposition



Principles of Quantum Computing

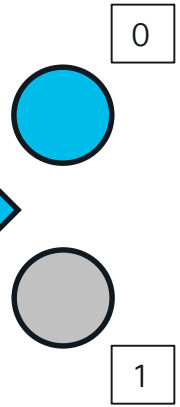
Entanglement



- Entangled qubits correlate with each other to form a single system.
- Measuring the state of one of the qubits allows us to know the state of the other.
- Quantum entanglement enables qubits to interact with each other instantaneously.
- This is not affected by distance or limited to the speed of light.

Principles of Quantum Computing

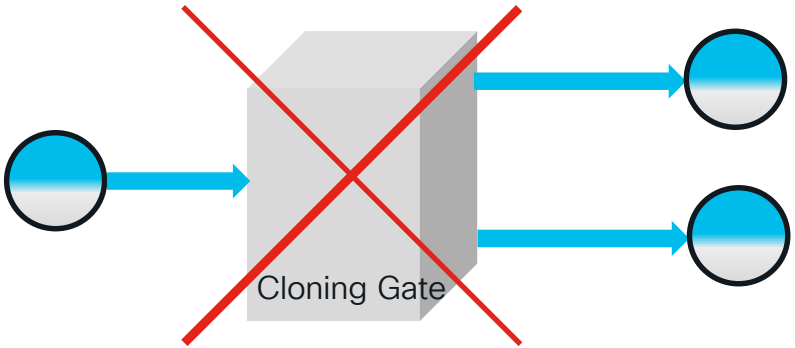
De-coherance



- Qubits are fragile.
- Measurement of Qubit states also result in de-coherance.
- Qubit loses quantum property and collapses into the classical binary state.

Principles of Quantum Computing

No-cloning Theorem



It is impossible to create an independent and identical copy of an arbitrary unknown quantum state.

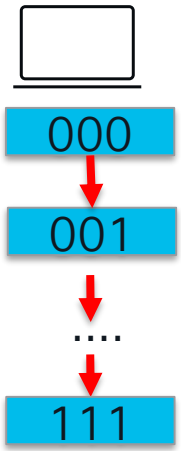
This property is vital in quantum cryptography.

It forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key.

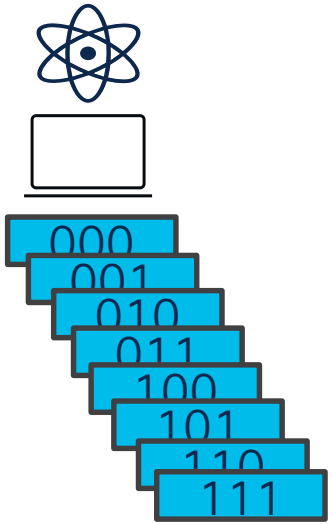
The No-Cloning Theorem

Principles of Quantum Computing

Quantum Parallelism



Classical Computer



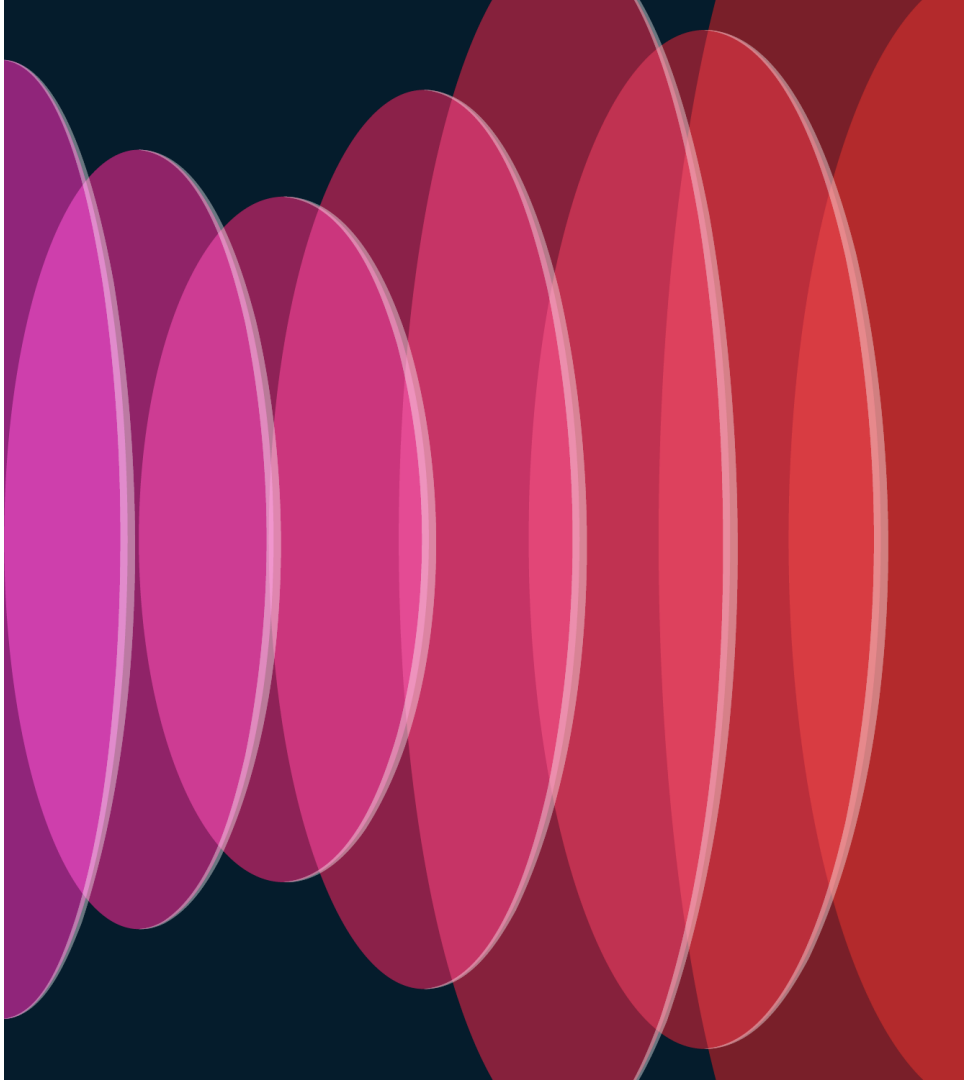
Quantum Computer

A classical silicon-based computer can solve one problem at a time (or a few on multi-core computer).

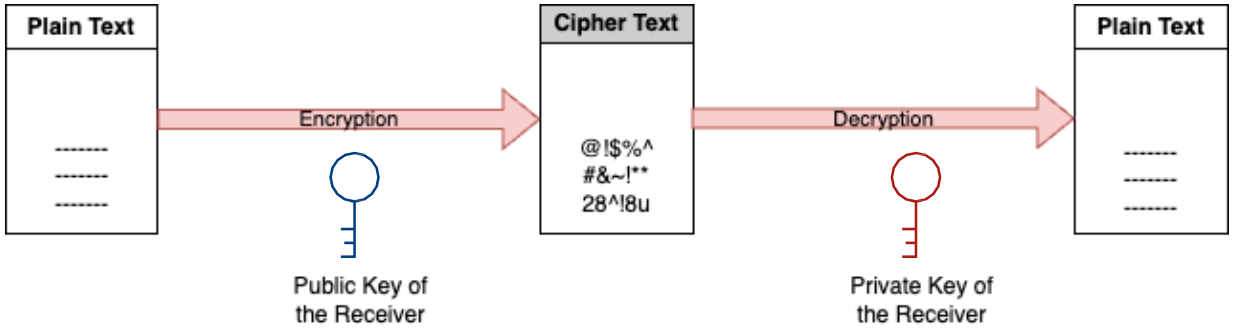
With “n” bits, a classical computer chooses one of 2^n values to do the computation.

