Quantum Key Distribution

Today and Tomorrow

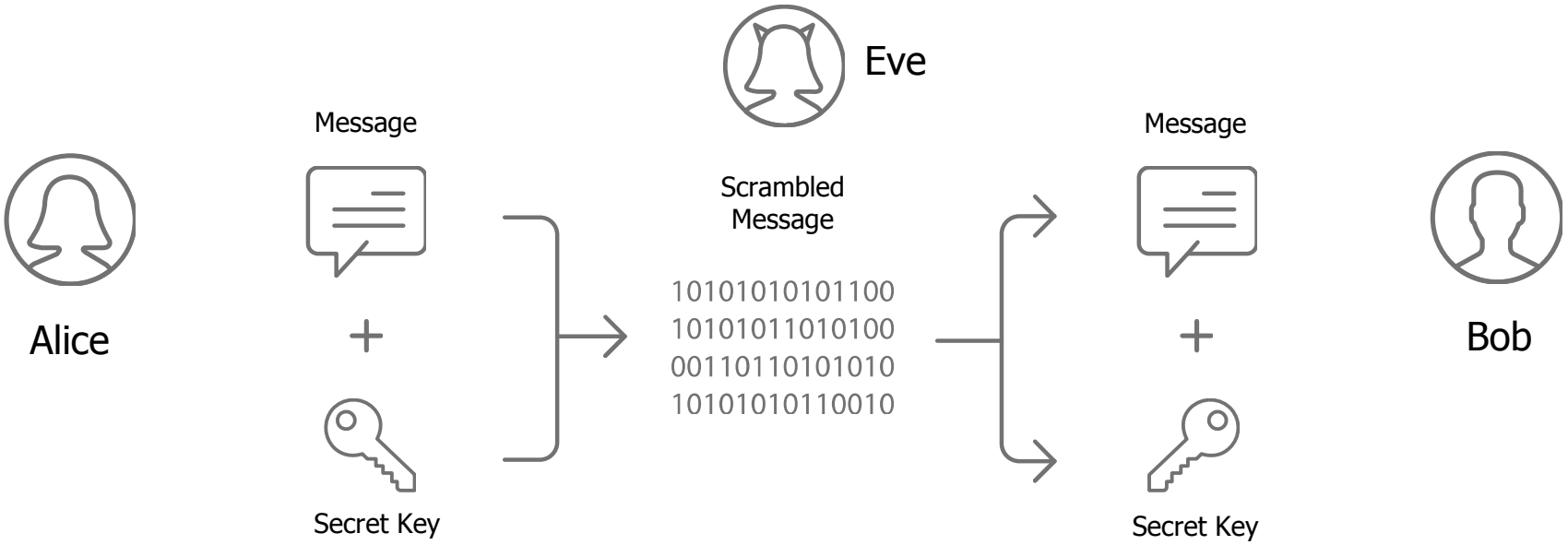
Bruno Huttner
QKD Product Manager @ ID Quantique
Co-chairman of QSS WG @ CSA

September 2016

Outline

- QKD Today
  - Principle
  - Eavesdropping on a quantum channel
  - Proof of security
  - Pros and Cons of QKD
  - How it is used in practice.
- QKD Tomorrow
  - Trusted Nodes
  - QKD in space
  - A global QKD network

