Post-Quantum

Cryptography Conference

Communication among Financial Institutions: What are the available answers to the quantum threat?

As central banks, financial institutions, and payment platforms rely heavily on secure communication for transactions, client information, and regulatory compliance, the advent of quantum computing poses a significant threat to some of the classical encryption methods underpinning these systems. Quantum computers, with their potential to solve integer factorization (used in RSA) and discrete logarithm problems (used in ECC) exponentially faster than classical computers, could break widely used cryptographic systems like RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), which secure most financial communications today. This quantum threat calls for proactive strategies to ensure the long-term security of financial networks. In this work, we have explored the available solutions, working closely with different encryption technologies and key management systems. The network is based on cloud VPN, providing a high level of cryptoagility, or the ability to switch between cryptographic algorithms efficiently, and shows significant interoperability among providers featuring standard protocols."

Giuseppe Bruno
Head of Division at Bank of Italy

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity (“business league”) under Utah law (10462204-0140) | pkic.org

PKI Consortium

Building a Quantum-Safe Communication Infrastructure

Giuseppe Bruno

January 16, 2025

Post-Quantum Cryptography Conference

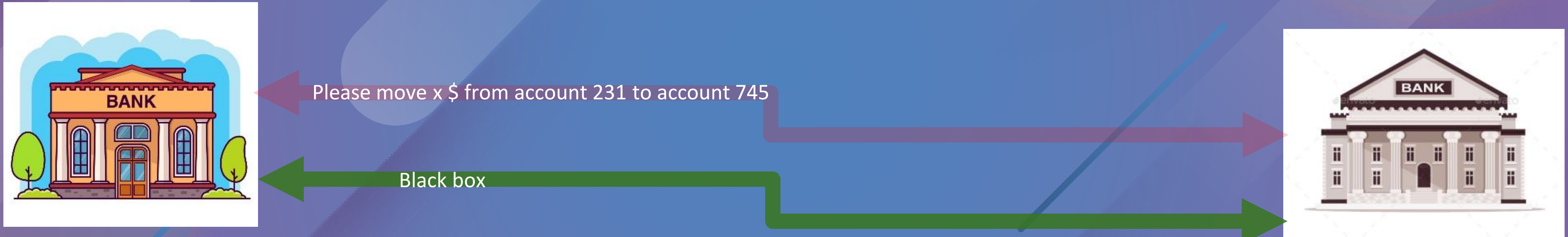
University of Texas, Austin

BANCA D'ITALIA
EUROSISTEMA

Technological showcase

The need of Encryption

It doesn’t seem right. Anybody can see and change the message

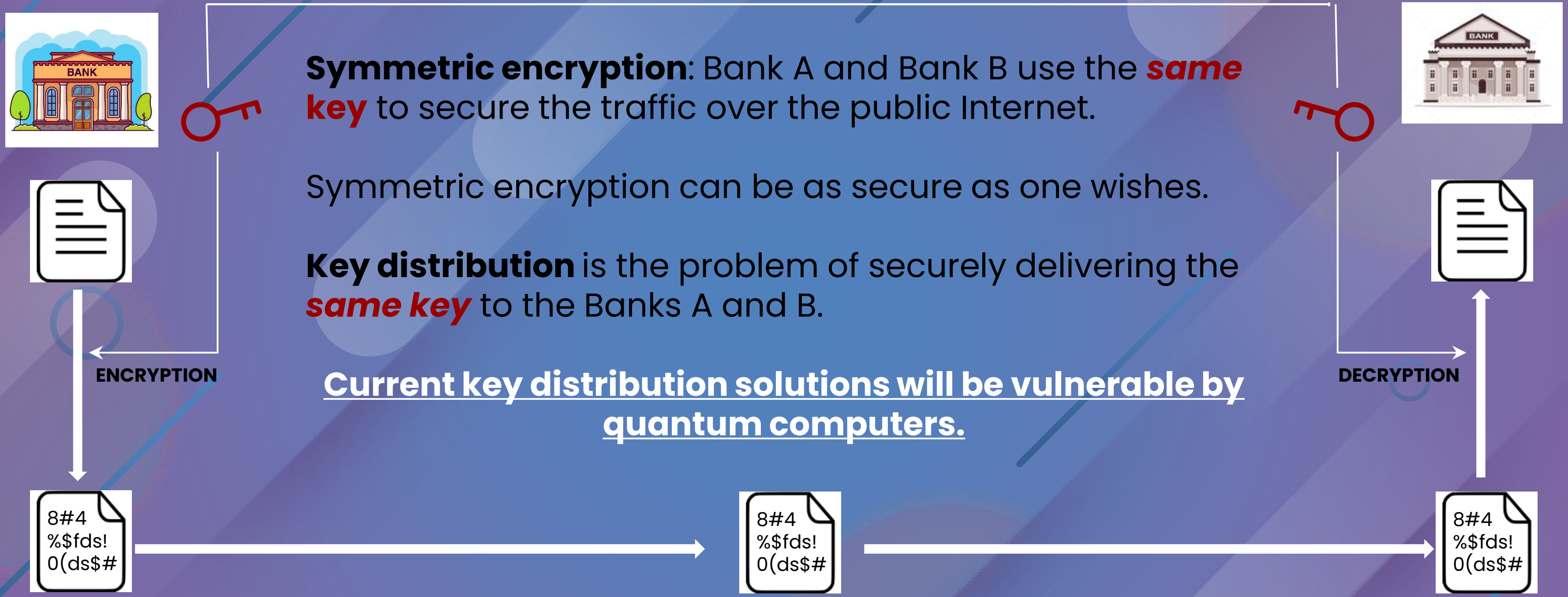


Please move x $ from account 231 to account 745

Black box

Now I feel much more relieved

The Problem of Key Distribution



Symmetric encryption: Bank A and Bank B use the ***same key*** to secure the traffic over the public Internet.

Symmetric encryption can be as secure as one wishes.

Key distribution is the problem of securely delivering the ***same key*** to the Banks A and B.

Current key distribution solutions will be vulnerable by quantum computers.

Key Distribution in a Quantum World

Quantum Key Distribution

C. Bennet & G. Brassard

Solve the problem using **Physics**

Symmetric Key Establishments

Claude Shannon

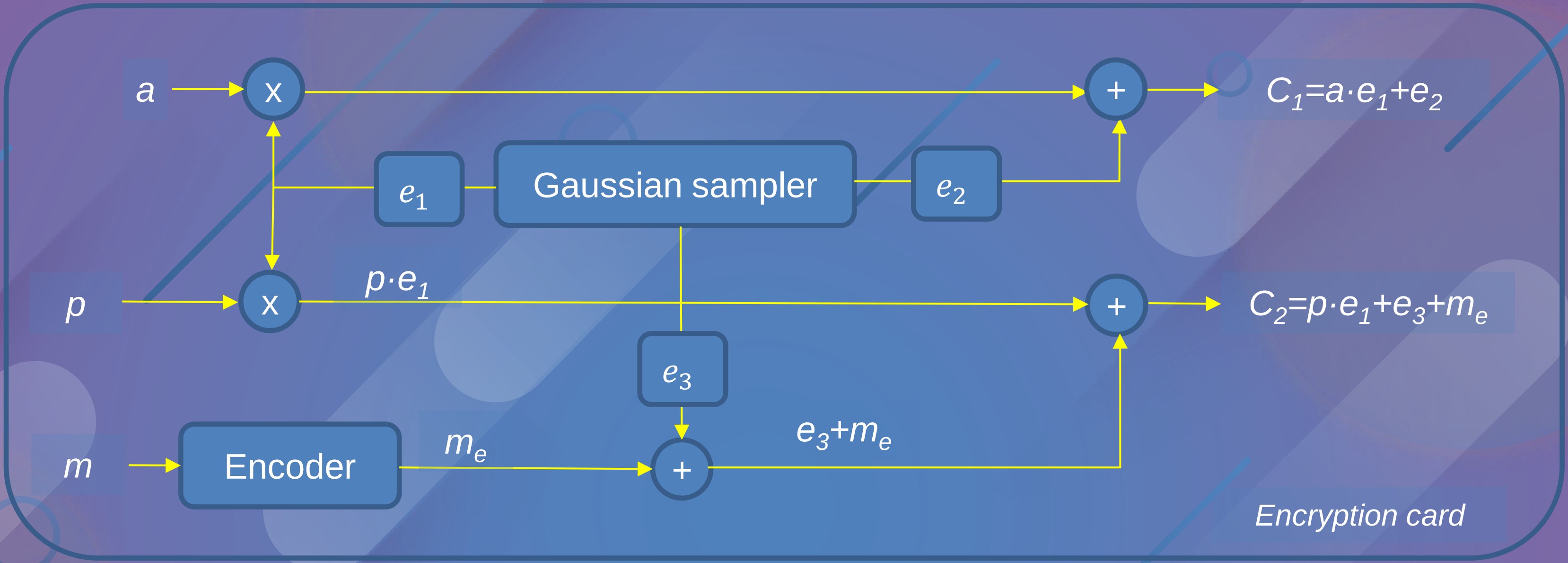
Solve the problem using **Logistic and Entropy**