With n-qubits, all the 2^n values are used to computation at the same time in parallel.

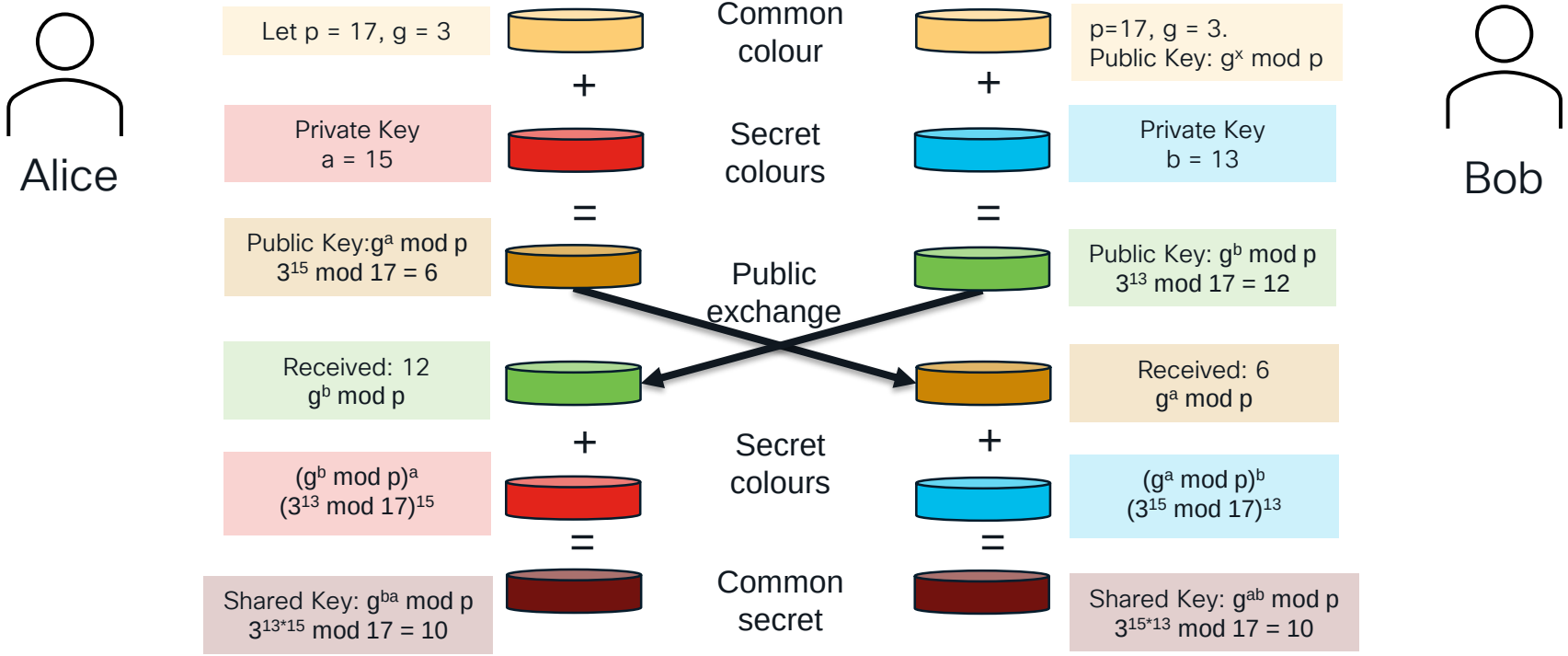
Impact on cybersecurity



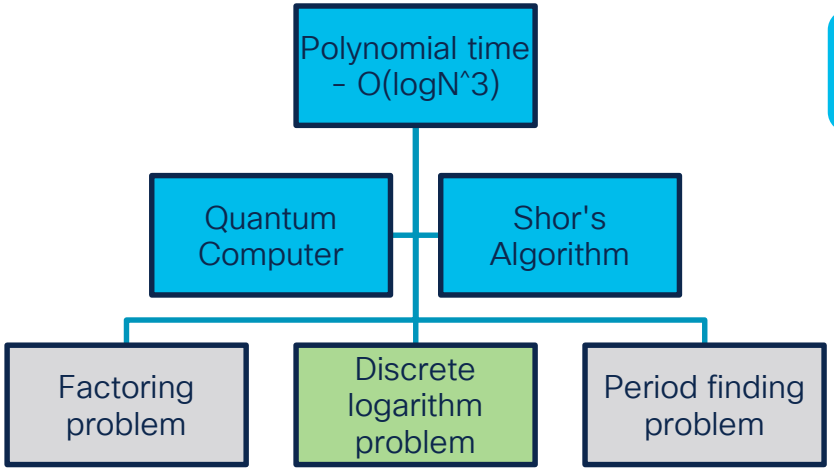
Asymmetric Key Cryptography

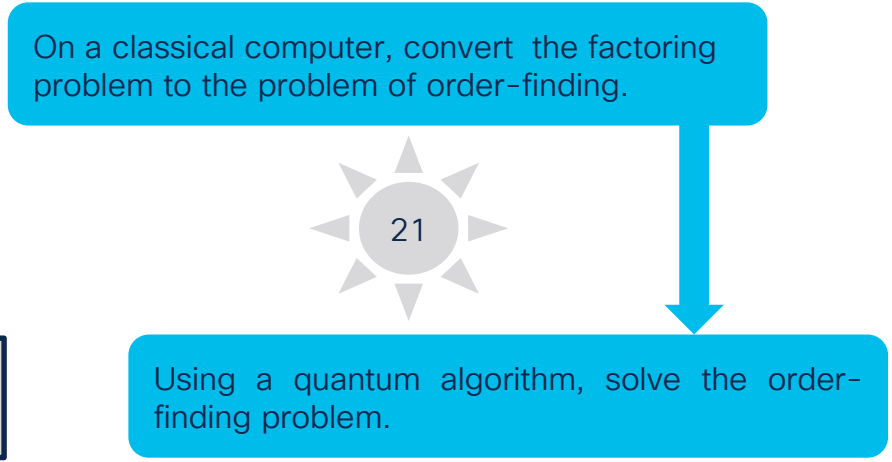


Diffie Hellman Key Exchange



Shor’s Algorithm

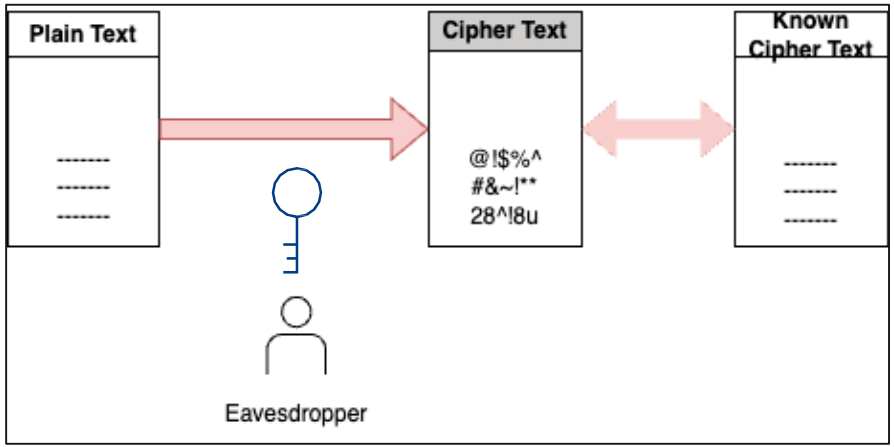




Source: Shor's Algorithm

Impact on Symmetric Key Cryptography

Grover's Algorithm



Solution for an unstructured search.