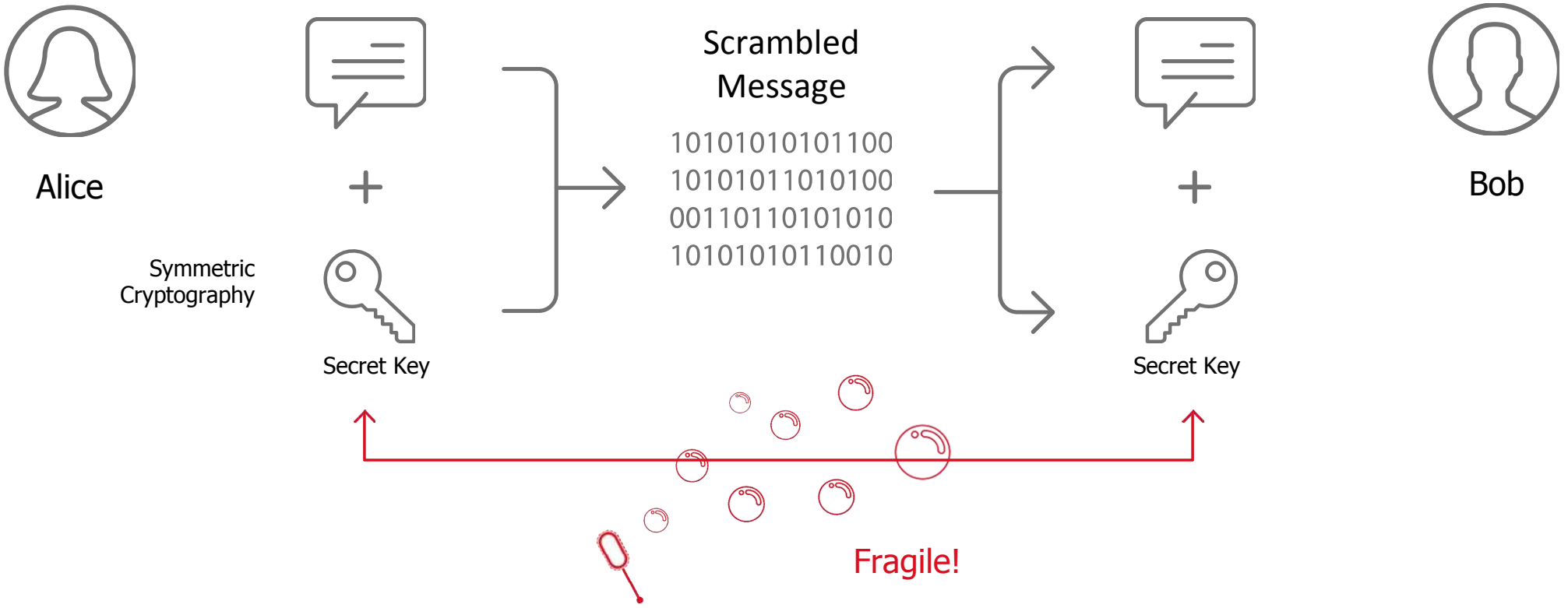
The scenario: Symmetric Cryptography



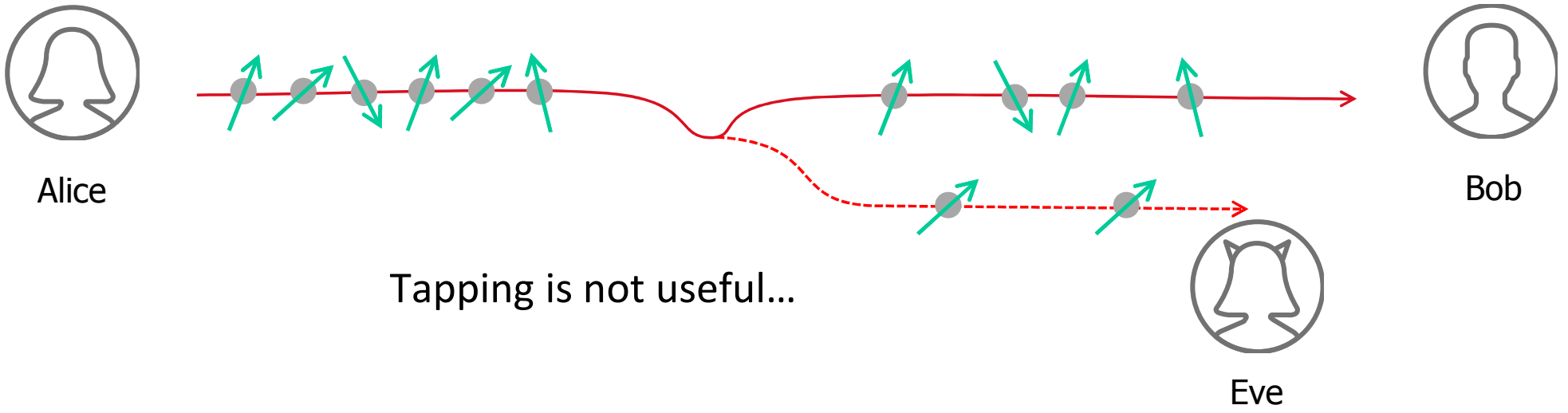
Secret key distribution methods:

- Trusted courier (☹)
- Public key cryptography (not quantum-safe today…)
- Quantum key distribution

Quantum Key Distribution (QKD): Basic idea

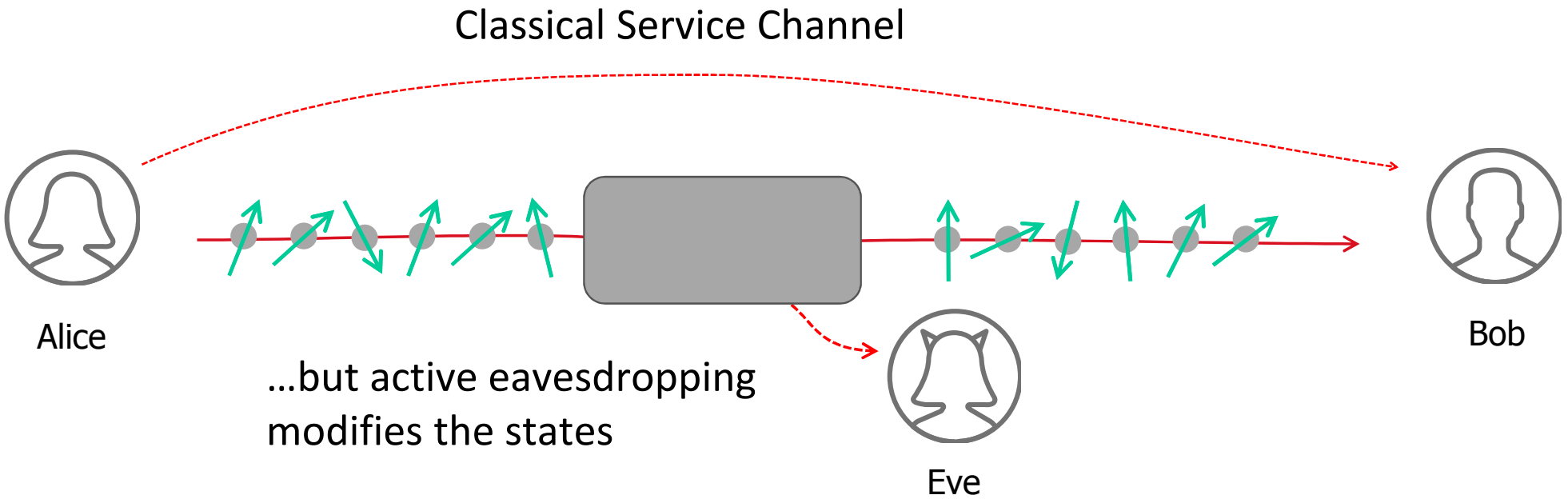


QKD: The quantum Channel

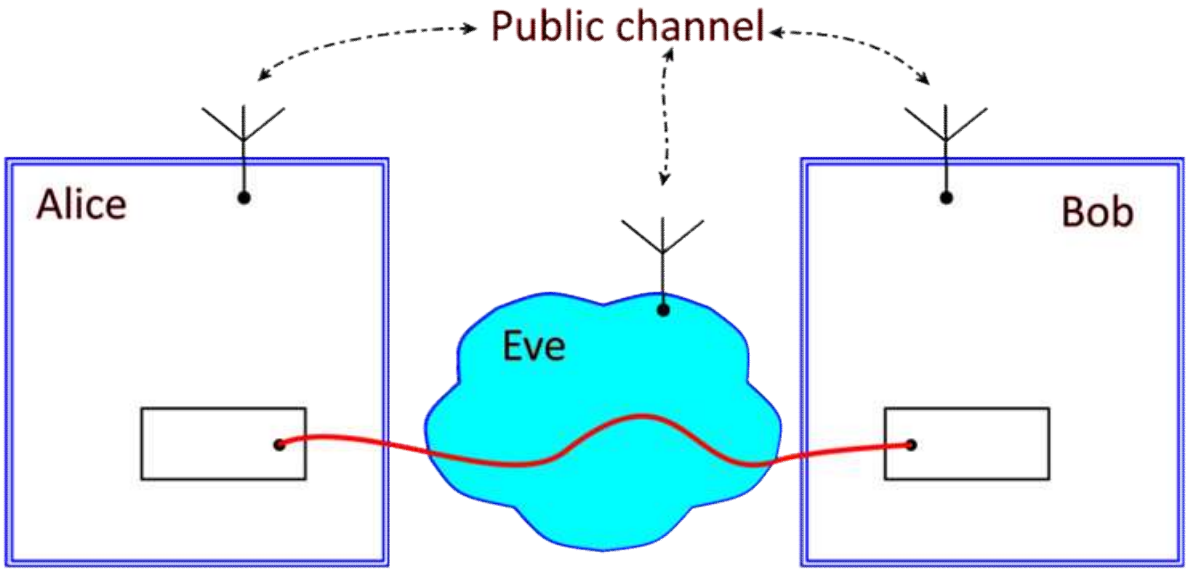


Tapping is not useful…

QKD: The quantum Channel



QKD: The set up



4 assumptions:

1. Alice and Bob operate in a protected environment
2. Public channel is authentified

3. Eve cannot use the QC to probe Alice and Bob's setup
4. QC only carries quantum states within the pre-defined Hilbert space

→ Proof of security

QKD: Pros & Cons

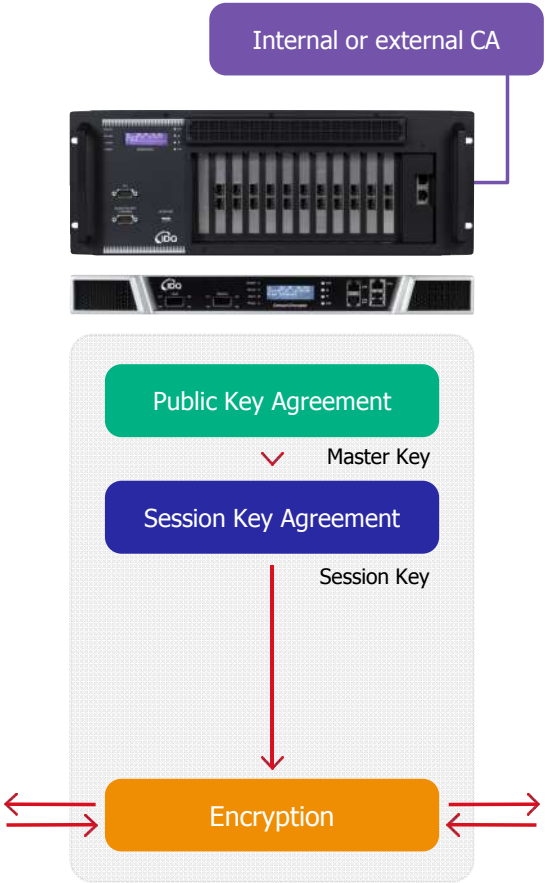
Pros	Cons
Based on different principle (physics)	Need physical infrastructure
Not impacted by QC	Limited distance between nodes (to date)
Provable security of transmission	Only part of the solution: Needs conventional crypto to use the key (e.g. symmetric key encryption); And post-quantum Authentication
Real-time eavesdropping possible only	
Adds one layer of security	

➔ More complicated and costly to implement

➔ Useful for high-level and long-term security

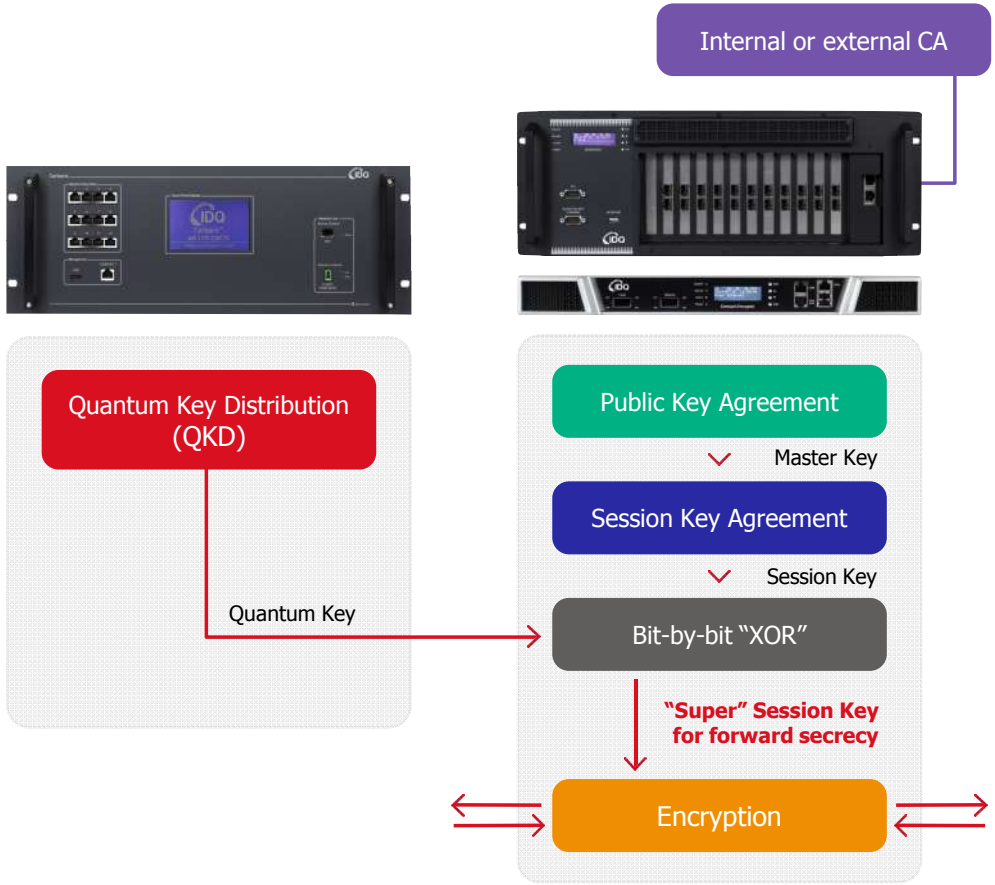
Implementation: Encryption in Default Mode

- Key exchange interoperable for all encryptors
- State-of-the-art FIPS approved key management
- RSA-2048 or ECC for public key agreement
- AES 256 CTR or GCM mode for high-speed data encryption
- AES Master and session keys, with session key updated up to once per minute
- Fully automatic – set and forget
- High quality key material generated by IDQ‘s Quantum True Random Number Generator (selected encryptors)
- May be upgraded to QKD