Post-Quantum Cryptography

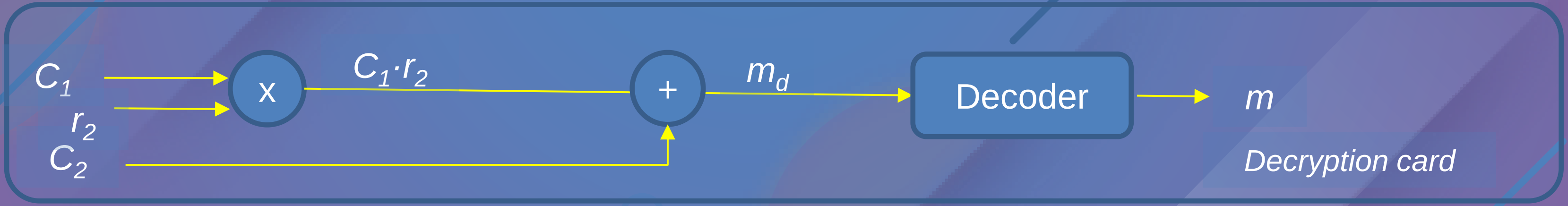
Oded Regev

Solve the problem using **Mathematics**

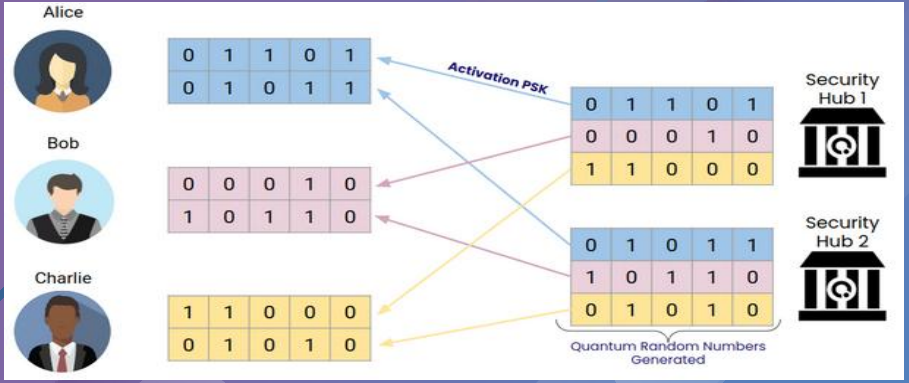
Post Quantum Cryptography R-LWE



Key gen: r$_1$, r$_2$ and a are random polynomials. $p \leftarrow r_1 - a \times r_2$ pub key is (a, p) priv key is r_2