Proposed by Lov Grover.

Number of steps using classical computation -> O(N)

Given y = f(x), Find input value x, such that,

- f(x) =1 for only one value of x,
- f(x) = 0 for all other

Number of steps using quantum algorithm -> O(sqrt(N)). Provides Quadratic Speedup.

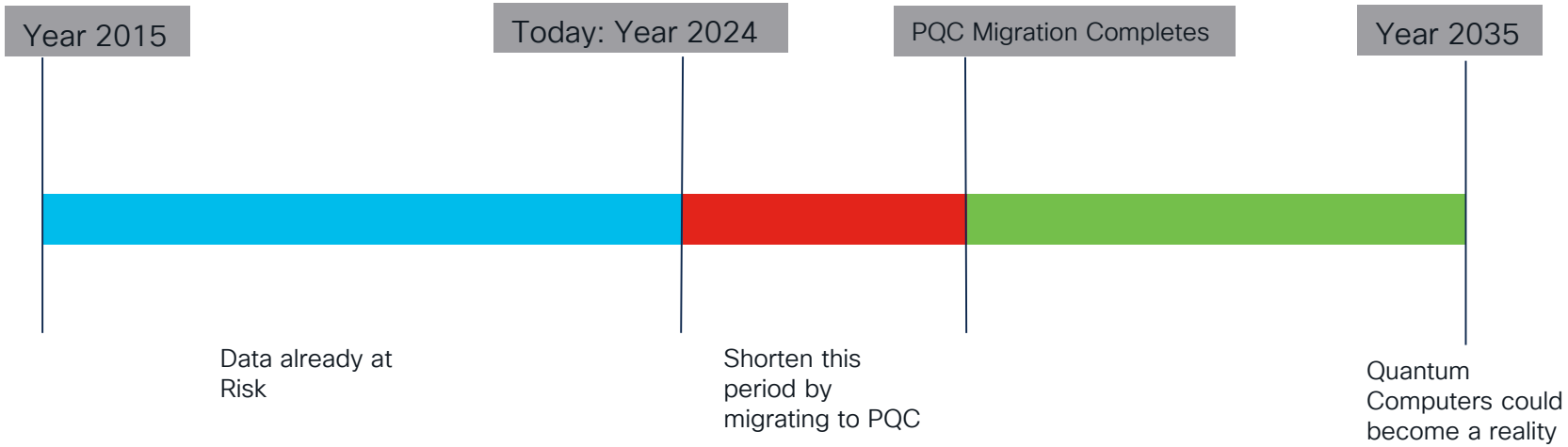
How Common Cryptographic Algorithms are impacted?

Cryptographic Algorithms	Type	Purpose	Impact from Large Scale Quantum Computer
RSA	Asymmetric	Signatures, Key establishment	No longer secure
DH / DSA	Asymmetric	Signatures, Key exchange	No longer secure
ECDH / ECDSA	Asymmetric	Signatures, Key exchange	No longer secure
AES	Symmetric	Encryption	Larger Key Size Needed
SHA-2, SHA 3	---------	Hash Functions	Larger Key Size Needed

Source: NISTIR 8105 Report on Post-Quantum Cryptography

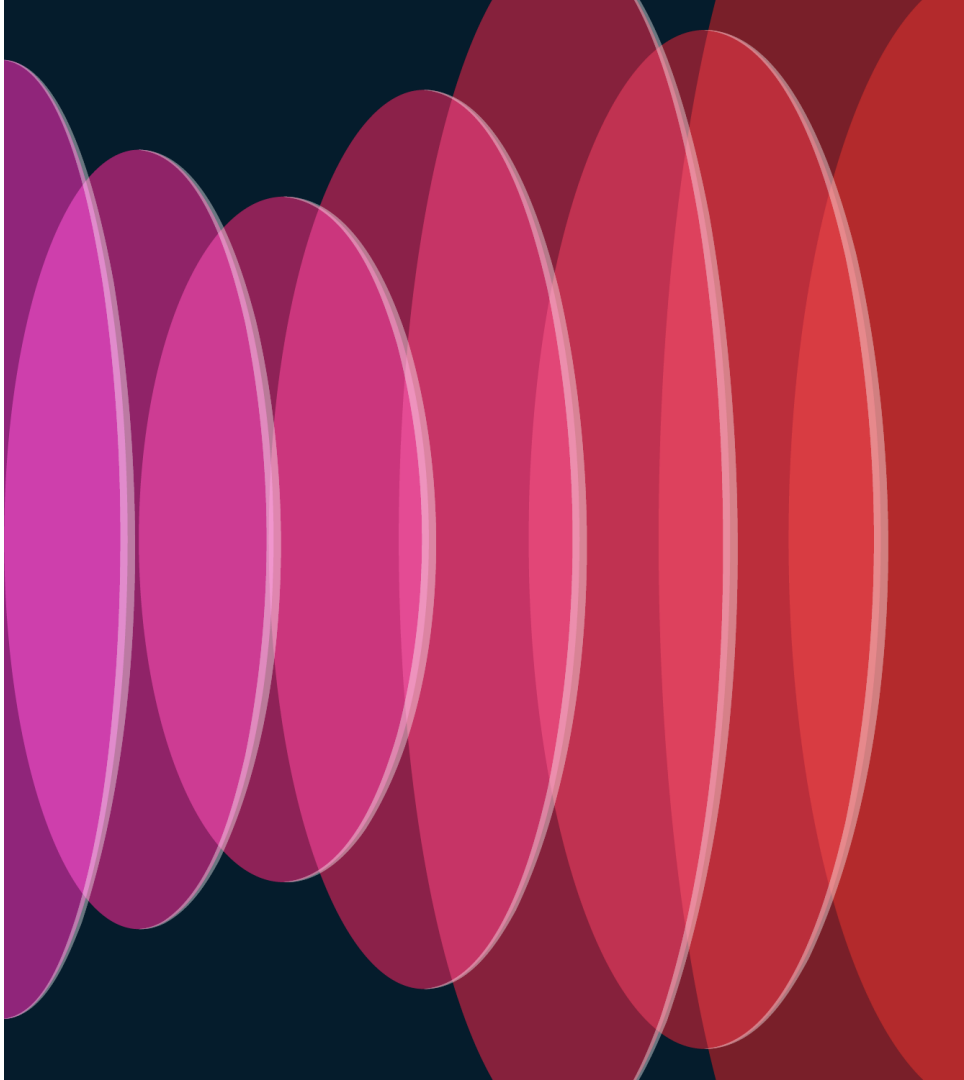
Quantum Urgency

Harvest Now, Decrypt Later!



Post Quantum Cryptography is needed today!

Quantum Safe Cryptography



cisco Live!

Techniques for Quantum Safe Cryptography

Hardware Techniques

Quantum Key Distribution

Quantum Safe Symmetric Cryptography

Increasing Key Length for Symmetric Key Encryption (Eg: AES128 -> AES256)

Quantum Safe Asymmetric Cryptography

Hash Based Cryptosystems
Code Based Cryptosystems
Multi Variate Based Cryptosystems
Lattice Based Cryptosystems

Quantum Key Distribution

- A secure communication method
- Implements a cryptographic protocol.
- It involves components of quantum mechanics.
- Eg: Fibre Optics, Satellite Based

Communicating users can detect the presence of eaves droppers.

