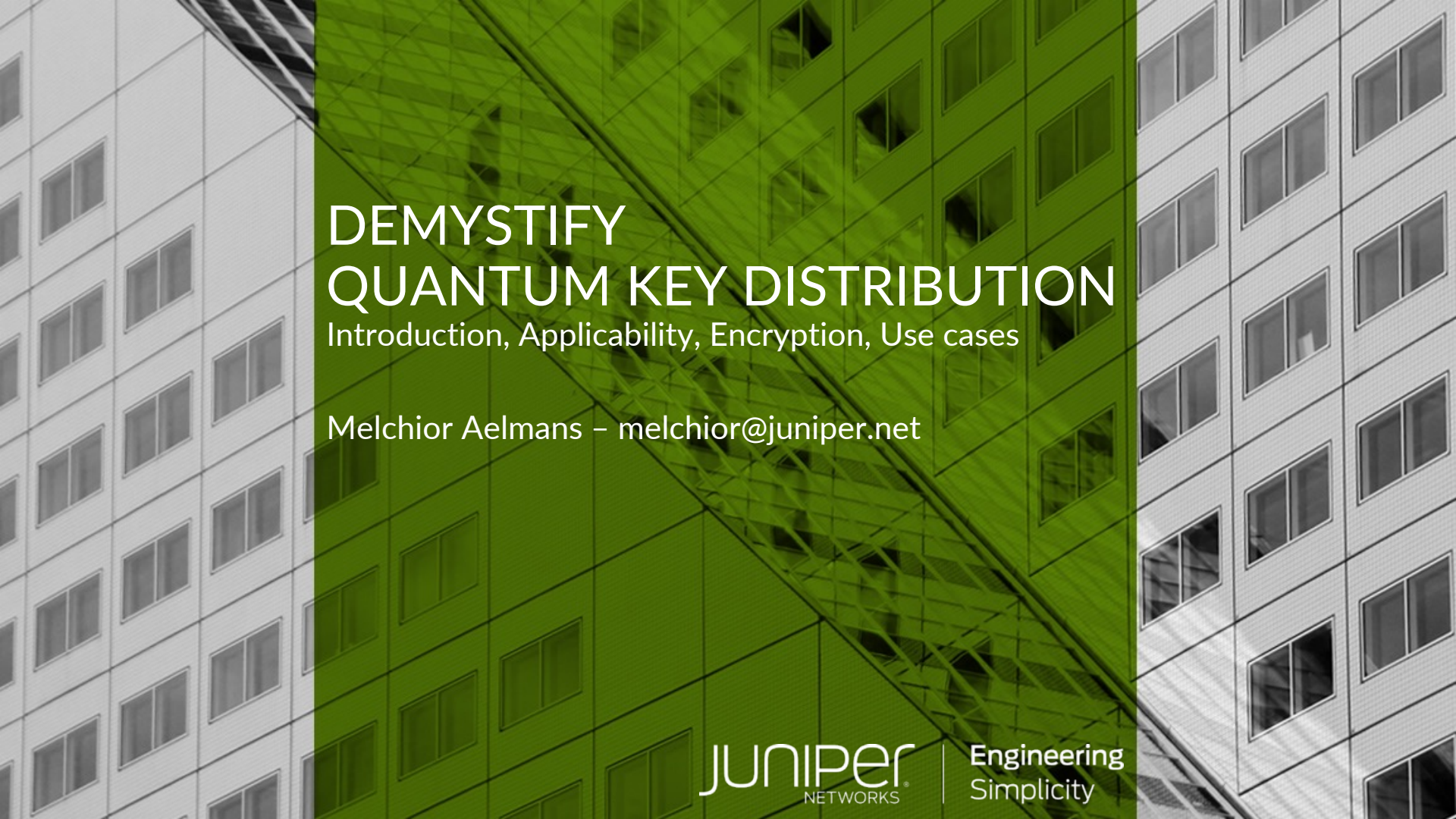


DEMYSTIFY QUANTUM KEY DISTRIBUTION

Introduction, Applicability, Encryption, Use cases

Melchior Aelmans – melchior@juniper.net

Juniper Networks | Engineering Simplicity

AGENDA

- Introduction to Quantum Networking and Internet
  - Quantum language and terminology
- Demystify Quantum Key Distribution (QKD)
  - How does QKD work
- Pulling QKD and encryption together
- Internet Exchange Point use case
- What's next?

A tale about
Alice, Bob and Eve

POTENTIAL FIELDS OF INTEREST

There are three quantum technology areas that could be interesting for a Quantum Safe Strategy:

1. **Quantum Random Number Generators (QRNG)**

   QRNG has become a key enabling technology for quantum-level security in mobile devices, data centers and even medical implants, to name just a few current-day applications.

2. **Quantum Key Distribution (QKD)**

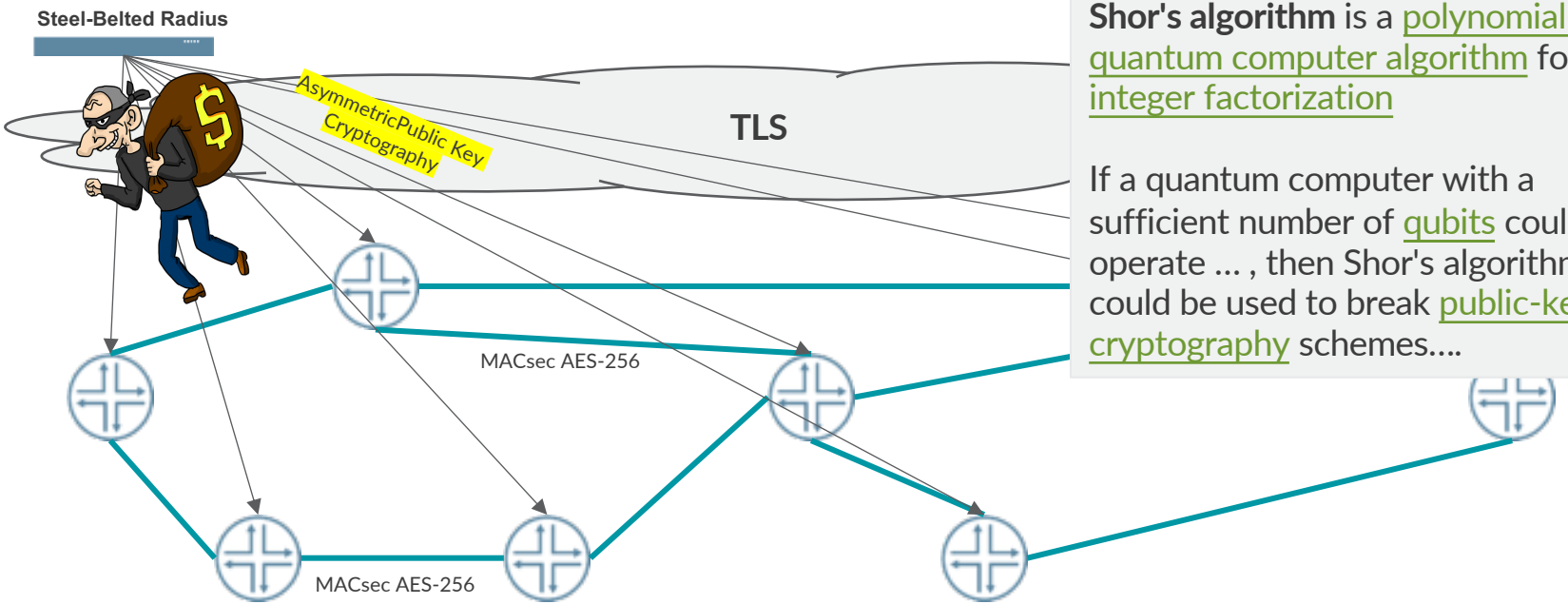
   QKD is a provably secure communication mechanism that utilizes the properties of quantum mechanics to share randomly generated symmetric encryption keys between two parties. The random secret keys are only known only to the endpoint parties and can not be intercepted by a third-party eavesdropper. This in contrast to traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions. These functions with the advent of quantum computing, can more quickly reverse the functions used to generate the keys.

   Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key is then used by any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel.

3. **Post Quantum Cryptography (PQC)**

   Post-quantum cryptography refers to mathematical cryptographic algorithms (usually public-key algorithms) that are thought to be more secure against a cryptanalytic attack by a quantum computer than current-day public-key algorithms.

PROBLEM STATEMENT: PUBLIC KEY CRYPTOGRAPHY SCHEMES



Problem:
Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization

If a quantum computer with a sufficient number of qubits could operate … , then Shor's algorithm could be used to break public-key cryptography schemes….

MACsec AES-256 has no known vulnerability itself from Quantum computers

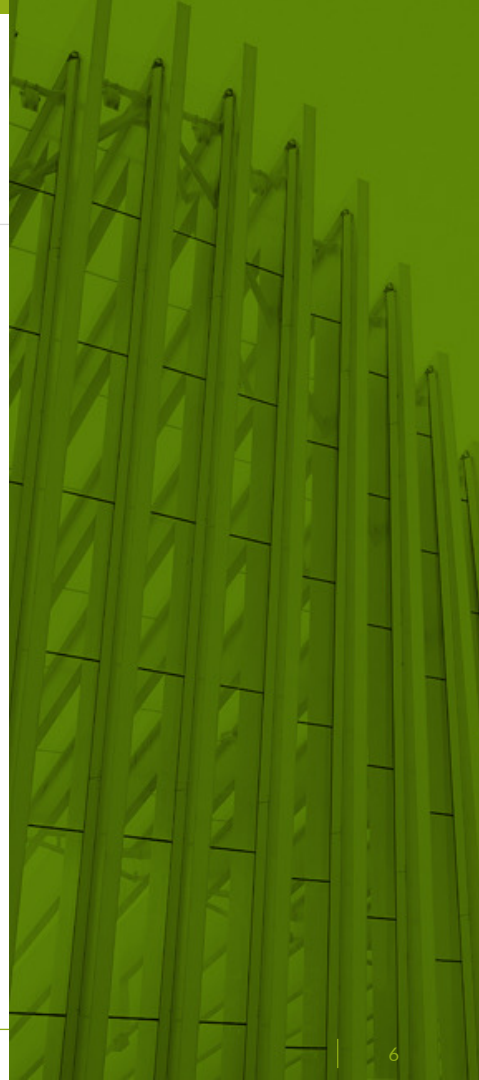
WHAT IS AND WHAT ISN'T? DEBUNKING!

- QKD is Key-Distribution using photons, it is NOT distribution of Quantum-Keys (what are those?).
- Post-Quantum Cryptography (PQC) is not the successor of Quantum Cryptography or QKD. It only tells us that the crypto algorithms have been invented after Quantum computers have been taken into account.
- Quantum Secure doesn't mean "quantums" (QKD) are protecting the network. It means the network is secure against attacks using Quantum Computers
- To use QKD requires ZERO Quantum Computers. Keys are generated through quantum-mechanic effects at room temperature, not computed.

Conclusion: It is less spooky than you might think!

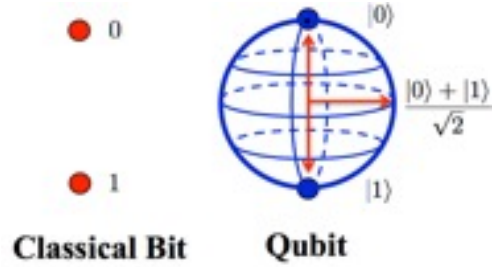
INTRODUCTION TO QUANTUM

- Quantum language and terminology



QUBIT

- A qubit (or quantum bit) is the quantum mechanical analogue of a classical bit.
- A classical bit can have the value zero or one.
- In quantum (computing) the information is encoded in qubits.
- A qubit can be in state $|0\rangle$, $|1\rangle$ or (unlike a classical bit) in a linear combination of both states. The name of this phenomenon is superposition.
- The most peculiar property of a Qubit is that it cannot be copied.
- Further reading: https://en.wikipedia.org/wiki/Qubit



SUPERPOSITION

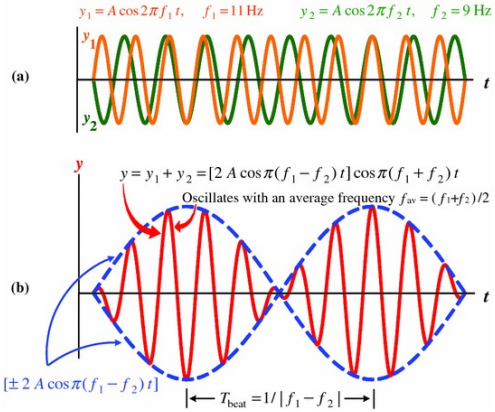
One of the properties that sets a qubit apart from a classical bit is that it can be in superposition. Superposition is one of the fundamental principles of quantum mechanics.

In classical physics, a wave describing a musical tone can be seen as several waves with different frequencies that are added together, superposed.

Similarly, a quantum state in superposition can be seen as a linear combination of other distinct quantum states. This quantum state in superposition forms a new valid quantum state.

Qubits can be in a superposition of both the basis states |0⟩ and |1⟩. When a qubit is measured (to be more precise: only observables can be measured), the qubit will collapse to one of its eigenstates and the measured value will reflect that state.

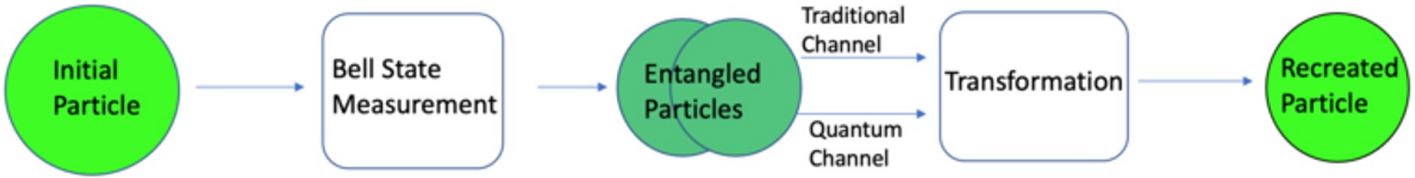
Further reading:
https://www.quantum-inspire.com/kbase/superposition-and-entanglement/



QUANTUM TELEPORTATION

Quantum teleportation is a technique for transferring quantum information (state) from a sender at one location to a receiver some distance away.

While teleportation is commonly portrayed in science fiction as a means to transfer physical objects from one location to the next, quantum teleportation only transfers quantum information.



The qubit held by Alice can be 0 as well as 1. If Alice measured her qubit in the standard basis, the outcome would be perfectly random, either possibility 0 or 1 having probability 1/2.

But if Bob then measured his qubit, the outcome would be the same as the one Alice got. So, if Bob measured, he would also get a random outcome on first sight, but if Alice and Bob communicated, they would find out that, although their outcomes seemed random, they are perfectly correlated.