Distributed Symmetric Key Exchange



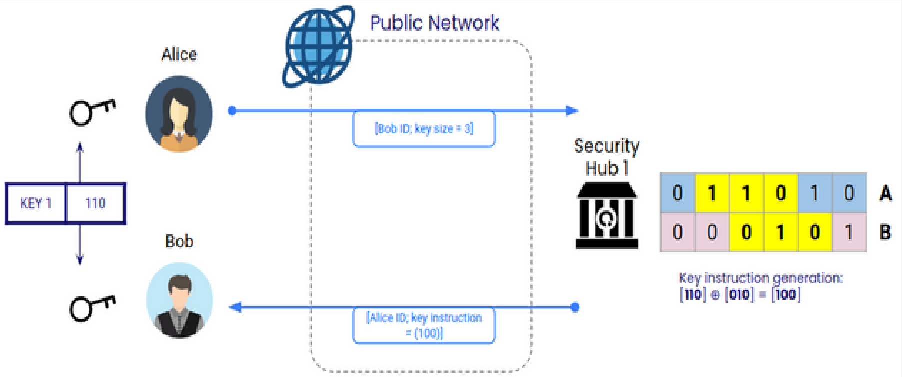
Alice:
0 1 1 0 1
0 1 0 1 1

Bob:
0 0 0 1 0
1 0 1 1 0

Charlie:
1 1 0 0 0
0 1 0 1 0

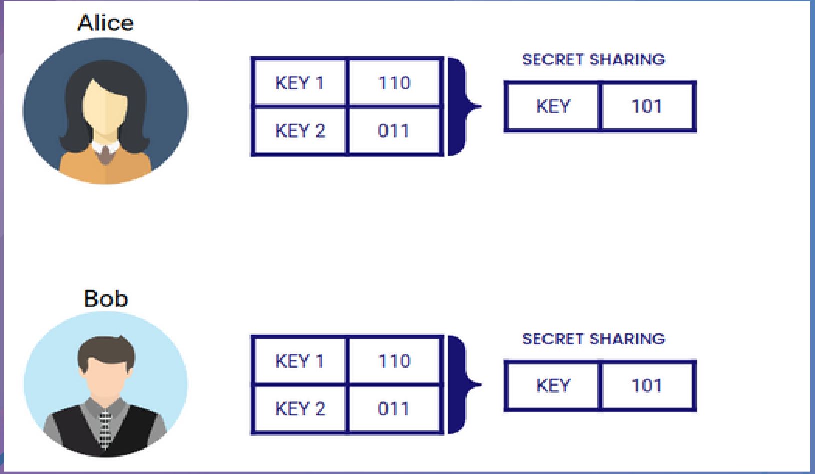
Security Hub 1:
0 1 1 0 1
0 0 0 1 0
1 1 0 0 0

Security Hub 2:
0 1 0 1 1
1 0 1 1 0
0 1 0 1 0



A: 0 1 1 0 1 0
B: 0 0 0 1 0 1

Key instruction generation:
[110] ⊕ [010] = [100]



Alice:

KEY 1	110
KEY 2	011

KEY	101

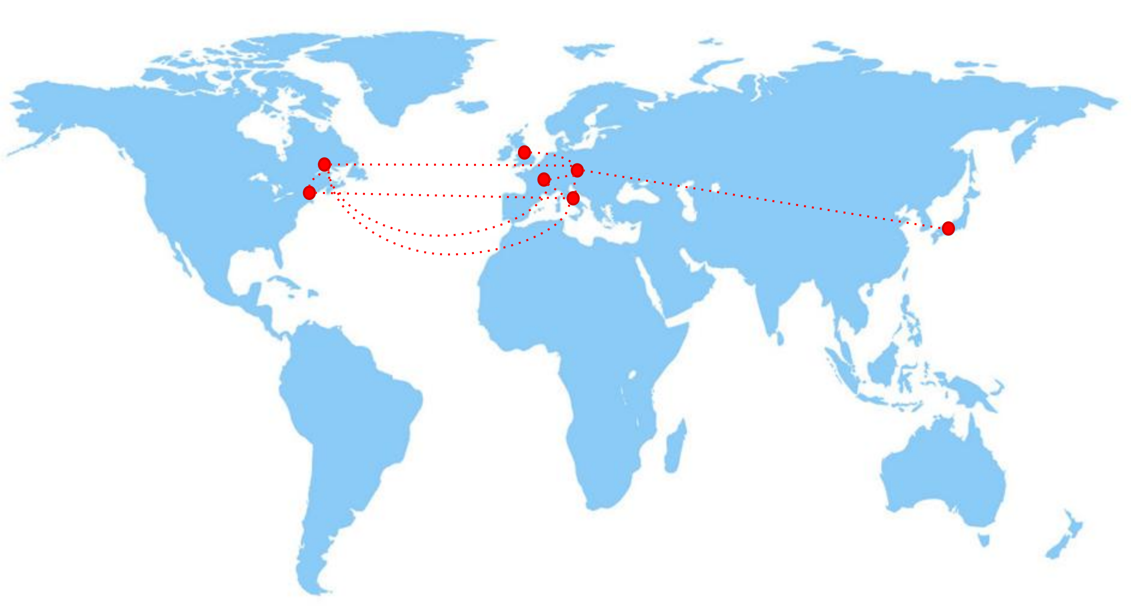
Bob:

KEY 1	110
KEY 2	011

KEY	101

Trust removal. Alice and Bob generate a key share from each Security Hub, and then combine these shares using a secret sharing protocol. This way, they remove the need to trust any single Security Hub.