In accordance with the Heisenberg uncertainty principle, a third-party observer will end up physically changing the values of some of the bits in the data stream in a detectable way.

As per the no-cloning theorem, it is physically impossible to make a perfect copy of an unknown quantum state.

Properties of quantum entanglement will cause de-coherance.

Quantum Key Distribution

Disadvantages

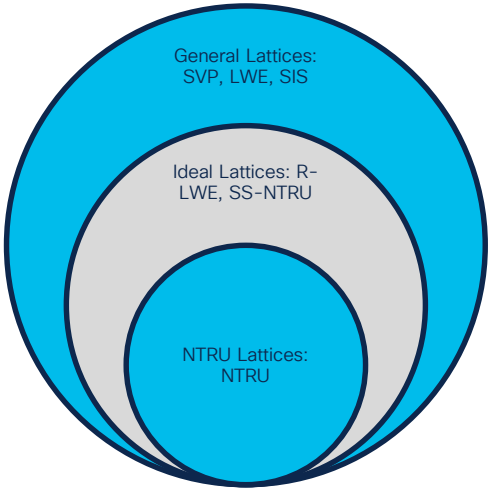
- Expensive dedicated hardware.
- Limited transmission distance.
- Need to support QKD protocols.
- Elegance of Public Key Cryptography is lost
- P2Pconnection between sites – O(N^2) connections.

Post Quantum Algorithms – NIST

Algorithm	Type	Class	Comments
CRYSTALS-Kyber	PKE/KEM	Lattice Based (M-LWE)	NIST Round 3 Winner
CRYSTALS-Dilithium	Signature	Lattice Based (M-LWE, M-SIS)	NIST Round 3 Winner
FALCON	Signature	Lattice Based (SIS)	NIST Round 3 Winner
SPHINCS+	Signature	Hash Based	NIST Round 3 Winner
BIKE		Code Based	Round 4
Classic-McEliece		Code Based	Round 4
HQC		Code Based	Round 4
SIKE		Super singular elliptic curve isogeny	Round 4 (Broken)

Source:
NIST PQC Standarization selected-algorithms-2022
NIST PQC Standardization Round 4 Submissions

NIST Algorithms based on Lattice Based Cryptography

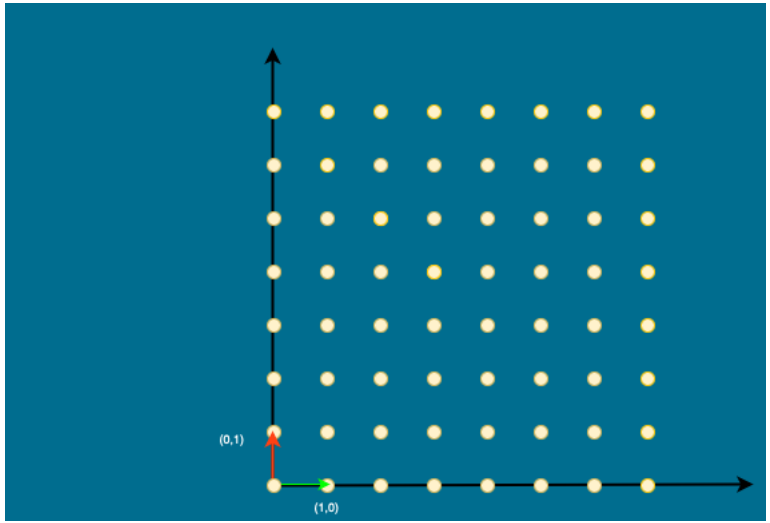


Algorithm	Underlying Hard Problem
CRYSTALS-Kyber	M-LWE Problem
FALCON	(SIS) over NTRU lattices
CRYSTALS-Dilithium	Module Lattices

1. The objective of Shortest Vector Problem (SVP), is to find the shortest non-zero vector within the lattice.
2. This problem is NP-hard.
3. No known quantum algorithm to solve SVP.

Lattice Based Cryptography

Lattices and Basis Vectors



Lattices are regular-spaced grid of a set of points that are infinite in number.

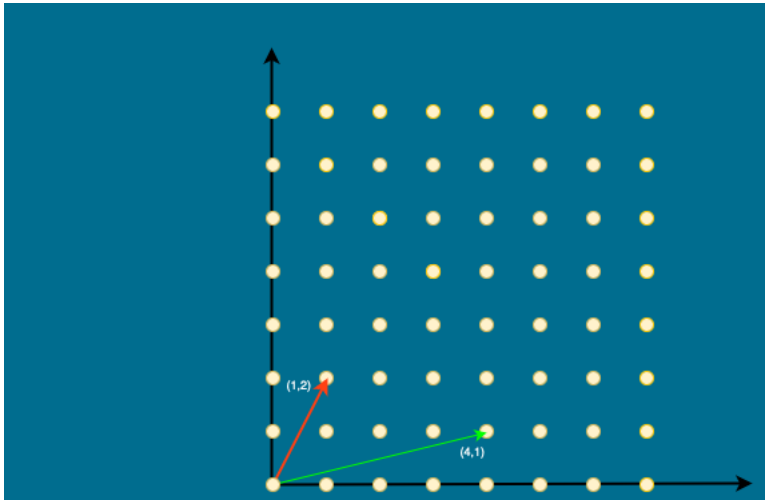
Vector is the name of a point, and the numbers on it are called coordinates.

A **lattice** is a collection of these vectors in an infinite series.

Basis is a collection of vectors used to present any point in the lattice grid that forms a lattice. Eg: Vector A= (1,0), Vector B = (0,1)

Lattice Based Cryptography

Custom Basis Vector



A lattice grid can be comprised of multiple sets of basis vectors. Eg: Vector A1= (4,1), Vector B1= (1, 2)

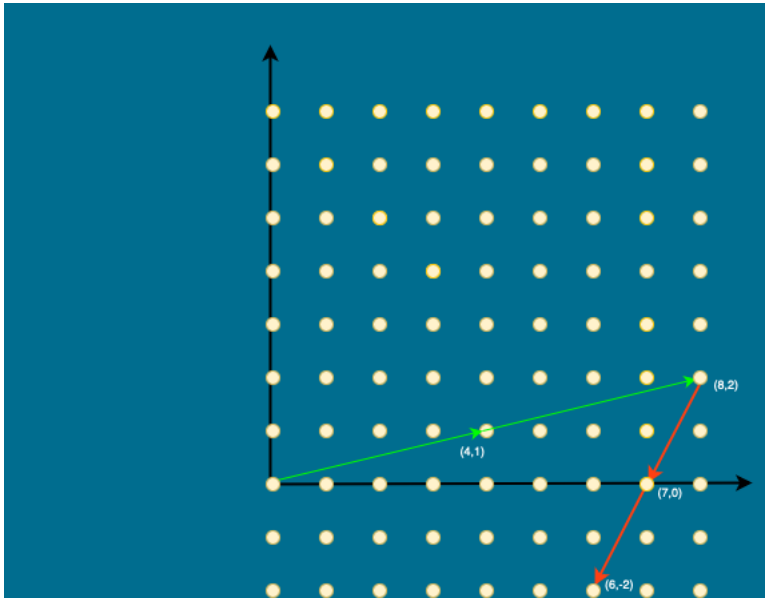
Basis vectors of a lattice is not unique.

A set of basis vectors almost orthogonal to each other can be defined as “good” basis vectors.