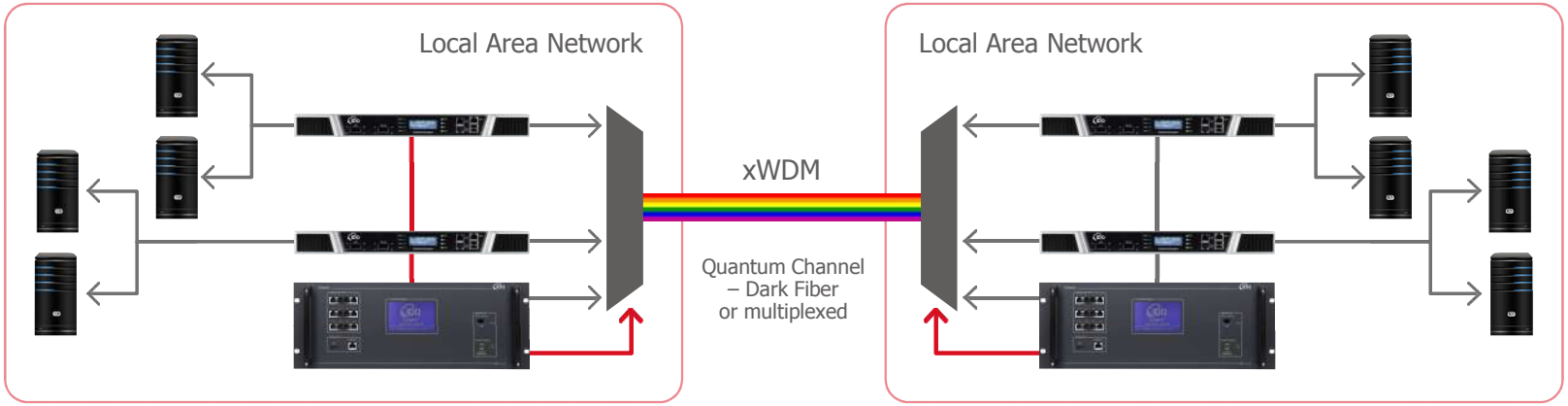


Implementation: Encryption with QKD Dual Key Agreement

- Quantum keys are based on high quality entropy (encryption key) from provably random QRNG.
- Quantum Key is mixed with the standard AES session key.
- Advantages:
  - Maintains existing encryptor certifications (eg. FIPS, CC).
  - Generates "super session“ key which guarantees forward secrecy.
  - Eavesdropping protection.
  - No single point of vulnerability back to public-key exchange or manual key exchange (where the initial keys remain static for a long period of time). In contrast each quantum key is independent & uncorrelated, and automatically updated every minute.



Quantum-Enabled Network Encryption: Today



...And Tomorrow!

Prediction is very difficult, especially if it is about the future" (Niels Bohr)

- Trusted Nodes for long-distance QKD
- Free Space QKD with satellites
- Global QKD Network based on Quantum Memories

What about long-distance: a complete Quantum Backbone in China with Trusted Nodes

SWISS QUANTUM

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

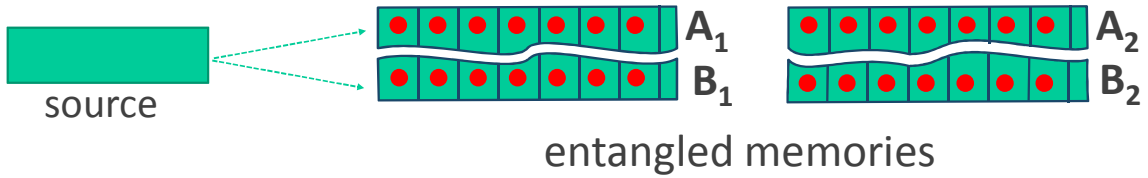
IDQ

A Global Network Based on Free Space QKD

- Free Space QKD
  - QKD links with LEO satellites & HAPs.
  - Satellite and/or HAP act as a trusted nodes to transport the key to the necessary location.
- Free space QKD is moving out of the lab & into industry
  - Chinese have launched a QKD satellite in August 2016.
  - Worldwide interest at the academic/government level
  - IDQ feasibility studies for practical systems (Eurostars and Swiss Space Office)

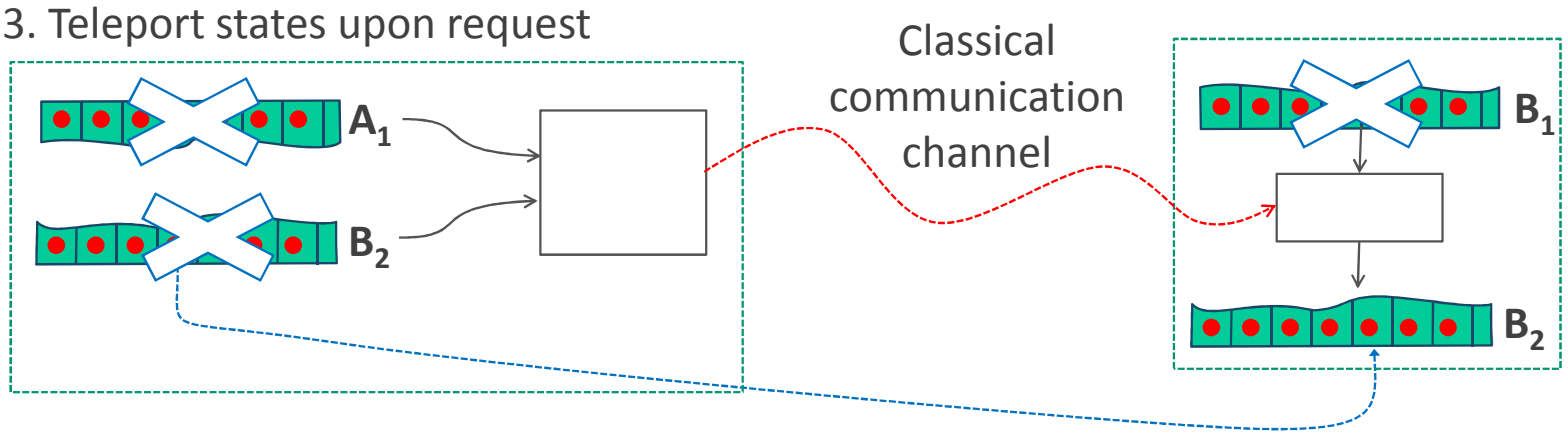
Global QKD Network based on Quantum Memories: 1. Building blocks