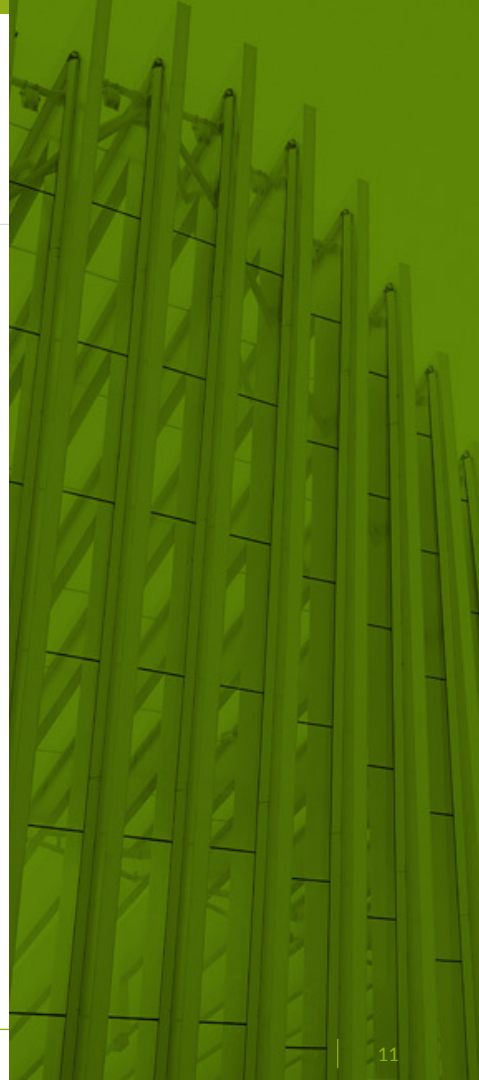
Further reading: https://en.wikipedia.org/wiki/Bell_state

ADVANTAGES AND CHALLENGES OF QUANTUM

	Details
Advantages and applications	• **No cloning:** qubits cannot be copied which makes them perfect for cryptography • **Superposition collapses:** when a qubit is measured the superposition collapses hence eavesdropping cannot go unnotified. • **Physics over math:** Quantum security relies on physics instead of math hence factoring keys is much harder (impossible).
Challenges	• **Decoherence**: The coherence of a qubit is its ability to maintain superposition over time. Environment, interactions with the external world cause the system to decohere. • **Qubit quality (fidelity)**: qubits in today's cloud-based quantum computers are not good enough for large scale systems. In some cases, the result we get can be indistinguishable from noise. • **Scaling**: We need to have innovations in the current ways we control wires, or multiple lasers, to create each qubit.

QUANTUM NETWORKING / INTERNET

- What is Quantum Networking
- Will there be a Quantum Internet?



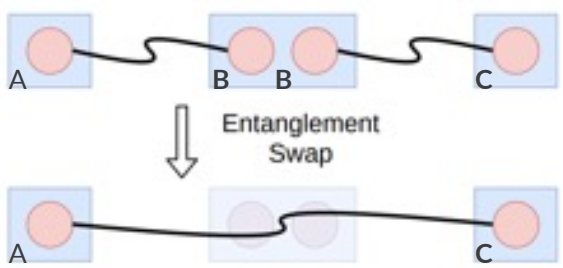
What is a Quantum Network? Or is it a Quantum Internet?

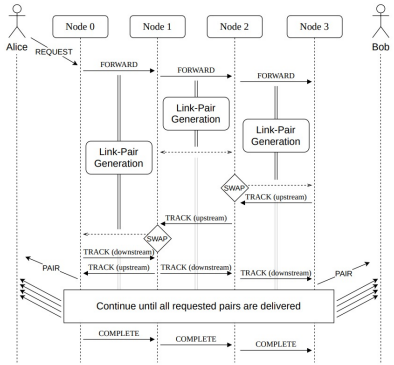
- Quantum networks facilitate the transmission of information in the form of qubits, between physically separated quantum end-nodes (quantum computers).
  - Physical (telecom) fiber or free-space. Currently only partly able to leverage xWDM due to loss of quantum state (decoherence).
- Basic network structure is analogous to a classical p2p network connecting end-points when processors with more than the local available qubits are available or when in need for storage.
  - Currently only direct connections between 2 end-nodes using optical switches that preserve quantum coherence.
- Signal amplification and the use of optical repeaters is not possible as quantum state will be lost, and qubits cannot be copied. Hence distance between direct connected quantum nodes currently of about ~120km.
  Using a Quantum Repeater longer distances should become possible but additional equipment is needed in the path for entanglement swapping and teleportation.

QUANTUM NETWORKING

- Two approaches to construct quantum networks; simply forward quantum information directly between nodes or create entanglement between not directly connected nodes (somewhat comparable to overlay networking) leveraging teleportation and entanglement swapping.
- Classical computer networks tackle the complexity of transmitting bits between two nodes by breaking down the transmission into several layers of a stack model, the Open Systems Interconnection model (OSI model). Work is ongoing to establish a comparable model to quantum network.

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

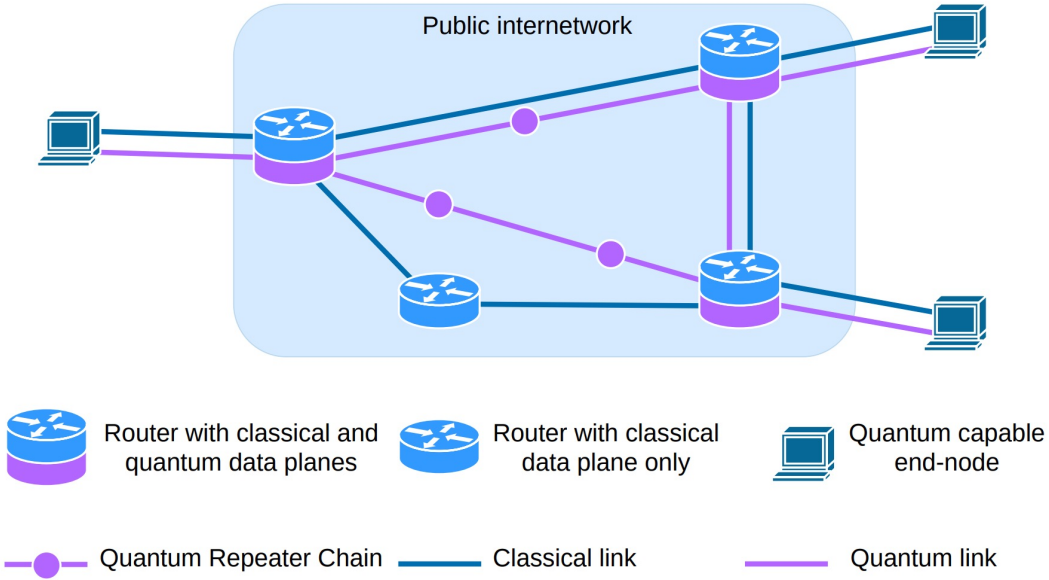




- Quantum applications can operate with imperfect quantum states — if the fidelity is above an application-specific threshold (for basic QKD the threshold fidelity is about 0.8).

Source: https://arxiv.org/pdf/2010.02575.pdf

Applications support based on quantum entanglement



"Quantum networks will use existing network infrastructure to exchange classical messages for the purposes of running quantum protocols as well as the control and management of the network itself. Long-distance links will be built using chains of automated quantum repeaters."