A set of basis vectors almost parallel to each other can be defined as “bad” basis vectors.

Lattice Based Cryptography

Shortest Vector Problem



Given the basis vectors, what integer linear combination of the vectors is closest to the origin.

Find the point closest to the origin.

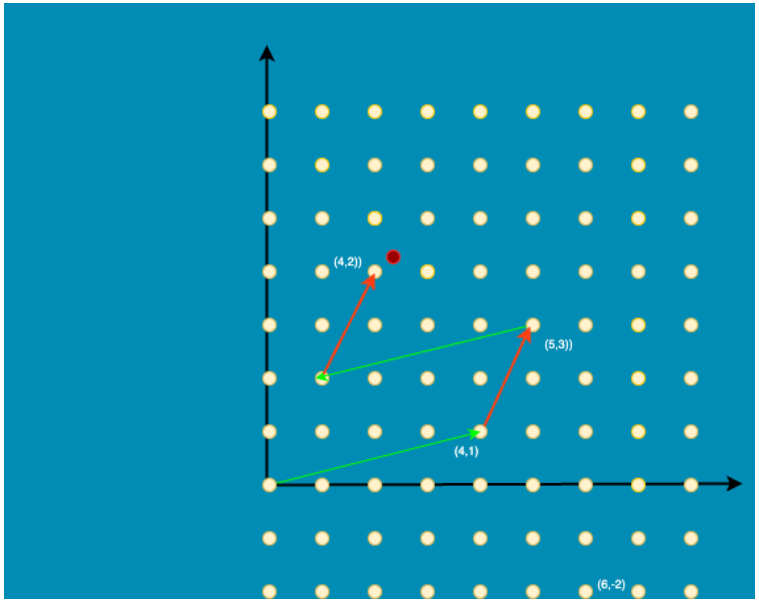
Let Vector A1= (4,1), Vector B1= (1, 2)

Point (7, 0) = 2A1 - B1 = sqrt(49)

Point (6, -2) = 2A1 - 2B1 = sqrt(40)

Lattice Based Cryptography

Closest Vector Problem



Given the basis vectors, what integer linear combination of the vectors is closest to the given point.

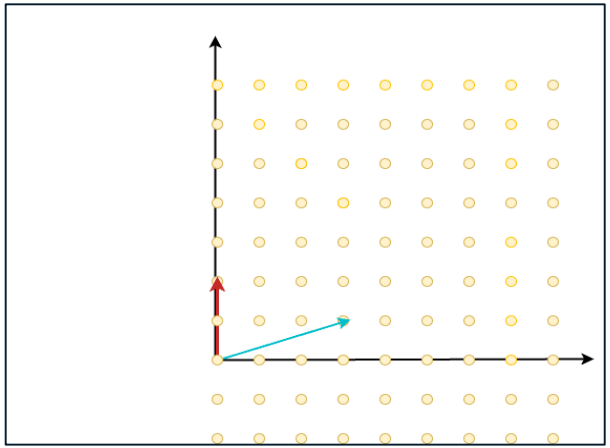
Find the lattice point closest to the given point.

Let Vector A1= (4,1), Vector B1= (1, 2)

