cisco Live!

Let's go

#CiscoLive

The bridge to possible

Threats to Public Key Cryptography and Quantum-Secure Solutions

Stephen DiAdamo, Research Scientist

BRKETI-1302

Cisco Webex App

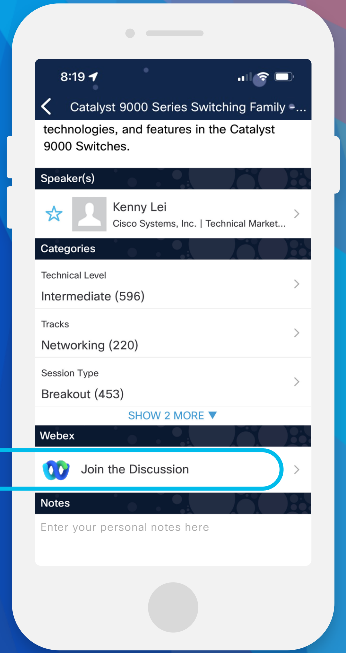
Questions?

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 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKETI-1302

Agenda

1. Preliminaries
2. Quantum Threats to Cryptography
3. Quantum-Secure Solutions
4. Options for Quantum Network Deployment
5. Conclusion

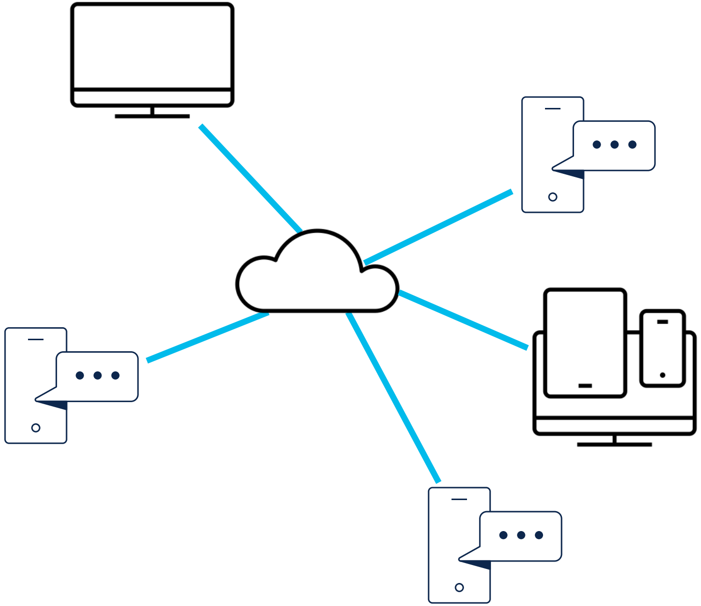
Biography

- Research Scientist at Cisco Quantum Lab
- From Canada, living in Germany
- PhD in quantum networking
- Research Focuses:
  - Quantum networks
  - Quantum information theory
  - Distributed quantum computing
  - Simulation tools for quantum networks

Communication Networks

Communication Networks

- A system that allows for the exchange of information between multiple devices or nodes
- Includes components such as routers, switches, and transmission lines to transfer data between different points in the network
- Communication networks can be used for various applications



The Internet

- A global communication network
- It uses various standardized communication protocols to facilitate the transfer of data

Security on the Internet

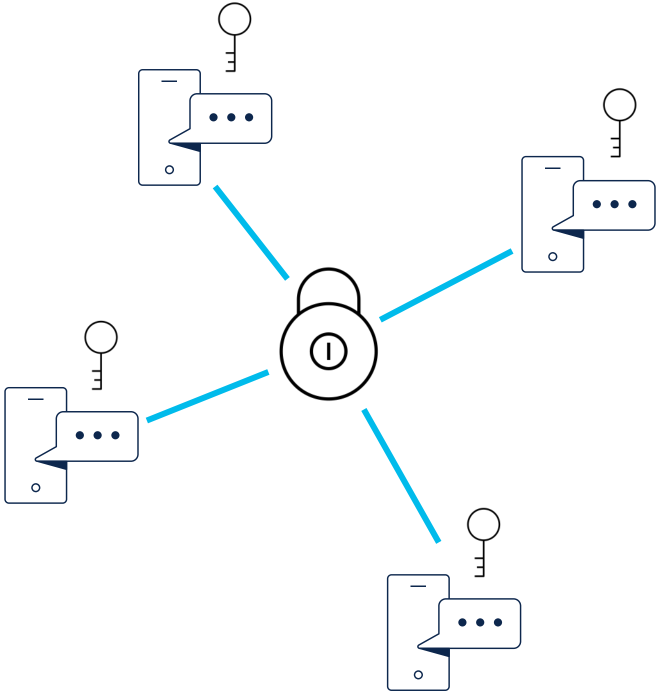
Encryption based on cryptography and authentication protocols are used to secure data