Source: https://arxiv.org/pdf/2010.02575.pdf

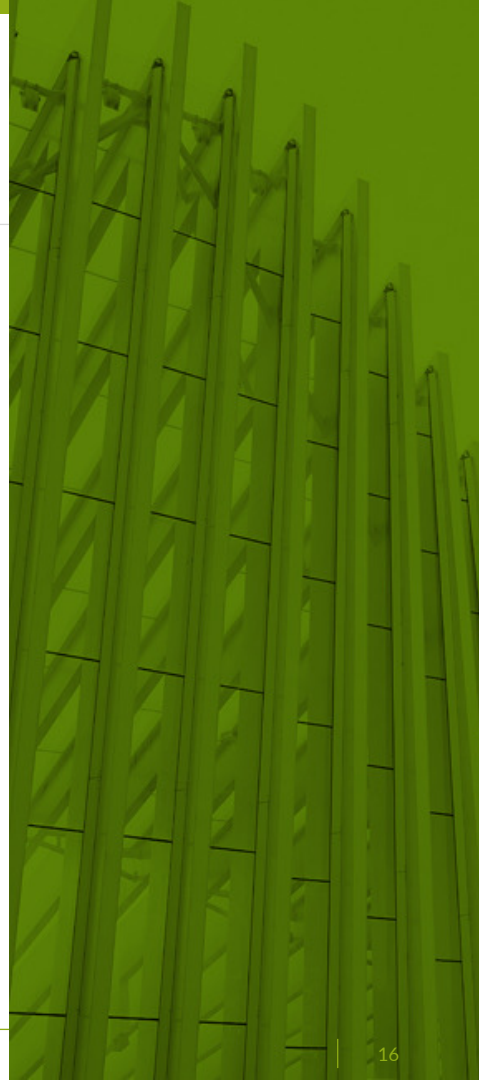
Possible applications for quantum in networking

In general quantum entanglement is well suited for tasks that require coordination, synchronization or privacy:

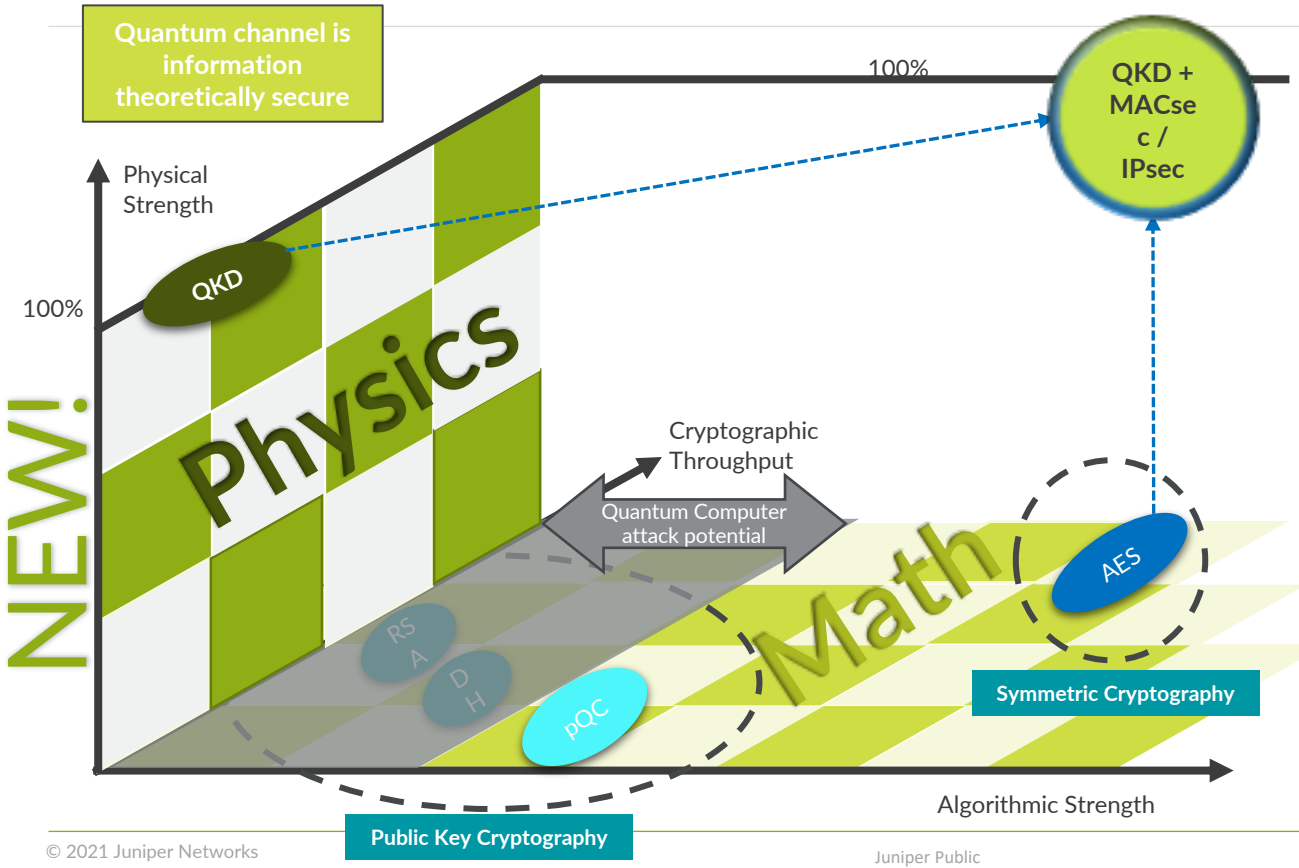
- Clock synchronization
- Leader Election
- Secure Access to resources (banking application for example)
- Telescope baselining or other geographically dispersed highly precise equipment
- Communication between quantum computers
- Sharing memory in quantum computers
- Quantum Key Distribution

DEMYSTIFY QUANTUM KEY DISTRIBUTION

- Symmetric Key Cryptography
- How does QKD work?
- Applying QKD

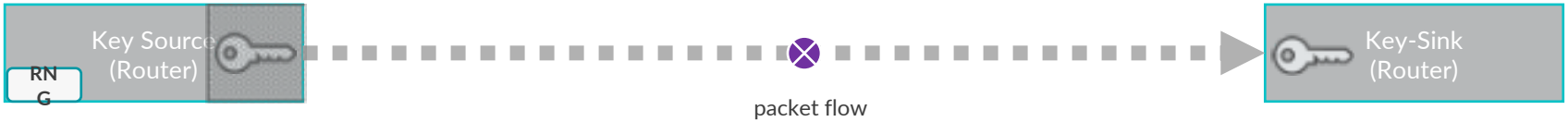


HOW DOES QUANTUM TECHNOLOGY DIFFERENTIATE?



QKD is one of multiple security enhancement investments being made across the industry to prevent the risk of Quantum Computing being used by malicious adversaries

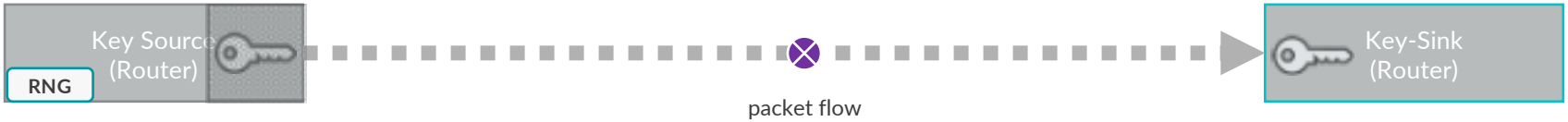
	sharing	Crypto Engine	Typical use	Entropy Source
Public crypto (RSA, DH)	Public key	Math	bootstrap	Local RNG
Symmetric (AES)	Private key	Math	Work horse	from local RNG or QKD
QKD	none	Physics	bootstrap	Quantum-RNG



1. A Key source generates a key by use of a Random Number Generator (RNG)
2. The Key-Source encrypts the key using Public Key Cryptography (PKI) and sends it to the Key-Sink