1. Generate and store entangled states in quantum memories

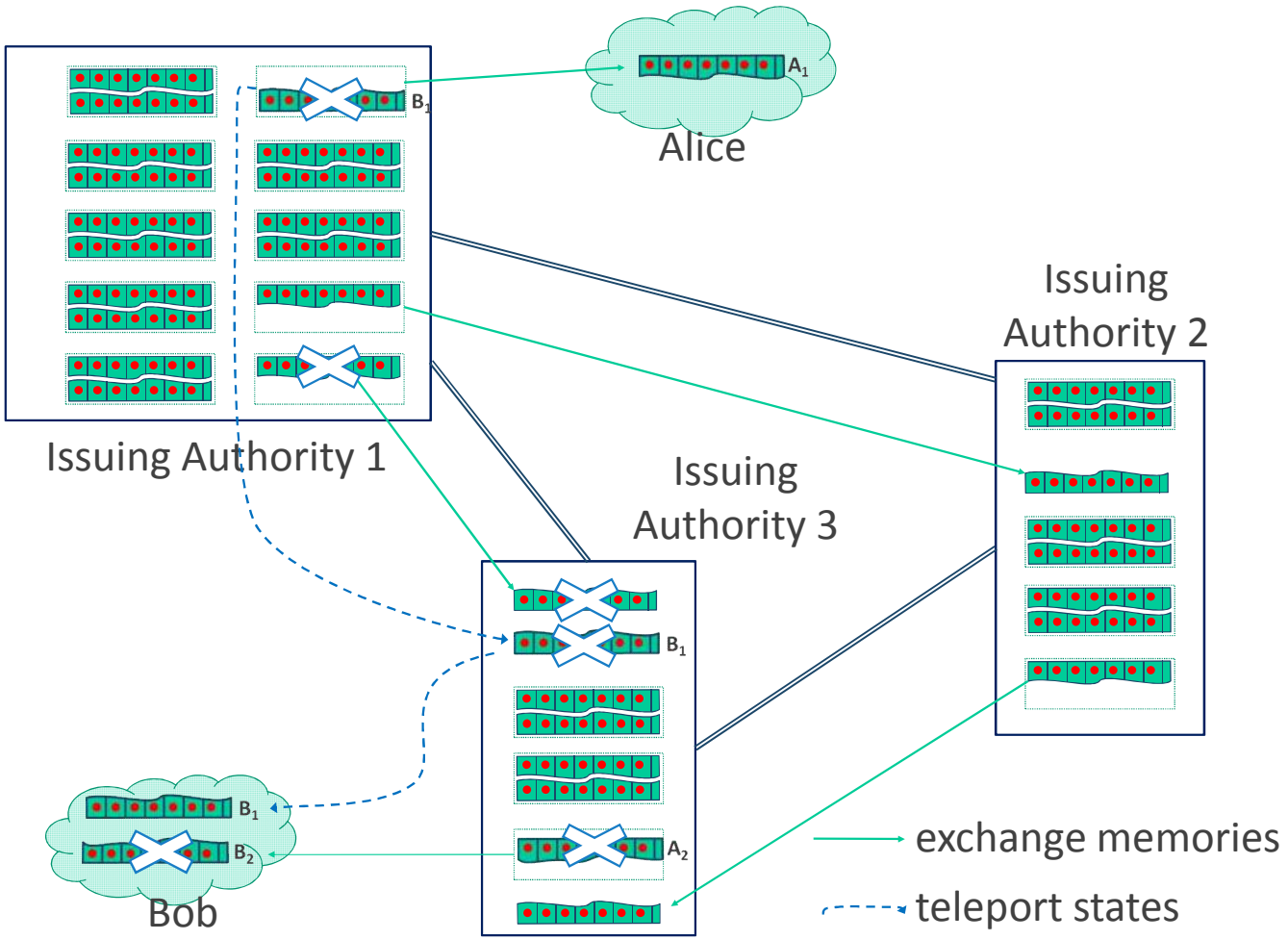


2. Distribute entangled memories

3. Teleport states upon request



Global QKD Network based on Quantum Memories: 2. Implementation



Global QKD Network based on Quantum Memories: 3. A world-wide QKD infrastructure

- Build a QM infrastructure
- Each node exchanges QMs with the others
- Customers come to any node to recharge their QMs (similar to bank notes and ATM infrastructure)

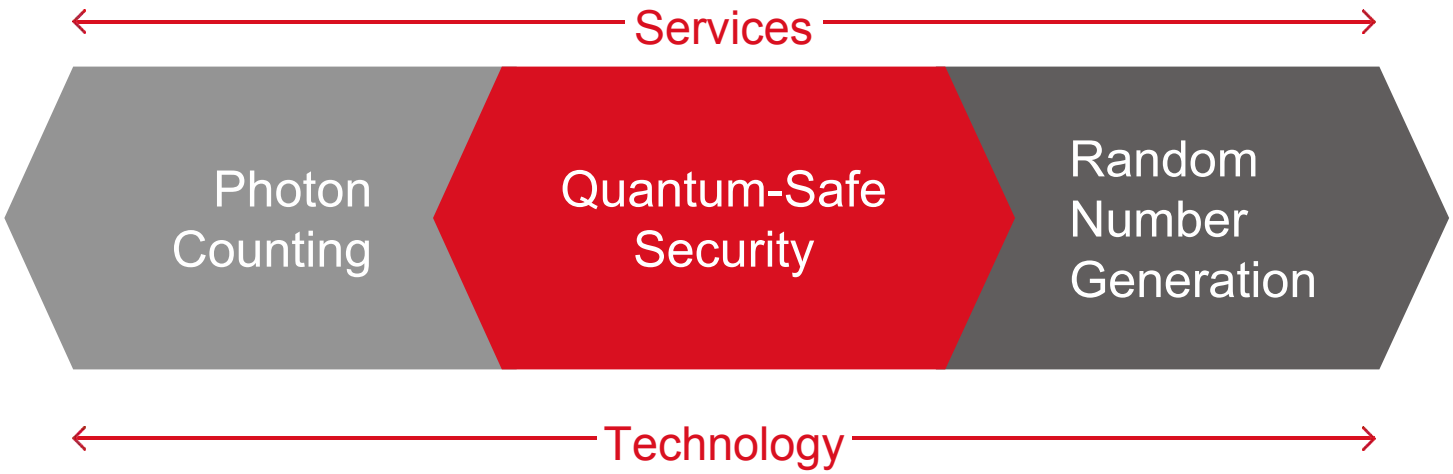
Summary

- QKD can and should be used **today** to improve security on high-value links requiring long-term security
- No risk, only adds one (very different) layer of security
- Quantum Resistant Algorithms and QKD should be used together to provide **Quantum-Safe security**
- Future world-wide QKD network is feasible

For more information
http://www.idquantique.com/

EXTRA SLIDES…

ID Quantique



Swiss company, founded 2001, based in Geneva.