Firewalls and intrusion detection systems are also used to protect network access

Cryptography

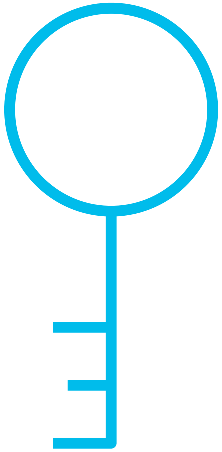
Cryptography

- The study of sending secret messages in the presence of adversaries
- Commonly done with “private” or “public” keys
- Security can be added using tamper-detecting methods



Key-Based Cryptography

- Uses a key, or several keys, to encrypt data
- Mostly split into public and private key cryptography
- Is widely used for securing online communication

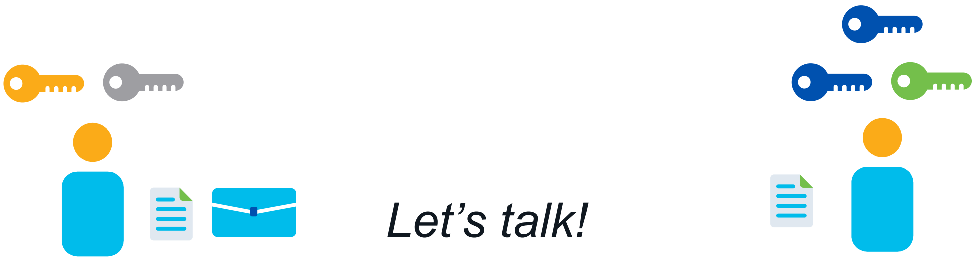


Private Key Cryptography

- Private keys are known only to the communicating parties
- When all parties share the same key, it is known as a symmetric key
- Distribution is difficult and often requires meeting in person or using a trusted courier

Public Key Cryptography

- The study of cryptographic protocols that work using public keys
- Public keys are generally paired with a private key
- Main type of cryptography for the Internet, one popular scheme is RSA



RSA-Based Public Key Cryptography

- The RSA algorithm generates a pair of keys, one for encryption and one for decryption
- The keys are generated using a complex mathematical formula that involves selecting two large prime numbers and using them to generate the keys
- Breaking RSA requires the ability to perform prime factorization

Quantum Information Basics

Qubits and Photons

- A qubit is the basic unit of quantum information
- A qubit can be in a superposition of binary states, meaning it can represent both 0 and 1 at the same time
- Qubits can be entangled, a property where the state of one qubit is dependent on the state of another qubit

Qubit Manipulation and Measurement

- Qubit state manipulation is the ability to prepare and control the state of a qubit
- Can be done through applying quantum gates or manipulating the system's environment
- A quantum measurement extracts information from a bit
- The measurement process can collapse the quantum state of the system, revealing a classical output result

Quantum States Cannot be Copied

- It is impossible to create an identical copy of an arbitrary unknown quantum state
- The act of measuring the state would necessarily disturb a superposition
- The no cloning theorem plays a crucial role in the security of quantum cryptography protocols

Entanglement

- A phenomenon where two or more qubits become correlated even when physically separated
- Allows protocols to perform correlated operations
- Maintaining entanglement is a major challenge in quantum information science due environmental sensitivity

Computing with Qubits

- The act of using qubits and quantum phenomena to perform computation
- Quantum computers use “superposition” and “entanglement” to compute many answers at once, but only one answer can be extracted at a time
- Quantum computers are difficult to build and will require many innovations