Result: key is known at source and sink

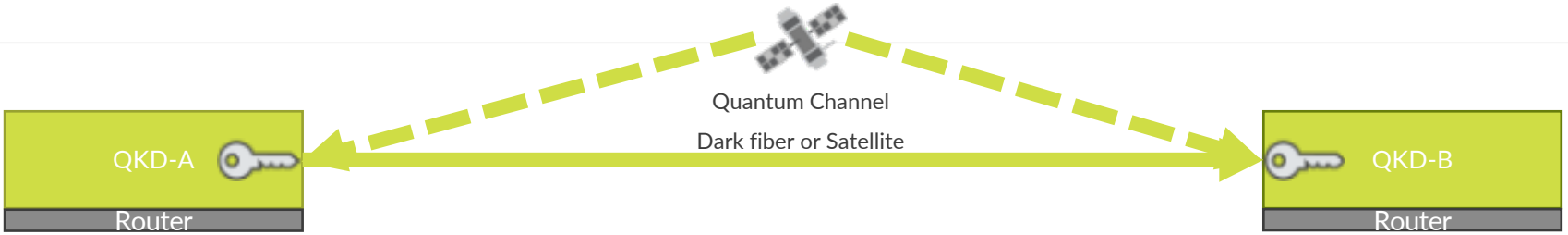
1. **Issue**: The full key information is transported over the data channel, can be intercepted without knowledge of Key-source and Key-Sink (store&decrypt later)
2. **Issue**: PKI is considered breakable with Quantum Computers using Shor's Algorithm



1. A Key source generates a key by use of a Random Number Generator (RNG)
2. The Key-Source encrypts the key using **pQC-based** Public Key Cryptography (PKI) and sends it to the Key-Sink

Result: key is known at source and sink

1. **Issue**: [same as today] The full key information is transported over the data channel, can be intercepted without knowledge of Key-source and Key-Sink (**store & much harder to decrypt later**)
2. **Issue**: pQC-PKI is considered resistant against attacks with Quantum Computers using Shor's algorithm. **But there is no proof that another Algorithm exists that could break the encryption**



1. Quantum Key Distribution enables two distant devices connected with a Quantum Channel to “distill” the same information on both devices

Result: key is known at source and sink

1. **Advantage**: **cannot be broken even if the adversary has unlimited computing power.** The distribution mechanism is **proven to be information theoretic secure** [Wikipedia]
   - Quantum state **cannot be intercepted without changing it’s state** and is detectable
   - Quantum state decays fast. It **cannot be stored for a long time** to decrypt it later

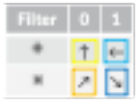
How does QKD work?

QUANTUM CRYPTOGRAPHY

BB84* PROTOCOL (SCHEMATIC)

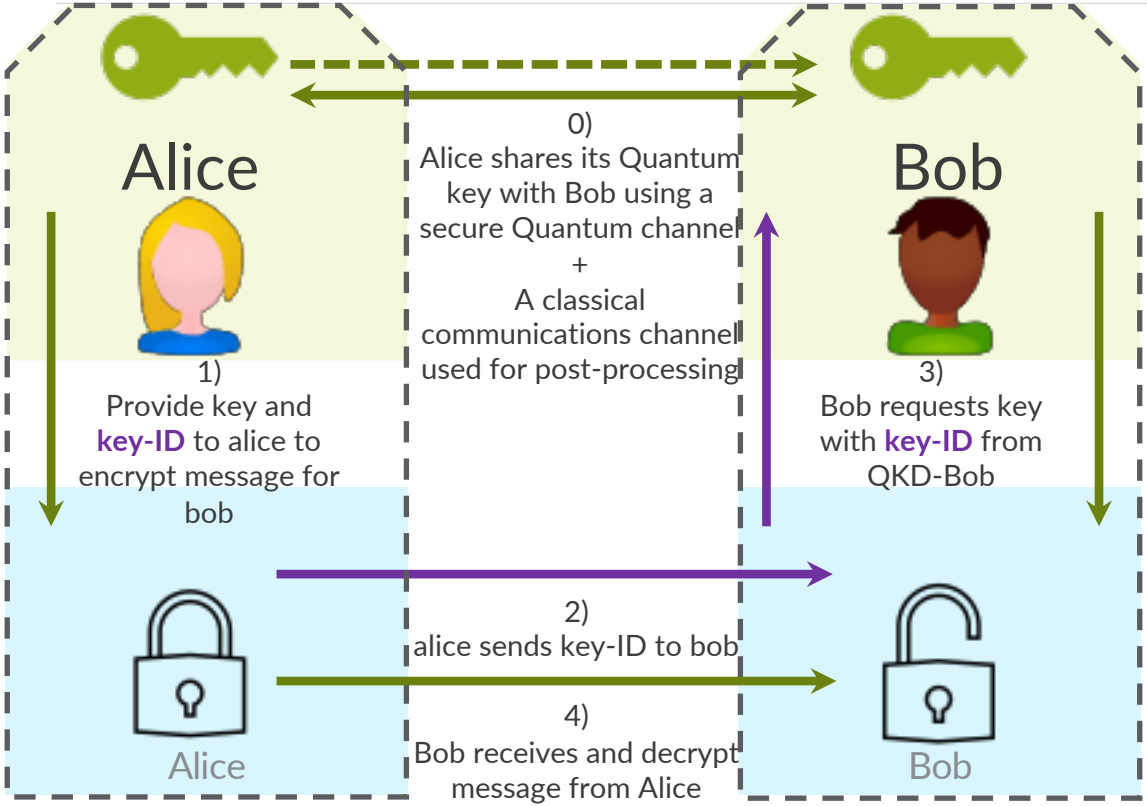
*invented by Ch. Bennett (IBM Research) & G. Brassard (University of Montreal) in 1984

Alice	Information	Bob	Information
Quantum Transmission			
Quantum Measurement Preparation			
Quantum Measurement			
Measurement post-processing			
Sifting through the Results			
Key Result			



BB84 exaplained: https://www.youtube.com/watch?v=IE5952ExMK8

QUANTUM KEY DISTRIBUTION USED IN ROUTERS



- Measuring the quantum state destroys the photon
- The Quantum State of photons cannot be replicated
- Eavesdropping is easily recognized
- Classical channel for post-processing does not carry the key

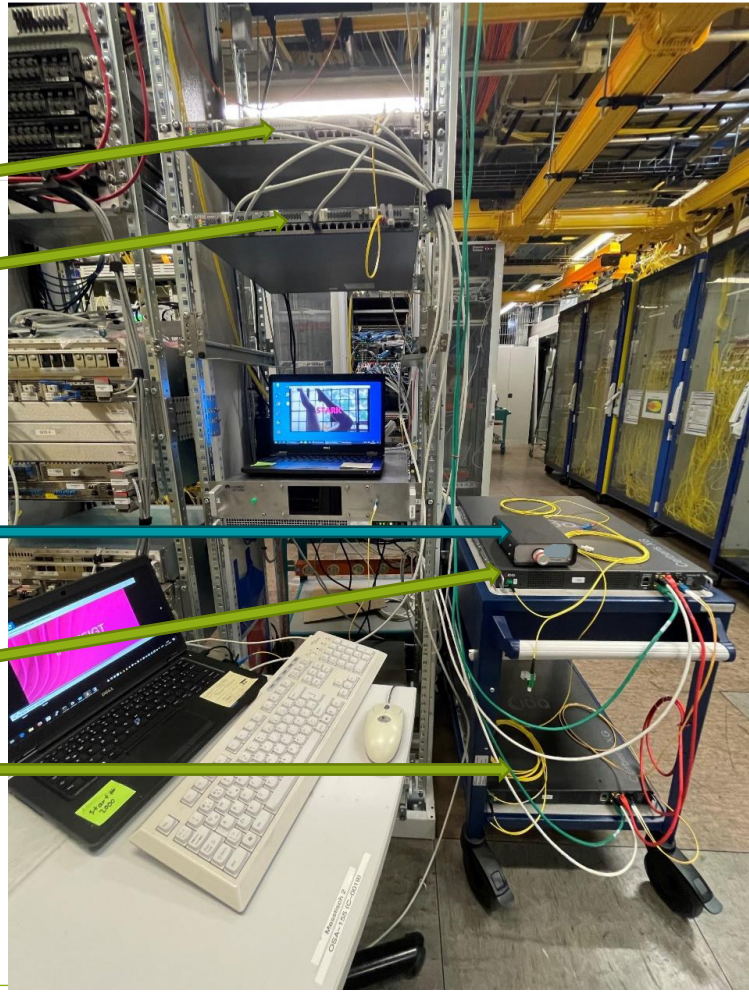
Quantum Cryptography security is based on quantum mechanics