Market Readiness

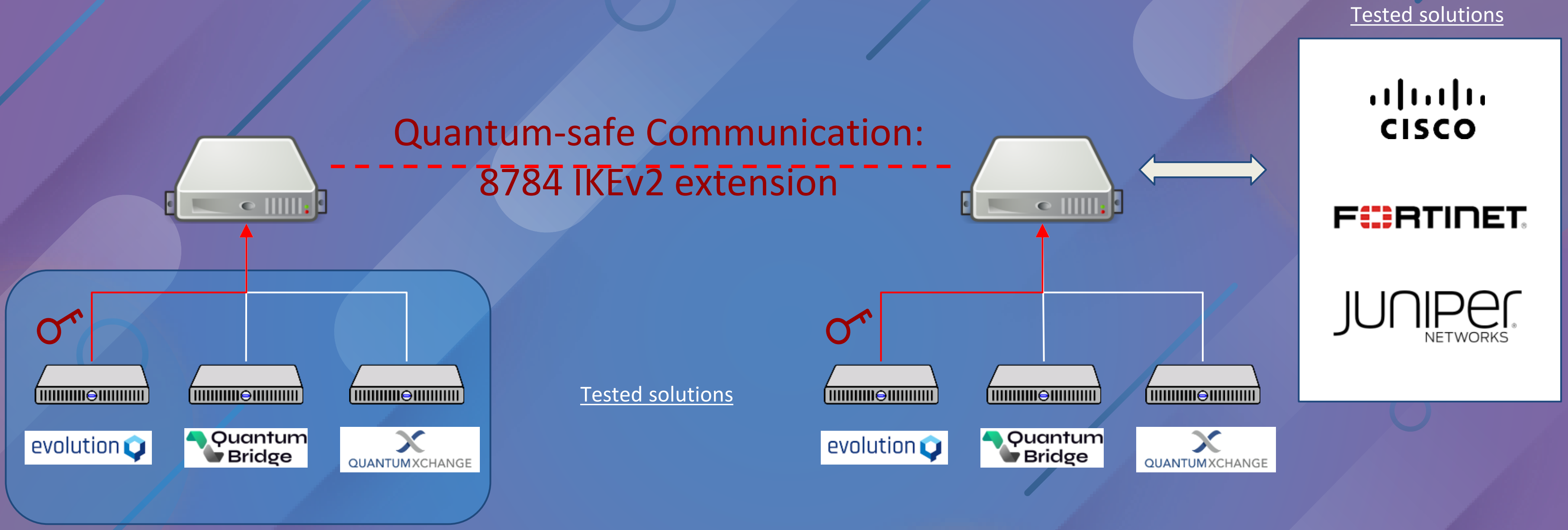


Case Study: a global quantum safe network

Case study results:

- QKD, DSKE, and PQC integrated in existing infrastructure.
- Multiple vendors: the market is contestable.
- The technology is **ready today**.

Market solutions: cryptoagility & interoperability



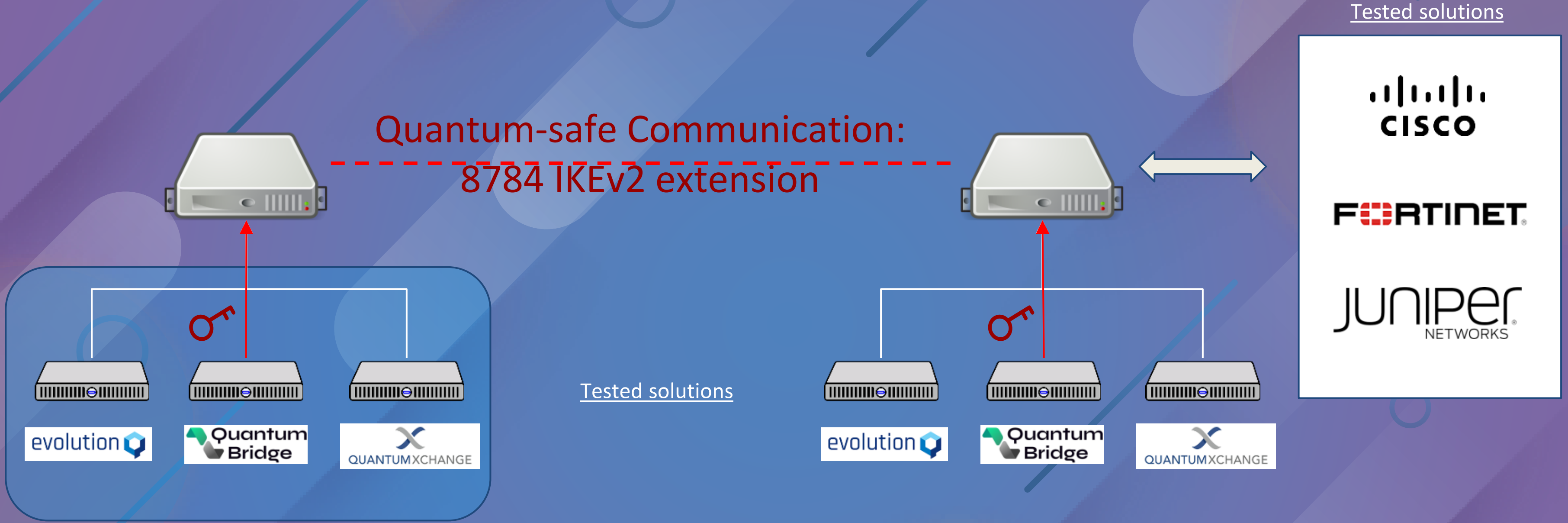
Quantum-safe Communication: 8784 IKEv2 extension

Tested solutions

Tested solutions

Different protocols and vendors can interoperate to provide quantum-safe communication