World leaders in Quantum-Safe Crypto.

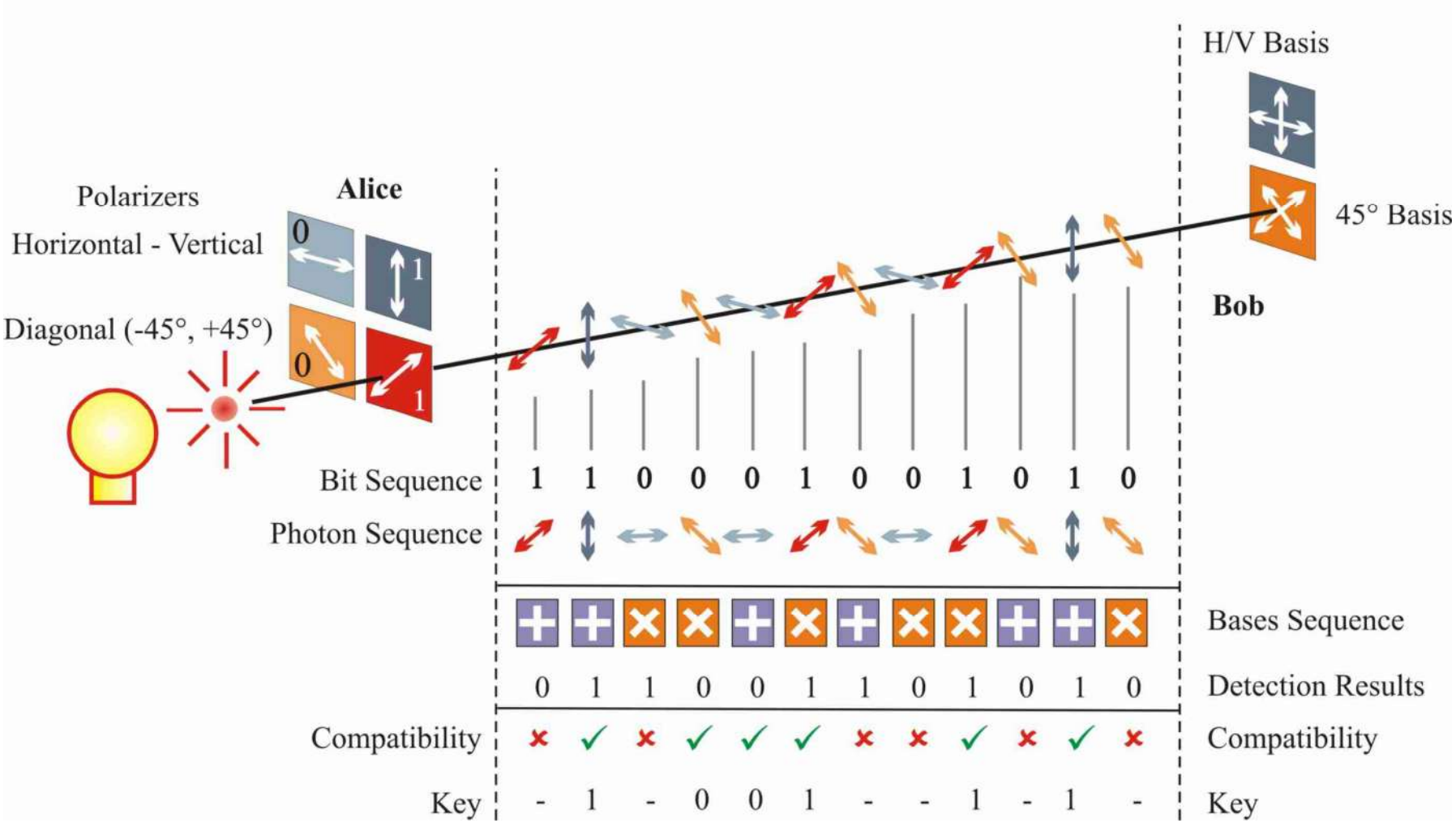
Quantum Key Generation

Quantum Key Distribution

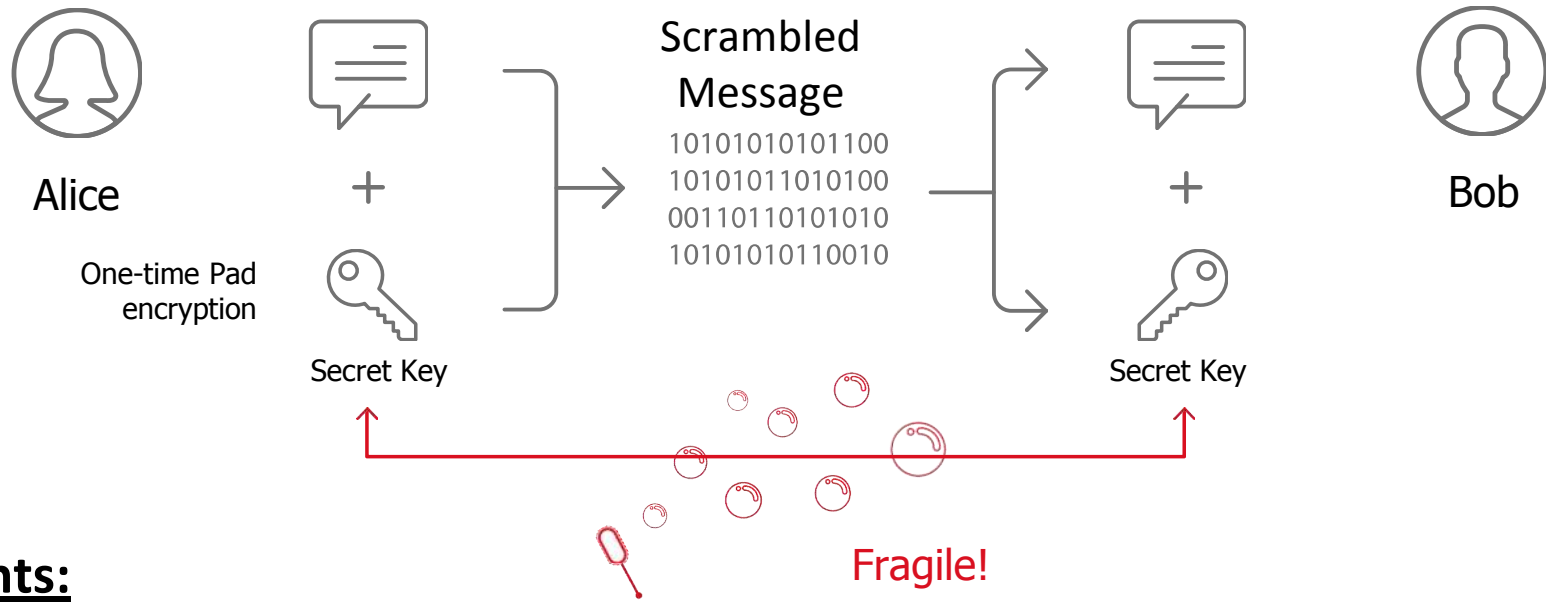
Quantum-safe high-performance layer 2 encryption

Spin-off of University of Geneva, Group of Applied Physics.