QUANTUM CRYPTOGRAPHY

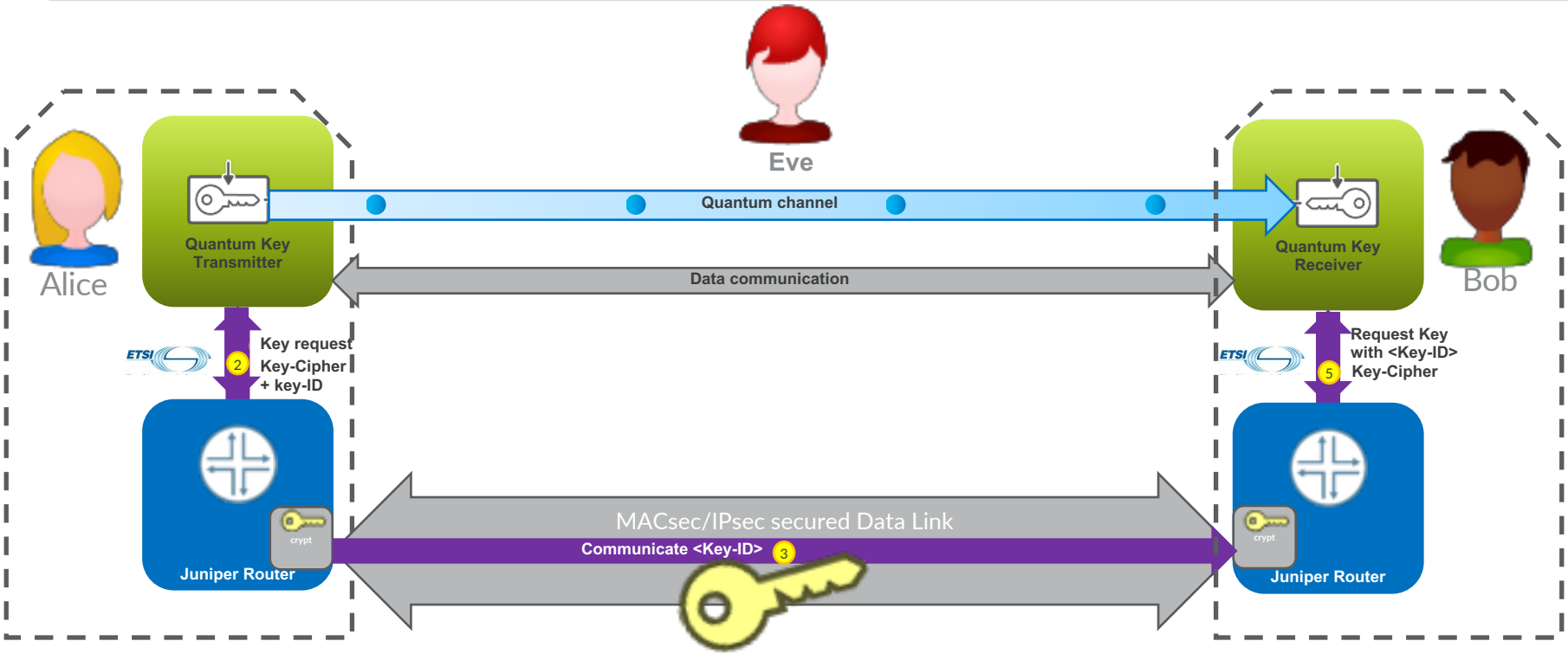
Alice and Bob
2* Juniper SRX380
MACsec @ 10G