CVP is the lattice point (2,4) = 1*A1+2*B1-1*A1

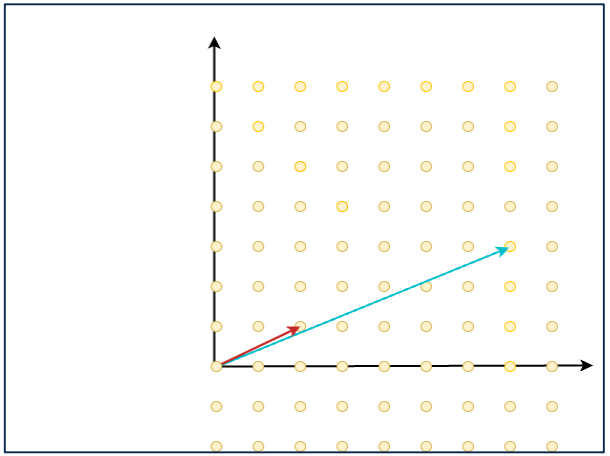
Lattice Based Key Exchange

Alice



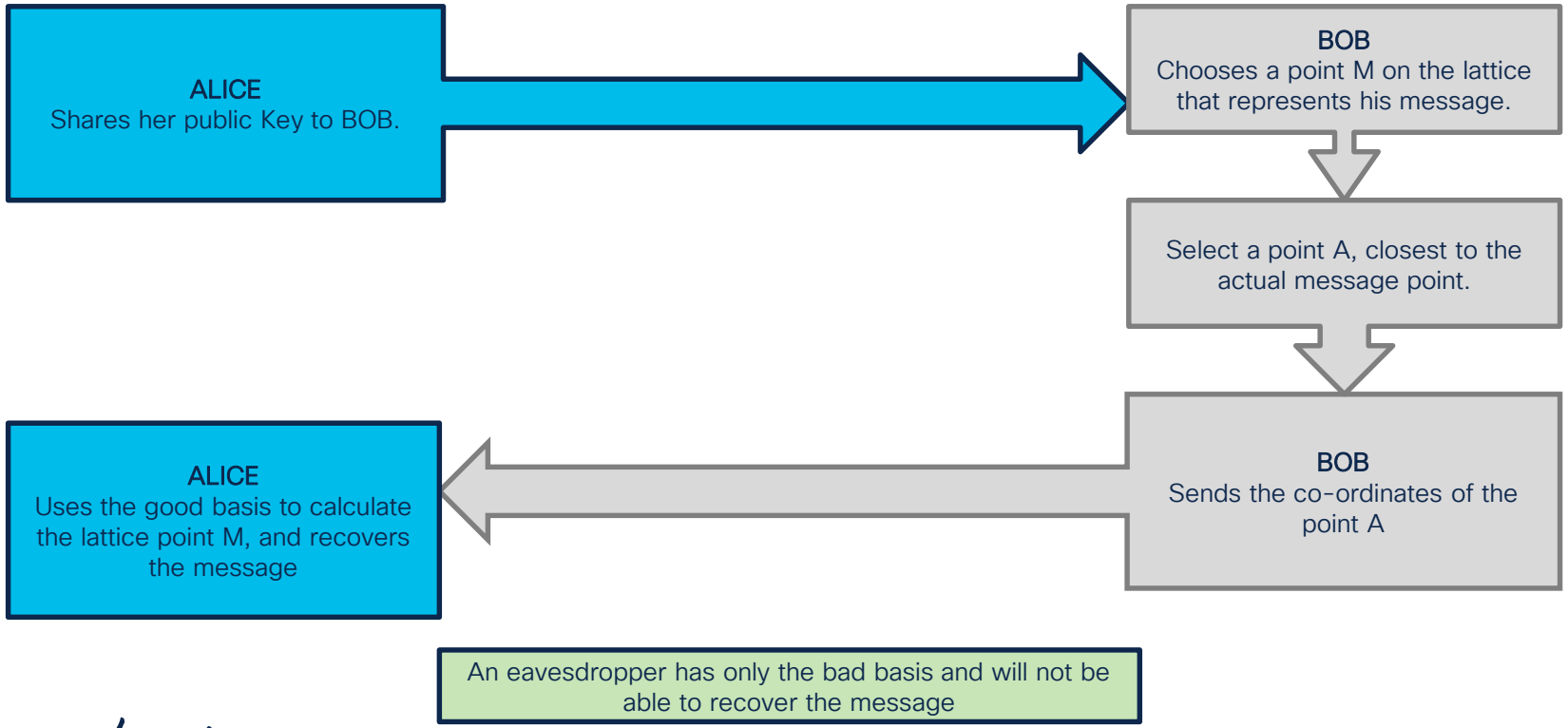
Good Basis: Private Key

Bob

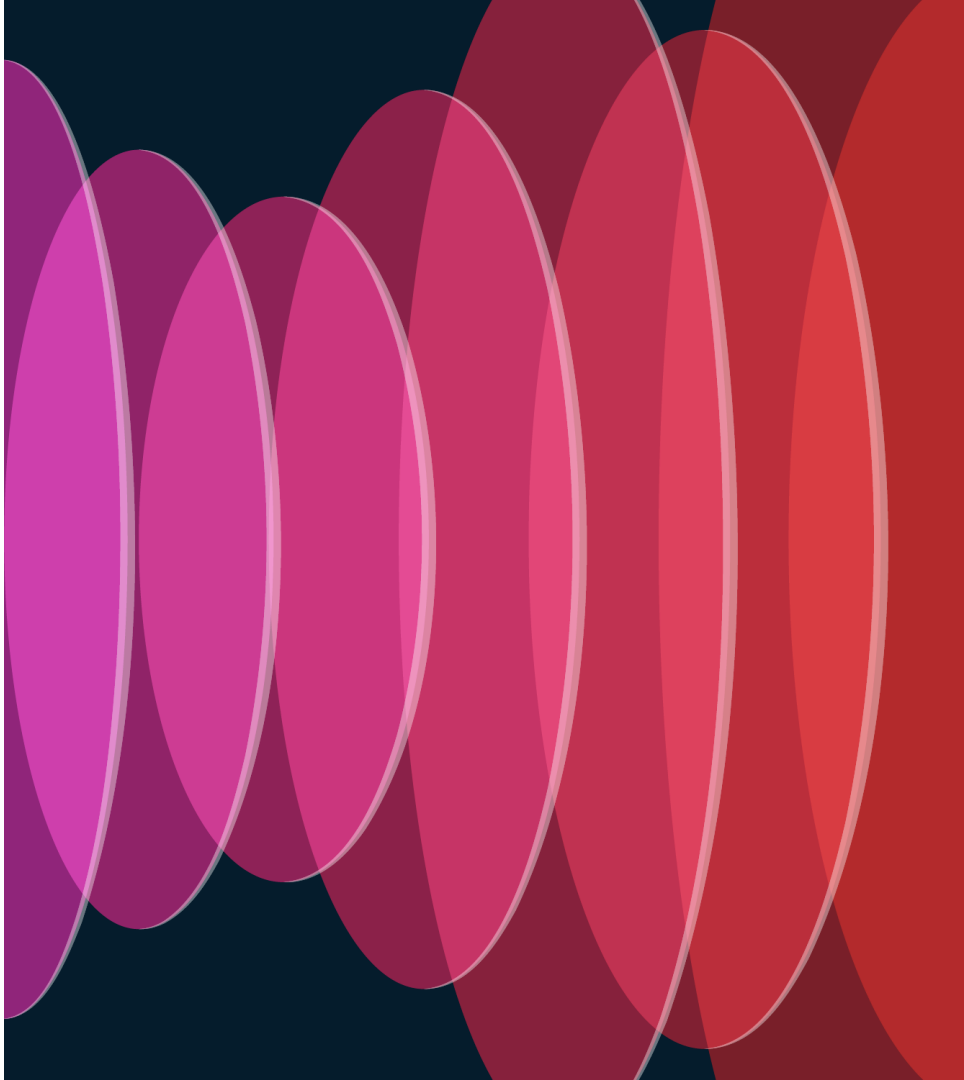


Bad Basis: Public Key

Lattice Based Key Exchange



Quantum Readiness of Cisco Firewall VPNs

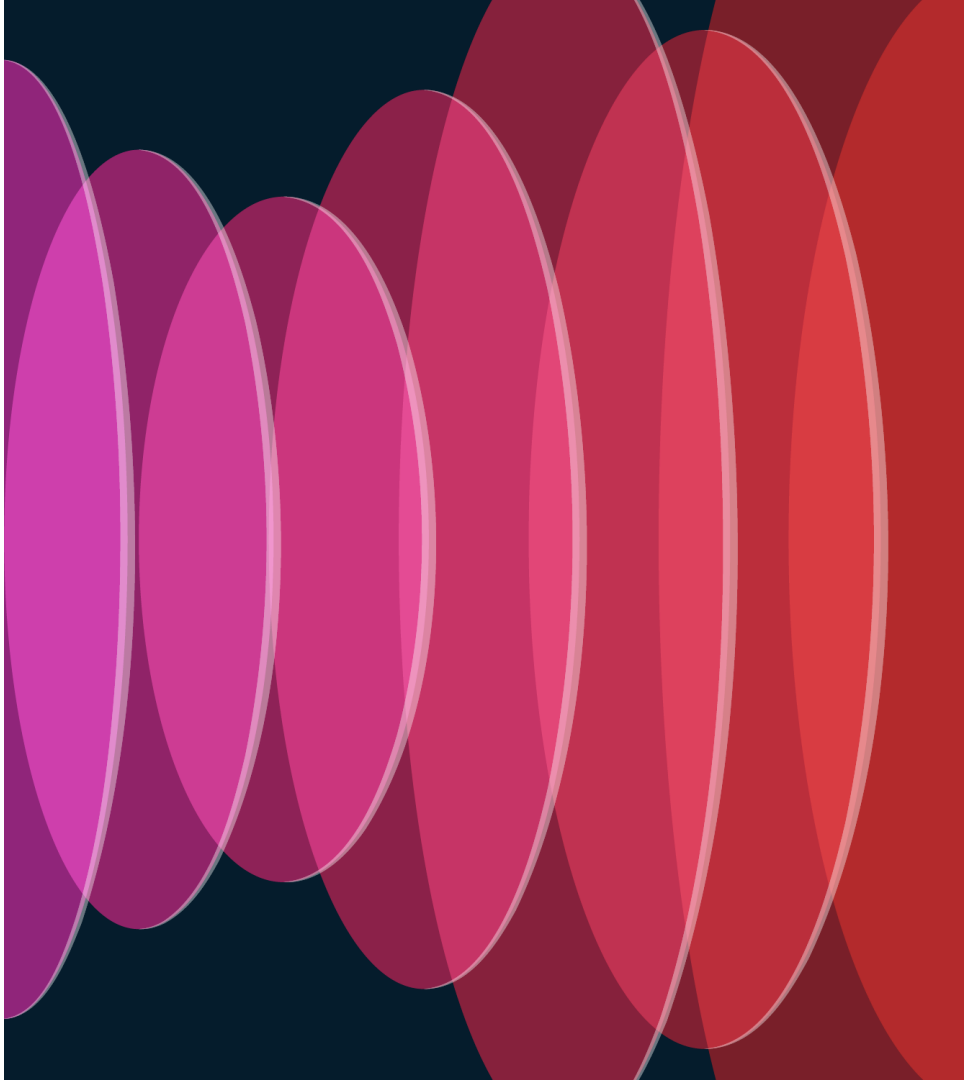


cisco Live!