QKD example: the BB84 protocol



A truly IT secure encryption scheme

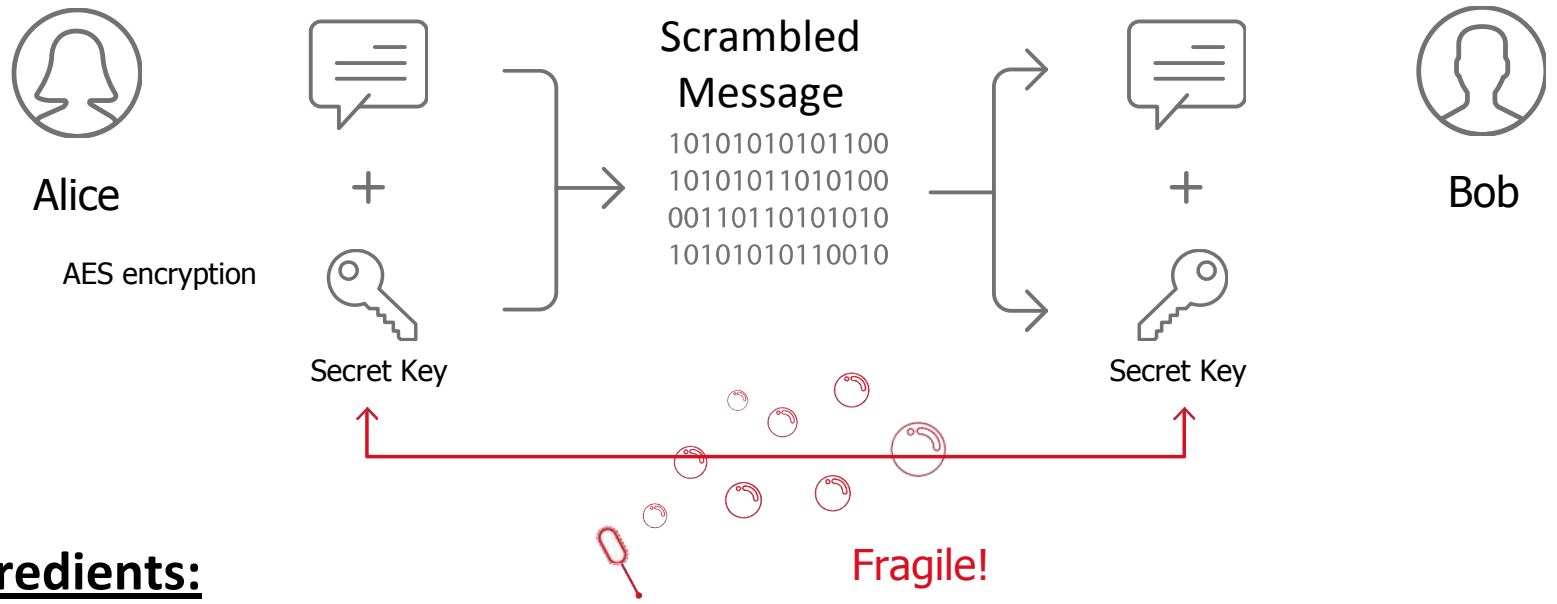


Ingredients:

- ❑ QKD for key distribution
- ❑ One-time-pad for encryption
- ❑ Wegman-Carter scheme for authentication