Threats to Public Key Cryptography

Quantum Threat to Public Key Cryptography

- Prime factorization is difficult to perform on classical computers
- Peter Shor invented a quantum algorithm that can perform prime factorization efficiently
- The threat of Shor's algorithm has created the field of "Post-Quantum Cryptography"
- Post-Quantum Cryptography is cryptography under the assumption that adversaries have quantum computers (sometimes even unlimited computational power)

Shor’s Algorithm

- A quantum algorithm that can efficiently factor large numbers into their prime factors
- First prepares a superposition of all possible inputs, then applies a quantum Fourier transform to the superposition
- Has the potential to be exponentially faster than classical algorithms for prime factorization

Is Shor’s Algorithm Really a Threat?

- To perform Shor’s algorithm may require millions of qubits with full quantum error correction
- Error corrected quantum computers are predicted to be 20 - 50 years away, so why bother worrying about this now?

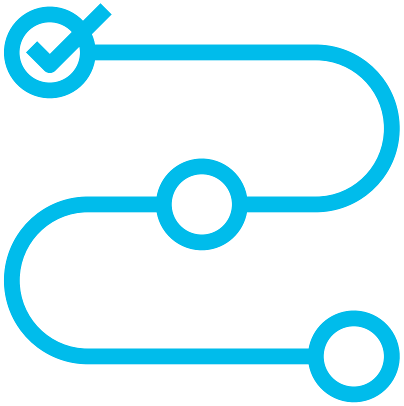
Why care about Shor’s Algorithm?

- Generally, it requires (at least) a 10-year buffer between when a new cryptographic protocol is invented and when it can be deployed wide-scale

- Can eavesdrop on communication now, store the data, and in 50 years, decrypt the information when EC’d quantum computers exist

What should we do?

- Continue efforts on quantum-secure security including both QKD and PQC
- Prepare for a change in encryption algorithms
- Collaborate
- Develop test beds



Quantum-Secure Security

A Brief Overview of Post-Quantum Crypto

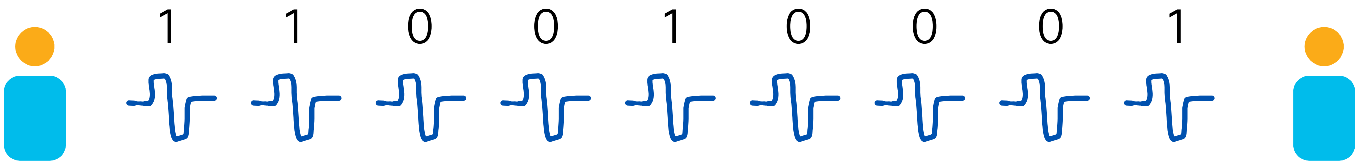
- A type of “classical” cryptography designed to be resistant to attacks by quantum computers
- Can uses lattice-based cryptography that is believed to be hard even for quantum computers to solve

Downsides of Post-Quantum Crypto

- Added computational complexity
- Can have larger key sizes
- No proof of security

Quantum Key Distribution

- Uses properties of quantum mechanics to ensure no eavesdropper is present during key exchange
- Relies on entanglement being "monogamous" and the "no-cloning" theorem
- Already sold as a commercial product



Protocols for Quantum Key Distribution

Entanglement based protocols

BB84

Alice

1) Generate 2 random binary strings: B_a *and K*

2) When $B_{a,i} = 0$, use the Z basis to prepare K_i, otherwise use the X basis.