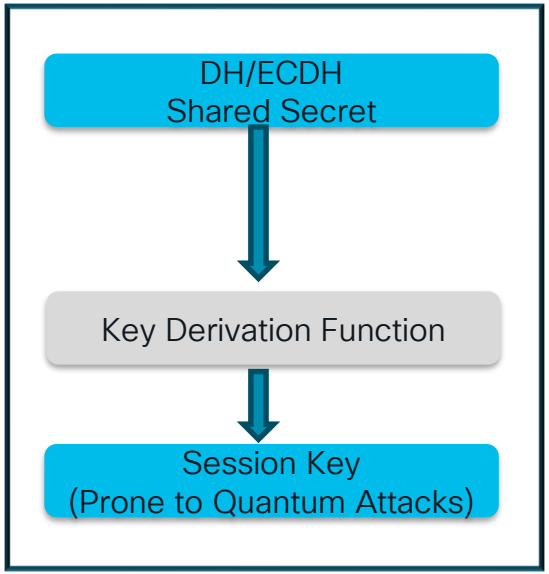
Software Based Approaches

- PPK - Post Quantum pre-shared Key (RFC 8784)
- Multiple Key Exchange (RFC 9242, RFC 9370)

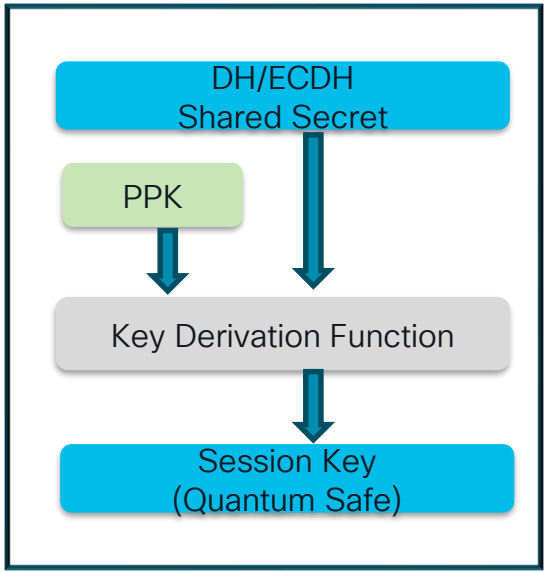
Post Quantum Pre-shared Key



VPN IKEv2/IPSec
PPK

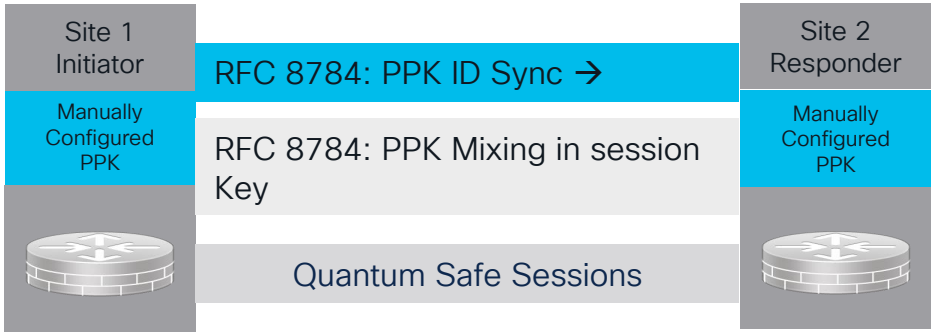


Single Key Exchange
(EC)DH



Post Quantum Pre Shared Key
(PPK)

VPN IKEv2/IPSec
PPK



- Post Quantum Preshared Key (PPK) is configured between the IKEv2 Initiator and Responder
- Configuration is part of IPSec tunnel-group.
- This value is mixed into the SKEYSEED derivation process.
- The subsequent key material can be now considered quantum secure.

VPN IKEv2/IPSec
PPK (RFC 8784) Configuration (ASA 9.18.1)

CLI Configuration Snippet

```
tunnel-group peer-1 ipsec-attributes
     ikev2 remote-authentication pre-shared-key *****
     ikev2 local-authentication pre-shared-key *****
     ikev2 remote-authentication post-quantum-key ***** identity test mandatory
no tunnel-group-map enable ike-id
```

Debug Logs
debug crypto ikev2 protocol 255

```
IKEv2-PROTO-7: (52): SM Trace-> SA: I_SPI=B4FC811A5AA58718 R_SPI=0B5553D5FBB84AB3 (I) MsgID = 00000000 CurState:
I_BLD_AUTH Event: EV_CHK_FOR_PPK
IKEv2-PROTO-7: (52): SM Trace-> SA: I_SPI=B4FC811A5AA58718 R_SPI=0B5553D5FBB84AB3 (I) MsgID = 00000000 CurState:
I_BLD_AUTH Event: EV_CHK_PPK_MAND
IKEv2-PROTO-7: (52): SM Trace-> SA: I_SPI=B4FC811A5AA58718 R_SPI=0B5553D5FBB84AB3 (I) MsgID = 00000000 CurState:
I_BLD_AUTH Event: EV_MIX_PPK
```

VPN IKEv2/IPSec

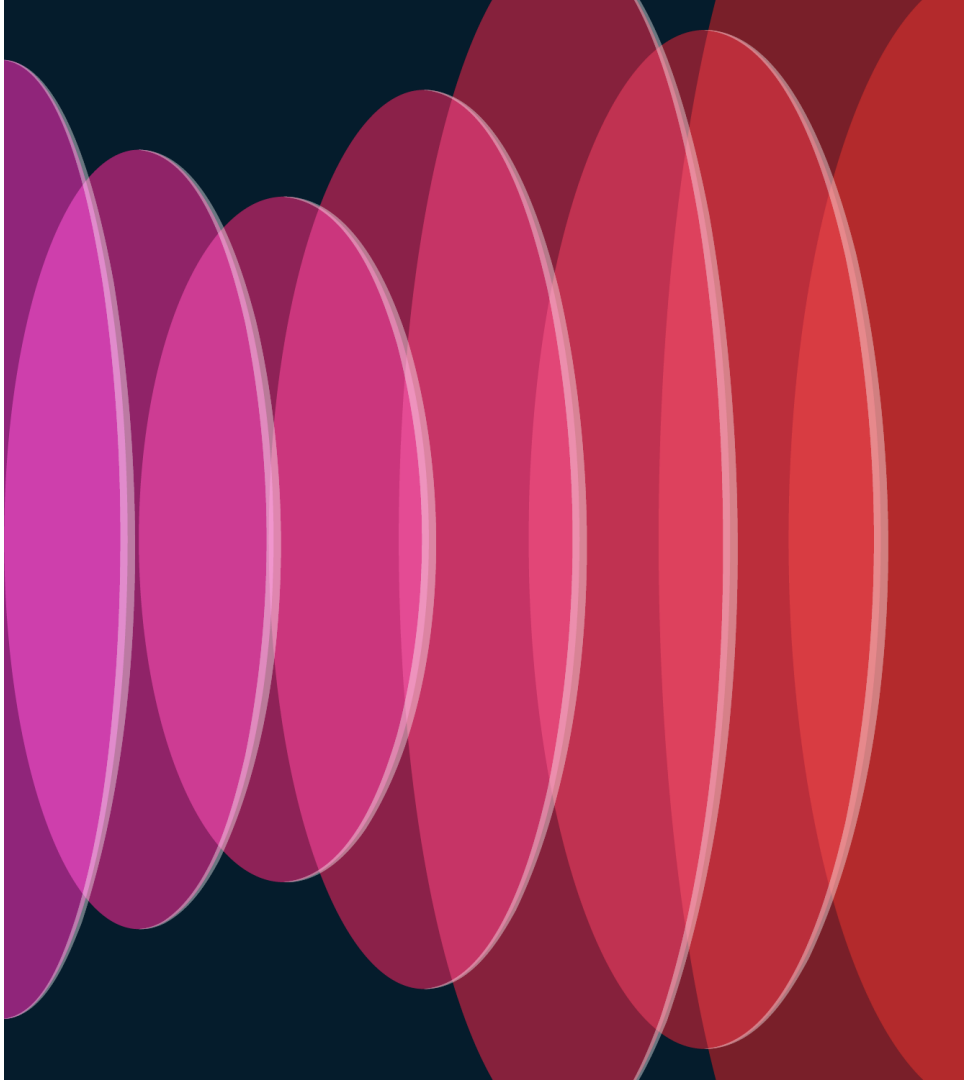
Advantages

- Provide Quantum Resistant Cryptography “TODAY”.
- Ensures Backward Compatibility.