….plus initial secret key

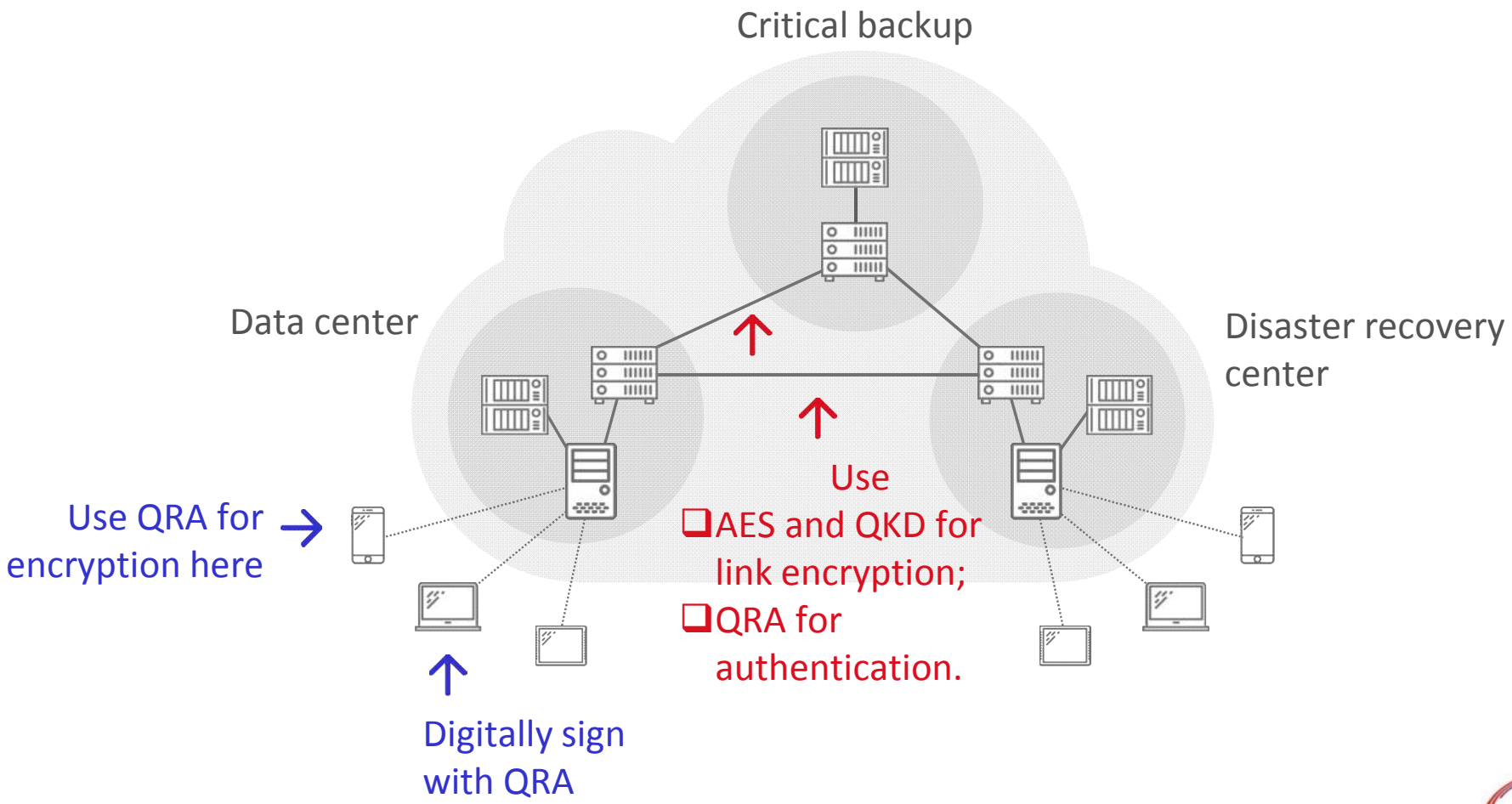
A widely accepted Quantum-safe scheme



Ingredients:

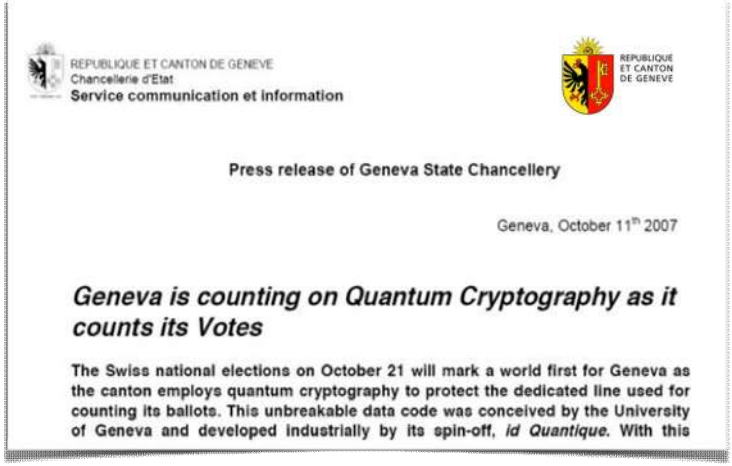
- ❑ QKD for key distribution
- ❑ AES for encryption
- ❑ Hash-based signature scheme for authentication (e.g.: Merkle scheme)

Example of a practical use case for QKD



Real implementation (1): Practical QKD in Government & Public Administration

- Geneva (Switzerland) uses QKD to guarantee confidentiality & integrity of data during federal & cantonal elections.
- Working since October 2007.



REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Service communication et information

REPUBLIQUE ET CANTON DE GENEVE

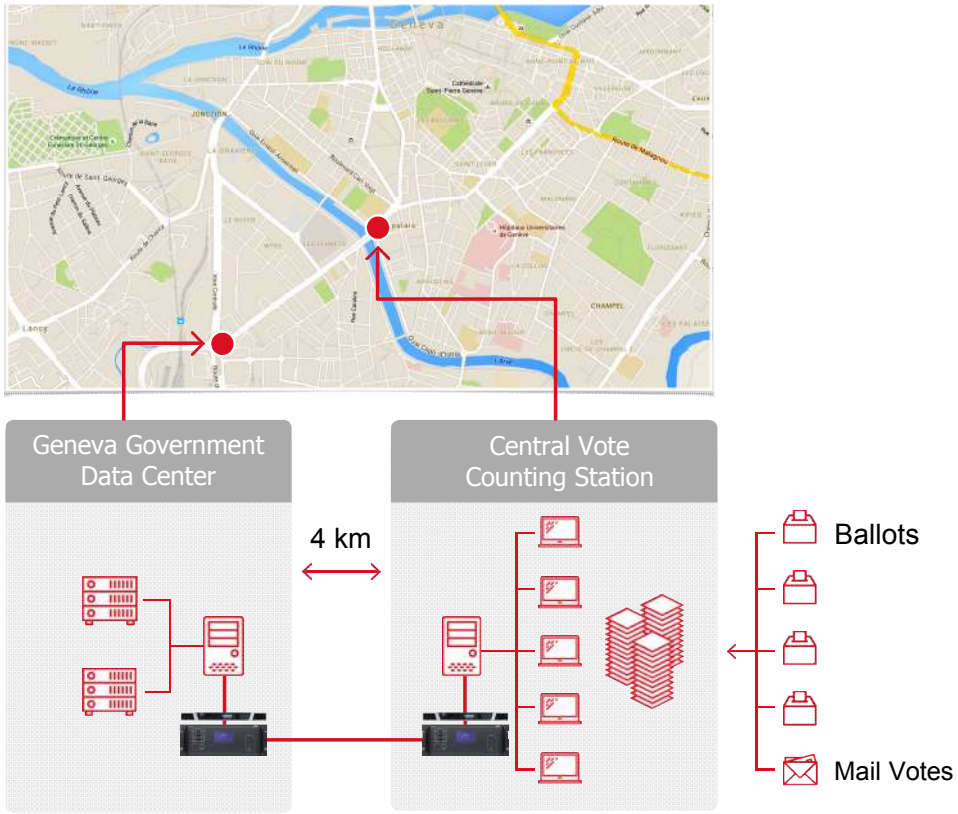
Press release of Geneva State Chancellery

Geneva, October 11th 2007

Geneva is counting on Quantum Cryptography as it counts its Votes

The Swiss national elections on October 21 will mark a world first for Geneva as the canton employs quantum cryptography to protect the dedicated line used for counting its ballots. This unbreakable data code was conceived by the University of Geneva and developed industrially by its spin-off, *id Quantique*. With this

Downtown Geneva



Cerberis QKD Solution

Real Implementation (2) : QKD in Data Center Interconnect

- European banks secure critical links between bank headquarters and Data Recovery Centers, and inside MAN.
  - All digital assets of bank pass over DRC link.
- Supports AES 256 bit key exchange every hour, with additional quantum key buffer.
- Quantum channel:
  - Either on dedicated dark fibre (up to 100km).
  - Or multiplexed with data over single fibre (up to ~30 kms).