3) When all bits are transmitted, reveal B_a to Bob

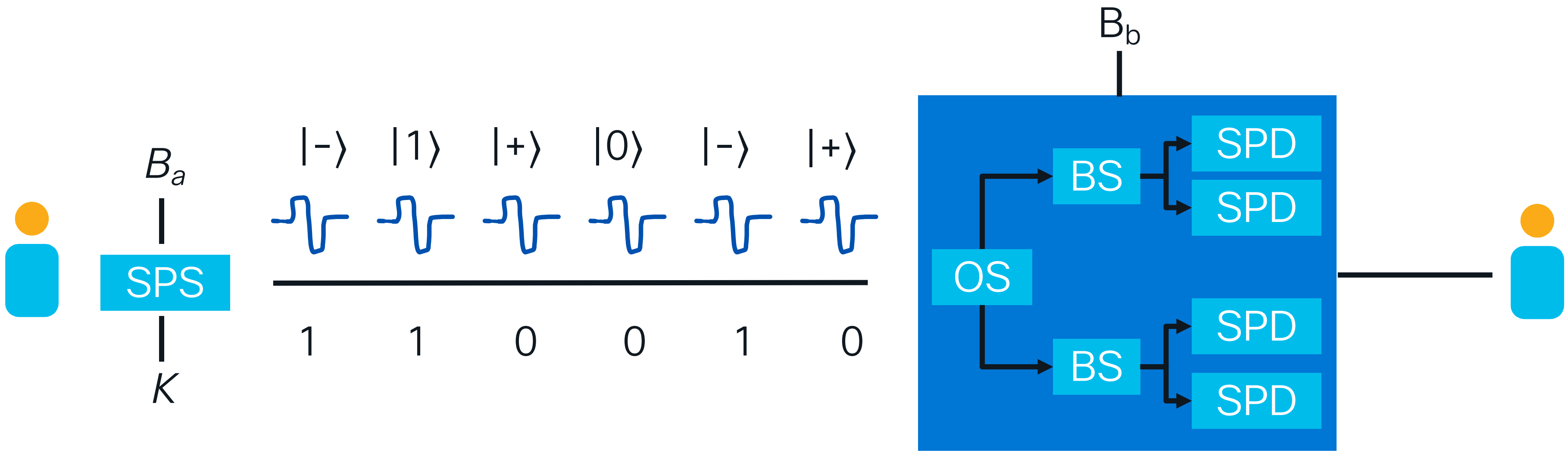
Bob

1) Generate 1 random binary string: B_b

2) When $B_{b,i} = 0$, measure the incoming qubit in the Z basis, otherwise measure in the X basis

3) When Alice reveals B_a, respond with the indexes that matched with B_b

BB84



Pros and Cons of QKD

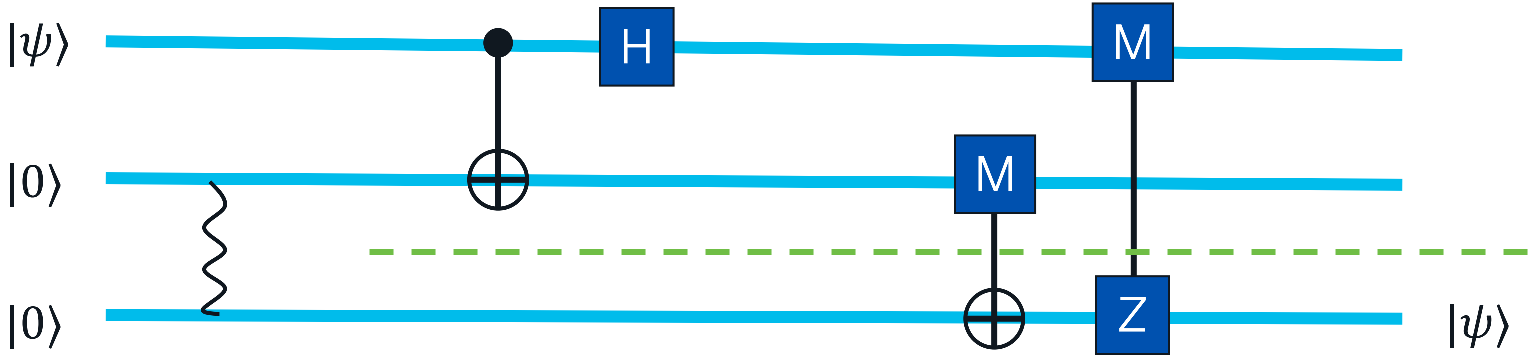
- Provably secure theoretically
- In practice, information can leak from “side-channels”
- Human error is not considered in the proof of QKD
- QKD is possible with today’s Internet technology, where no other PQC has been shown to have the same security

Deploying Quantum Networks

How can quantum states be transferred?