Disadvantages

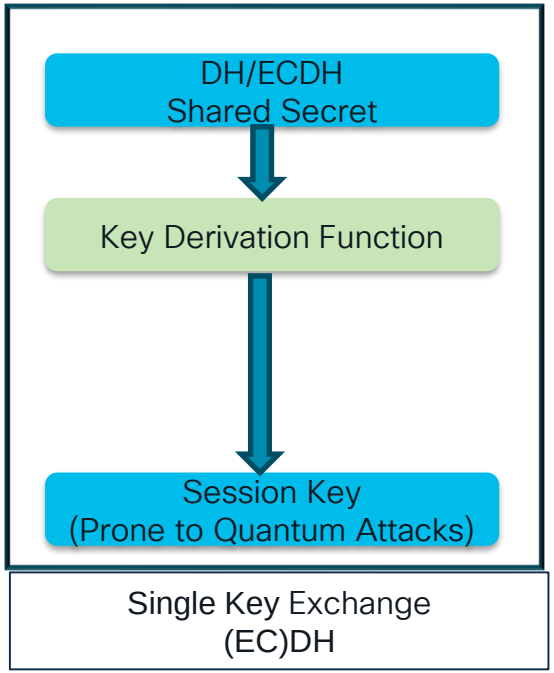
- Scalability challenges with Remote Access VPN users

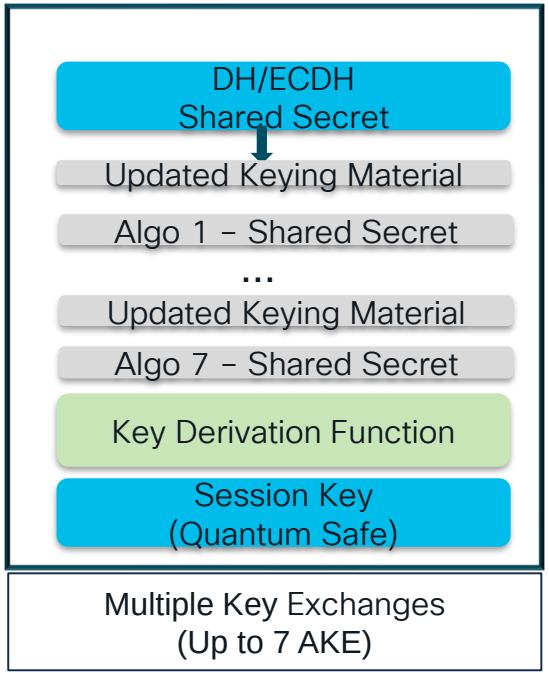
Multiple Key Exchange



VPN IKEv2/IPSec
Multiple Key Exchanges

VPN IKEv2/IPSec
Multiple Key Exchanges





VPN IKEv2/IPSec Multiple Key Exchange

Advantages

- Backward Compatibility.
- Provide Cryptographic Agility.
- Scalable
- Applicable to S2S and RA-VPN.

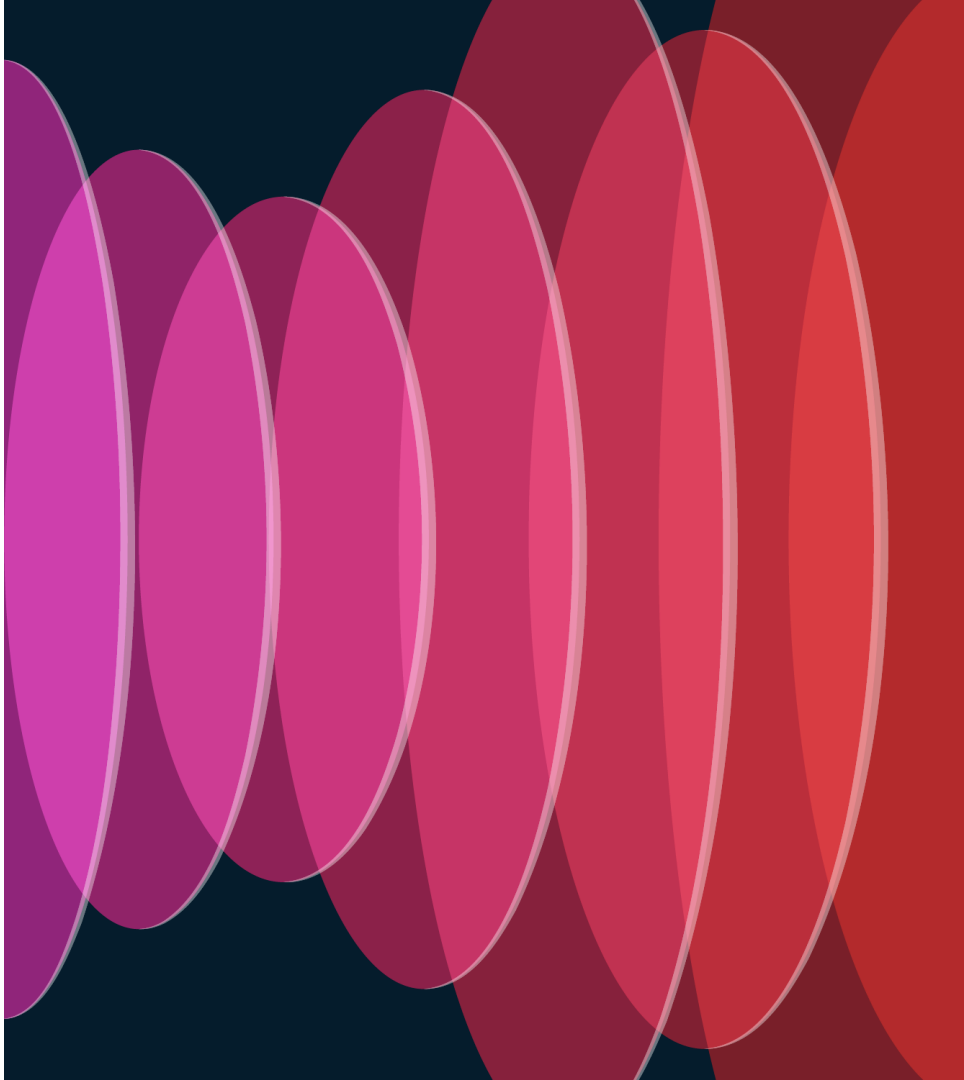
Disadvantages

- Efficiency
- Performance

Key Take Aways

- Advancements in quantum computing makes Public Key Cryptography insecure.
- Mitigation of the quantum computing threat is quantum safe cryptography.
- Organizations should start planning the transition to post quantum cryptography

Q & A



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:
  anubalas@cisco.com
  avetrive@cisco.com

Thank you