Eavesdropping simulation device

QKD-Tx & QKD-Rx



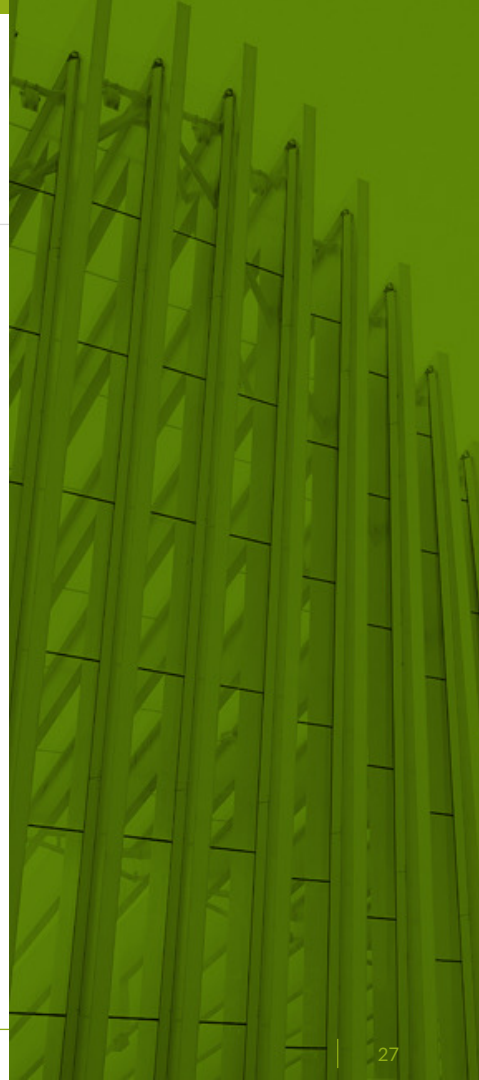
QUANTUM CRYPTOGRAPHY KEY EXCHANGE



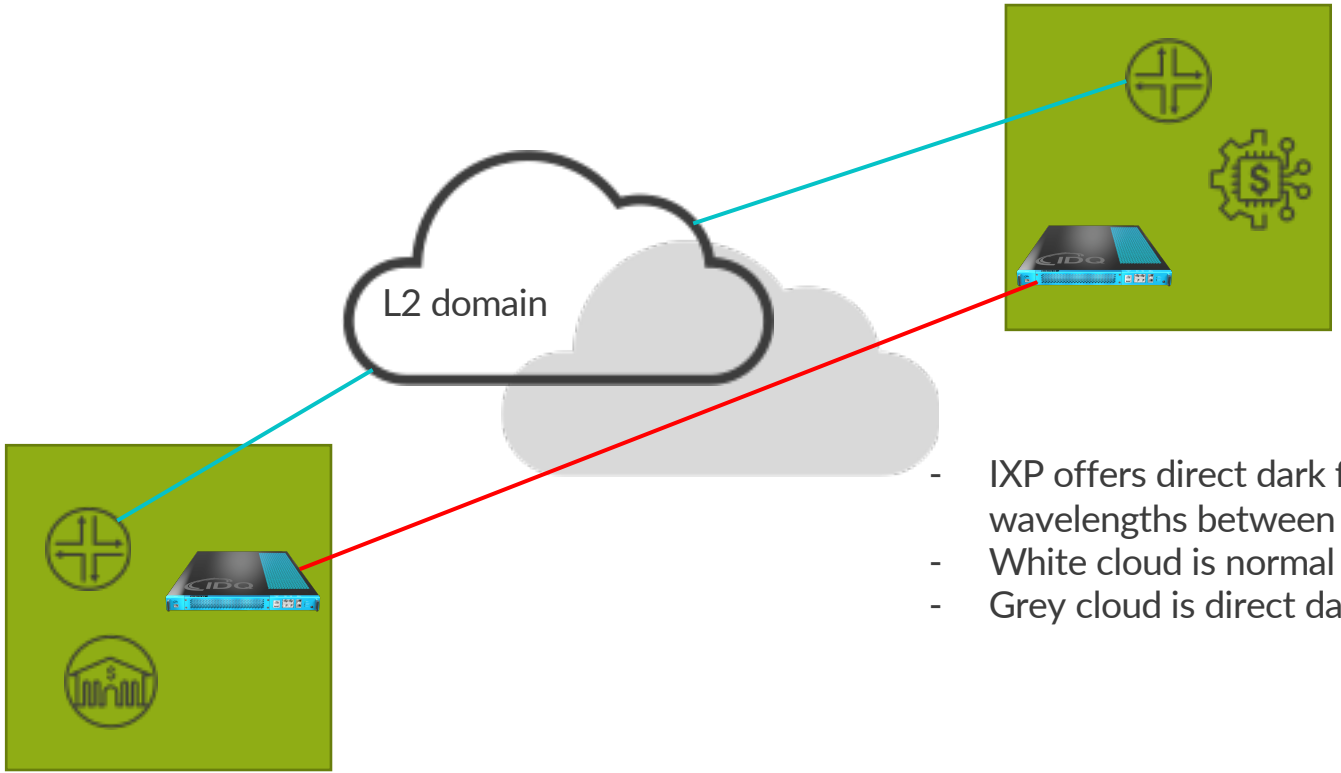
APPLICABILITY

- Keys are made available using ETSI REST API and can be consumed by many. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
- QKD usable in many symmetric-key algorithms and protocols that allow for hitless key rollover.
  For example: MACsec, TCP-AO, IPsec, etc.
- Commercial KQD products available from several vendors.

INTERNET EXCHANGE POINT USE CASE

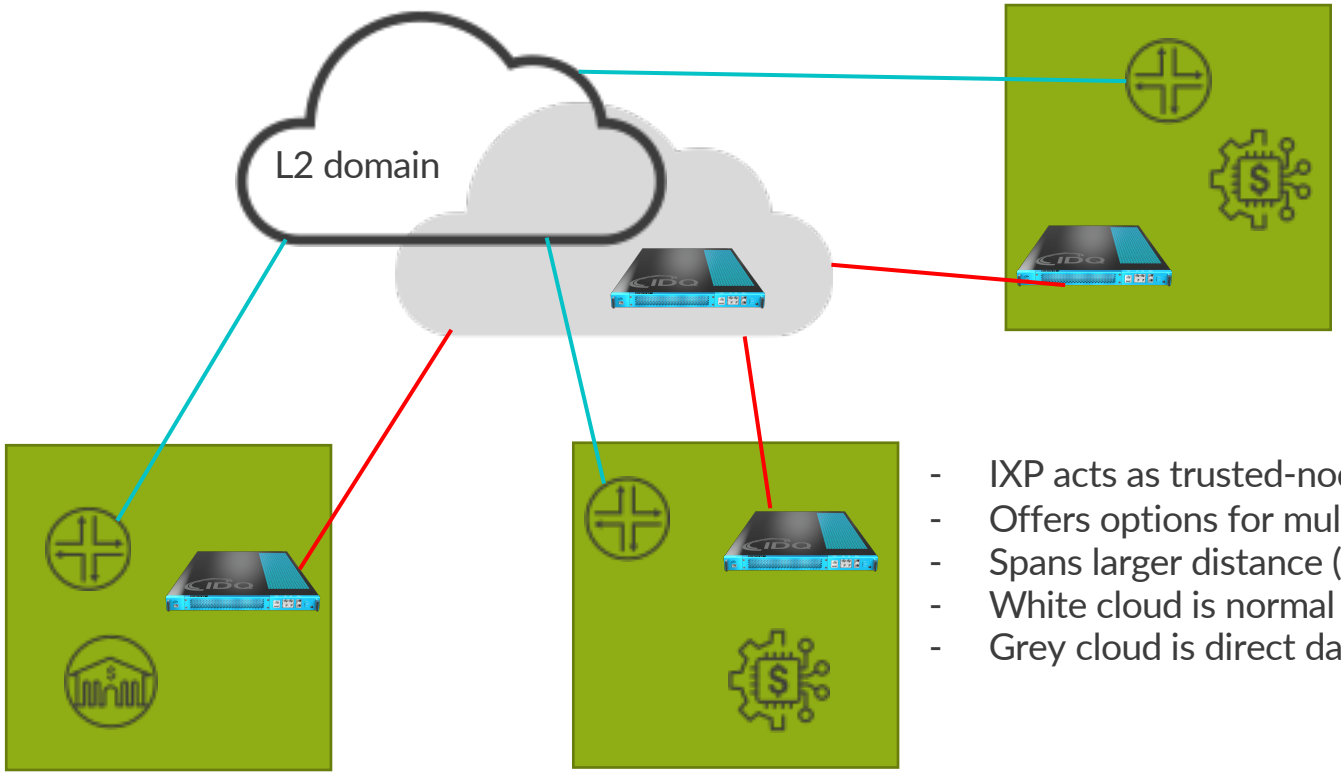


IXP USE CASE 1 – PASSIVE QKD



- IXP offers direct dark fiber connections or wavelengths between connected members
- White cloud is normal peering infrastructure
- Grey cloud is direct dark fiber connections

IXP USE CASE 1 – ACTIVE QKD



- IXP acts as trusted-node
- Offers options for multipoint
- Spans larger distance (2x120km)
- White cloud is normal peering infrastructure
- Grey cloud is direct dark fiber connections

WHAT'S NEXT?

First useable solutions are here but what is next?

WHATS NEXT?

- How to overcome the 120km distance between QKD boxes?
  - Quantum repeaters? SDN/SD-WAN? Satellite?
- How to distribute keys in locations where no QKD boxes are present but with preserving ‘quantum security’?
  - Remote/home workers, mobile users, small branch offices/POS
- Multipoint QKD?
- How to securely exchange keys between QKD boxes and consumers?
- Entangle >2 photons
- What else can we do with perfectly synchronised data?
- Leverage quantum keys to secure routing protocols? TCP-AO for example?

FURTHER READING / ADDITIONAL RESOURCES

- A quantum network stack and protocols for reliable entanglement-based networks
  https://arxiv.org/pdf/1810.03556.pdf
- Designing a Quantum Network Protocol
  https://arxiv.org/pdf/2010.02575.pdf
- Architectural Principles for a Quantum Internet
  https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/
- Applications and Use Cases for the Quantum Internet
  https://datatracker.ietf.org/doc/draft-irtf-qirg-quantum-internet-use-cases/
- Quantum Key Distribution (QKD) Protocols: A Survey
  https://ieeexplore.ieee.org/document/8527822
- **Quantum Key Distribution (QKD): Protocol and data format of REST-based key delivery API**
  https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
- Dancing with Qubits: Robert S sutor – Packt (ISBN-13: 978-1838827366)
- Cryptography Apocalypse: Roger A. Grimes – Wiley (ISBN-13: 978-1119618195)

QUESTIONS? REACH OUT!