1. Directly sending the state over a quantum channel

2. Using quantum entanglement to teleport the quantum state



Quantum Network Hardware Components

- **Quantum transmitters:** Generate and send quantum states, such as single photons, through optical fibers or free space.

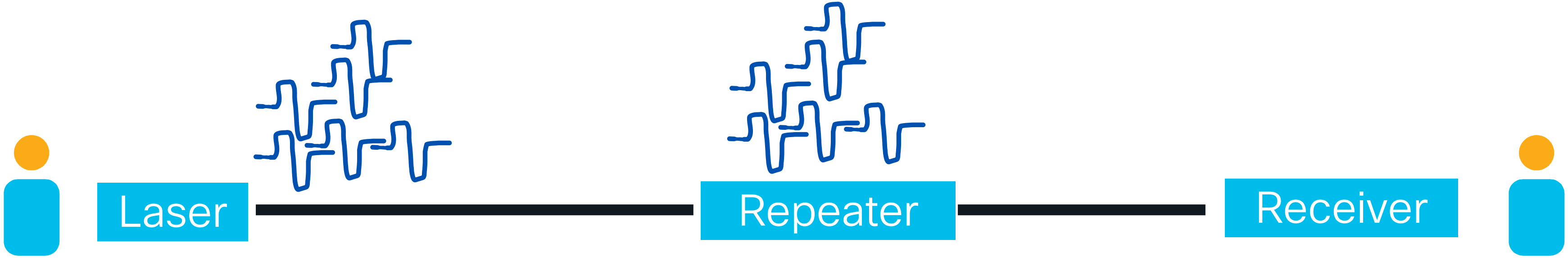
- **Quantum receivers:** Detect and measure the quantum states sent by the transmitter

- **Quantum memories:** Store quantum states for a short period of time, allowing for the synchronization of quantum communication protocols.

- **Classical communication infrastructure:** A quantum network also requires classical communication infrastructure to coordinate and control the quantum components.

Sending Classical Information

Sending Classical Information



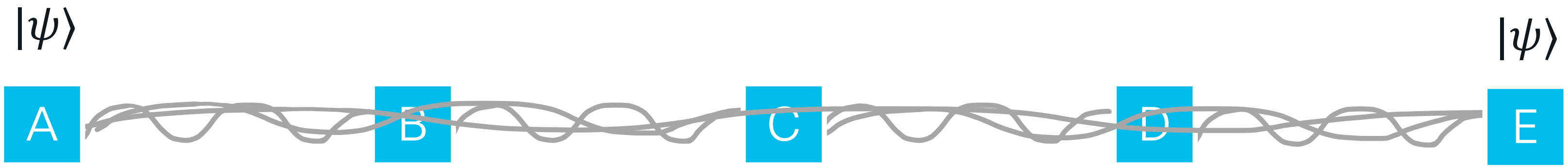
Sending Quantum Information

Issues with Direct Transmission

- Direct transmission of quantum states is very lossy
- Transmitting a quantum state over fiber optic cables is possible only up to a few hundred KMs
- In free-space networks (e.g., satellite) further distances are attainable, but not unlimited
- Classical methods of amplifying and error correction are possible, new methods are needed to surpass the finite distance limitations

Long-Range Entanglement Distribution

- Idea: Create entanglement and use quantum teleportation
- Distributing entanglement over large distances faces the same challenge as direct transmission, but there are key benefits:
  - Entanglement does not contain information
  - Entanglement swapping to distribute over long distances



Entanglement Swapping: Challenges

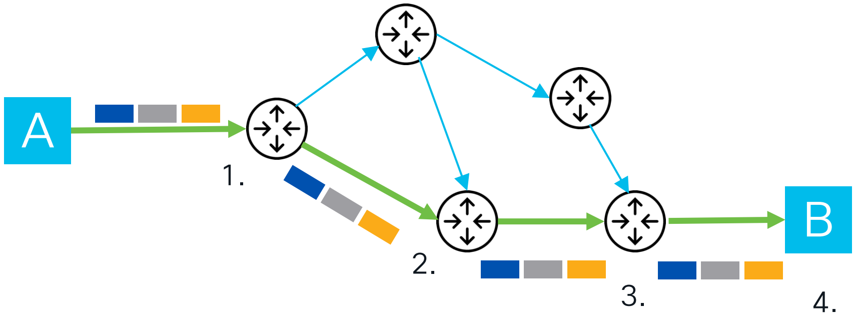
- Probabilistic task that very often fails
- Requires a high level of synchronization
- Requires a quantum memory
- Entanglement swapping is the most accessible solution now, other solutions require even more advanced technology