Market solutions: cryptoagility & interoperability



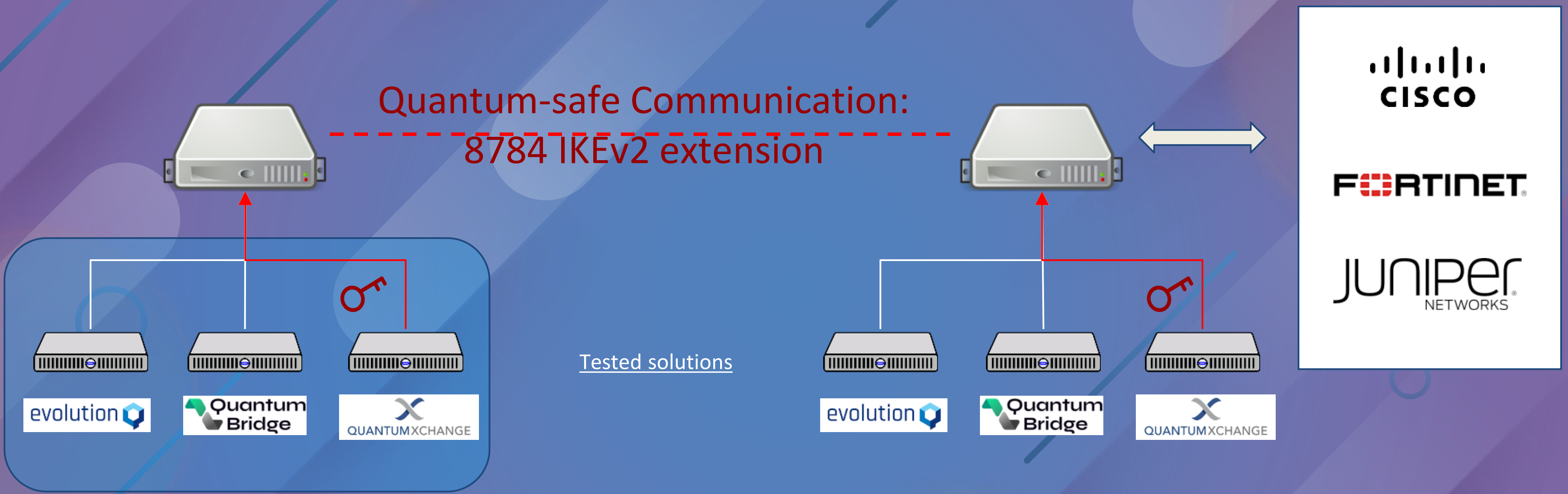
Quantum-safe Communication:
8784 IKEv2 extension

Tested solutions

Tested solutions

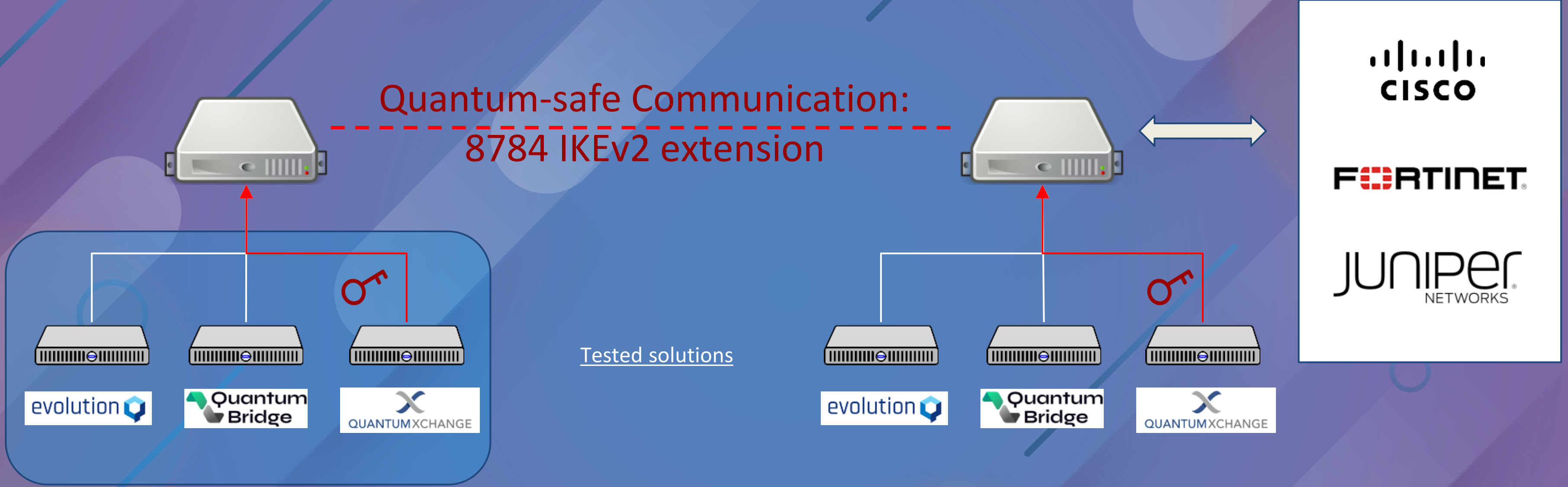
Different protocols and vendors can interoperate to provide quantum-safe communication