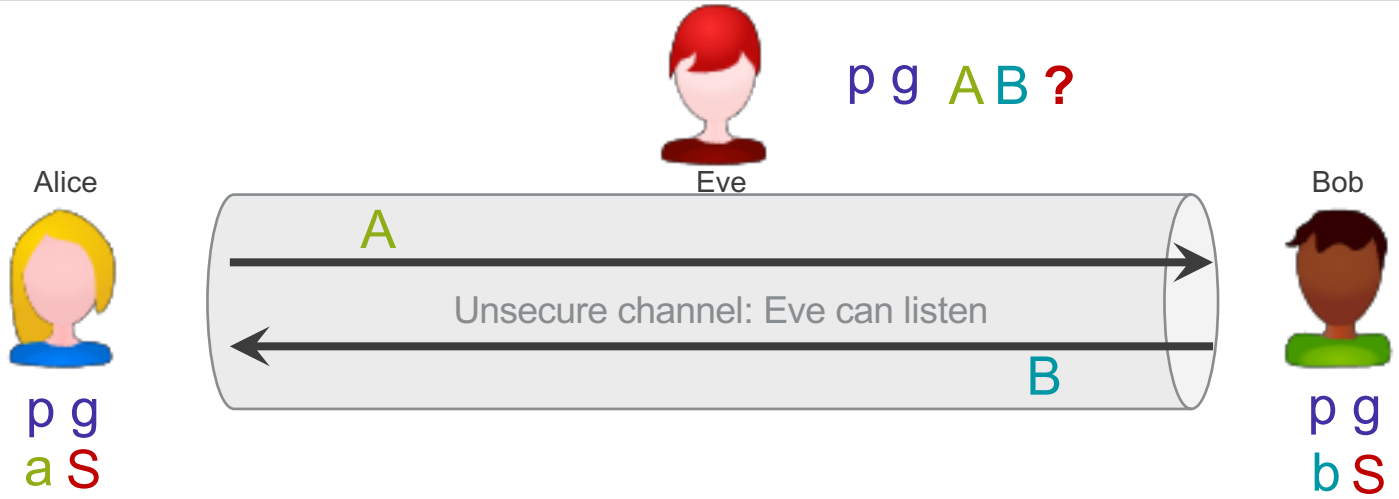
Melchior Aelmans
melchior@juniper.net

Juniper Networks | Engineering Simplicity

BACKUP SLIDES

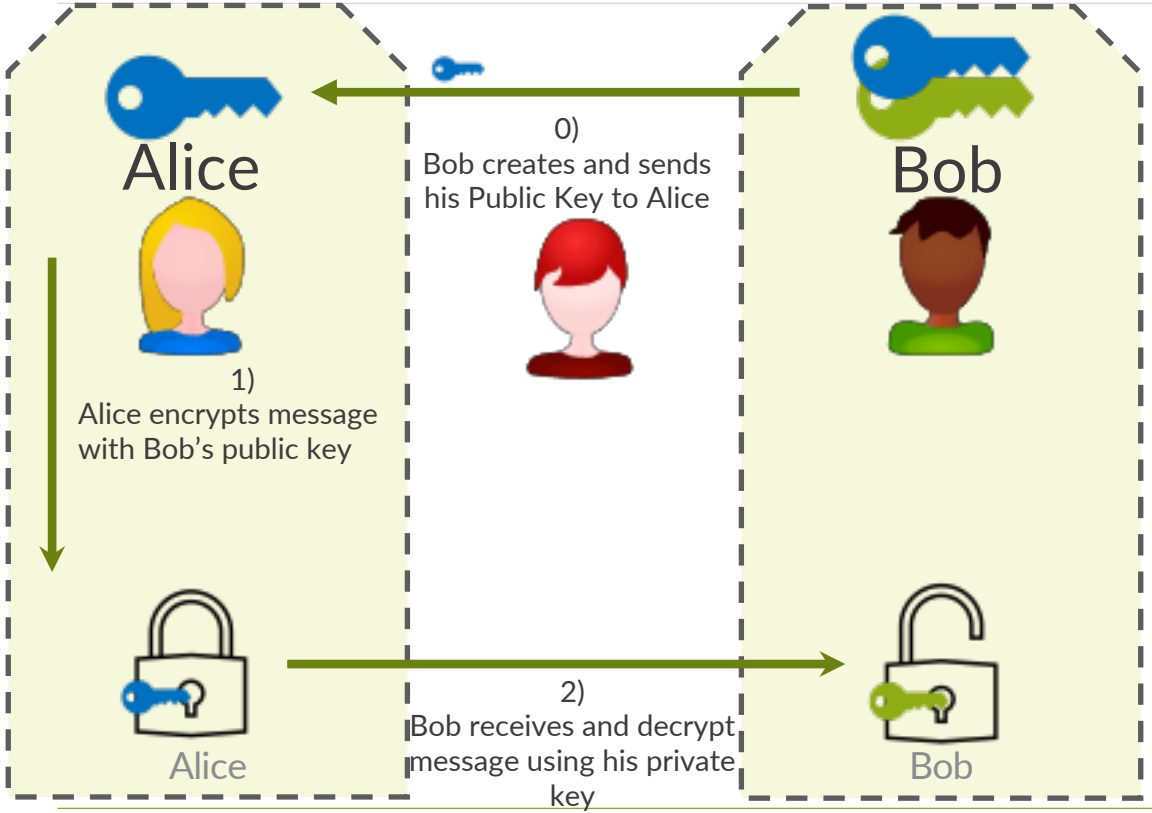
Quantum Concepts	Properties
Qubit	• Basic unit of information in quantum computing • Unlike classical bits, a quantum bit or qubit can be sort of in zero and one at the same time
Superposition	• Quantum states can be added(superposed) together to yield a new valid quantum state • A qubit can be in state $\|0\rangle$, $\|1\rangle$ or in a linear combination of the both states
No cloning	• Given an unknown quantum state there is no reliable way to produce extra copies of that state • Can be annoying when you want to protect quantum information from outside influence
Measurement	• Act of observing a quantum state and will yield a classical information such as a bit • If the state is in superposition, this measurement will 'collapse' it into a zero or one
Entanglement	• A pair of qubits can be entangled by bringing them close together and performing an operation • This entanglement will manifest in the outcome of measurements of the qubits
Teleportation	• A method of sending qubits between Alice and Bob using entanglement and a classical channel • An entangled qubit and the qubit (information to be sent) is measured by Alice to get a classical information. This information can be sent via a classical channel to Bob • Bob does a correction to his qubit using the classical information to recover Alice's qubit
Fidelity	• Fidelity is a measure of the "closeness" of two quantum states. • It expresses the probability that one state will pass a test to identify as the other.
Quantum decoherence	• Quantum decoherence is the loss of quantum coherence. • In quantum mechanics, particles such as electrons are described by a wave function, a mathematical representation of the quantum state of a system; a probabilistic interpretation of the wave function is used to explain various quantum effects. • As long as there exists a definite phase relation between different states, the system is said to be coherent. A definite phase relationship is necessary to perform quantum computing on quantum information encoded in quantum states.

DIFFIE-HELLMAN KEY EXCHANGE



1. Public announcement of a large prime modulus p and a generator g
2. Alice selects secret key (=private random nb.) a, and sends public key $A = g^a \bmod p$ to Bob
3. Bob selects secret key (=private random nb.) b, and sends public key $B = g^b \bmod p$ to Alice
4. Alice calculates $S = B^a \bmod p$ and Bob calculates $A^b \bmod p = S$ (=shared secret)
5. Due to computational complexity, Eve cannot compute S in **reasonable time** without knowing a or b

PUBLIC KEY CRYPTOGRAPHY



- relies on one-way functions (e.g. integer factorization or discrete logarithm) requiring complex calculations
- encryption is based upon mathematical calculations that are simple to compute, but require an infeasible amount of processing power to invert

- no need to establish a secret key
- distribution of a public key instead