Direct Transmission-Based Quantum Networks

- At smaller scales, a direct transmission-based network integrated into the fiber technology can be used
- Integrating quantum networks with Internet technology leads to a "co-existence network"
- Packet switching can be used which has many advantages for certain networks types

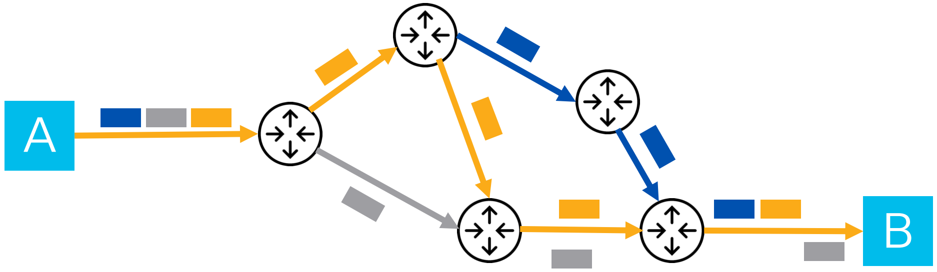
Circuit Switching

- Route is reserved
- Frames arrive in order



Packet Switching

- Route is dynamic
- Frames can arrive out of order

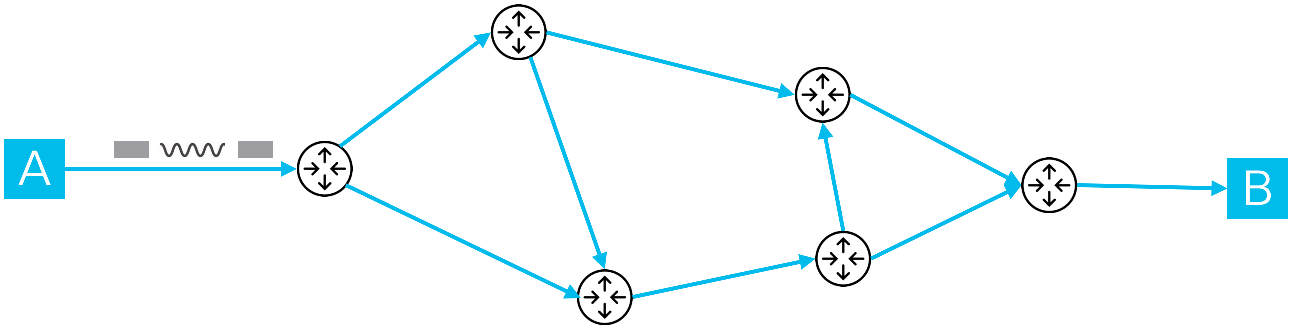


Integrating with Classical Networks

- Using existing deployed fiber for quantum networks is highly attractive
- It will require a high level of coordination and noise mitigation
- Quantum and classical routing algorithms will need to be compatible