Market solutions: cryptoagility & interoperability



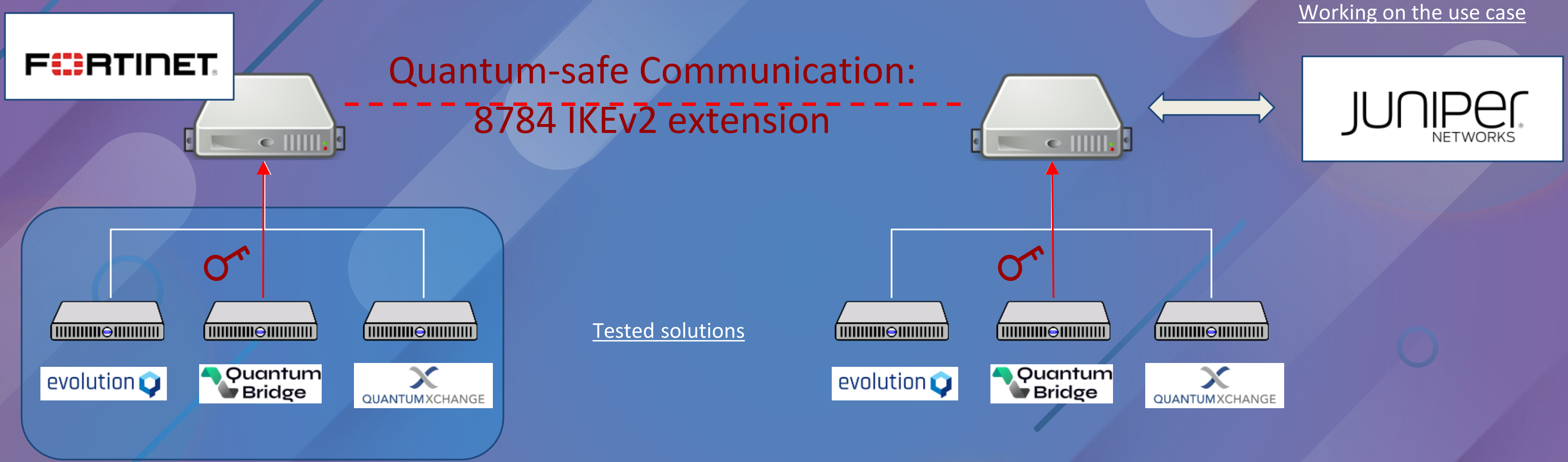
Different protocols and vendors can interoperate to provide quantum-safe communication

Can we interoperate between different encryptors?



Different protocols and vendors can interoperate to provide quantum-safe communication

Can we interoperate between different encryptors?



Quantum-safe Communication: 8784 IKEv2 extension

Working on the use case

Tested solutions

Different protocols and vendors can interoperate to provide quantum-safe communication

Thank you very much for your attention:

Questions?