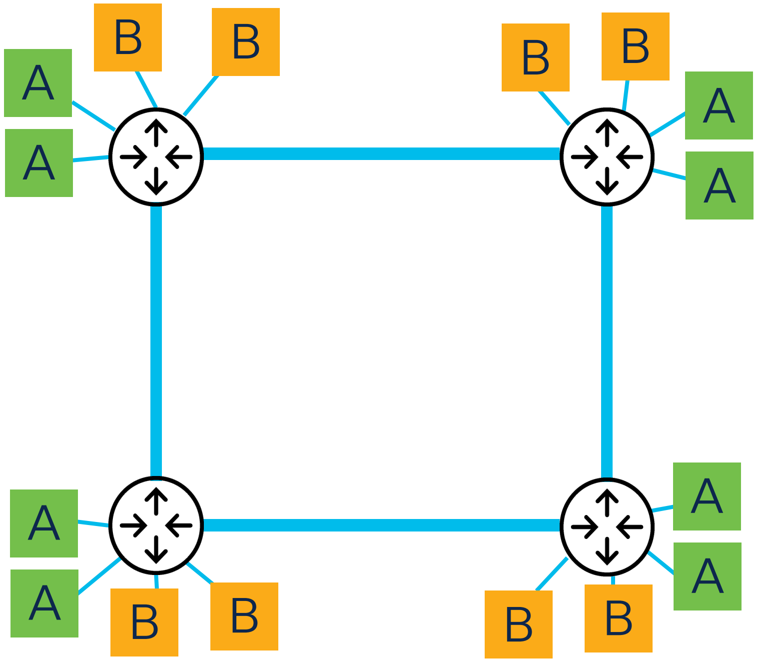
Packet Switching in Quantum Networks

- The frames are hybrid classical-quantum data frames
- Design compatible with both classical and quantum traffic



DiAdamo, Qi, Miller, Kompella, and Shabani. Phys. Rev. Research **4**, 043064 (2022).

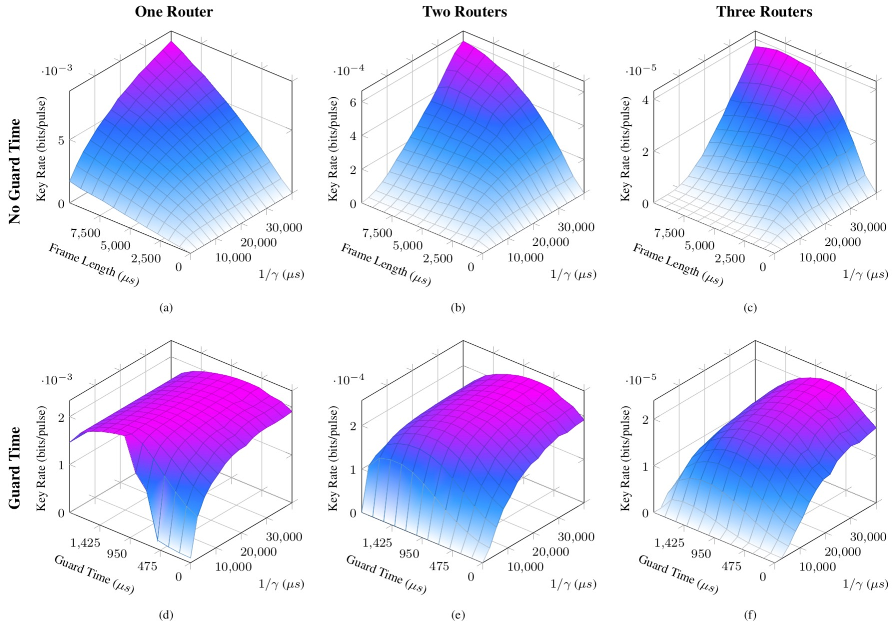
Packet-Switched QKD Networks



Mandil, DiAdamo, Qi, and Shabani. arXiv preprint arXiv:2302.14005 (2023).

Packet-Switched QKD Networks

- Practical key rates may be achieved without any optical storage
- Limited storage time in a fiber delay line can enhance performance
- QKD in a packet-switched network is feasible with today's technology!



Mandil, DiAdamo, Qi, and Shabani. arXiv preprint arXiv:2302.14005 (2023).

Conclusions

Summary

- Quantum algorithms can break the public key encryption schemes but building a quantum computer is very challenging
- QKD and PQC are methods for maintaining security in the era of quantum computing
- Techniques for long distances transmission cannot be used directly for quantum networks
- Robust entanglement generation and manipulation will be critical for a global quantum Internet

Outlook

- Quantum technology is rapidly advancing, and we should be preparing for future security threats now
- A likely solution for future security will be a hybrid PQC / QKD model, but is highly specific to the application
- Quantum and classical networks will, in some ways, be unified

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

Thank you

Let’s go