The future of Quantum Communications:
From QKD to the Quantum Internet

Quantum Communication Conclave
New Delhi

Bruno Huttner ; ID Quantique

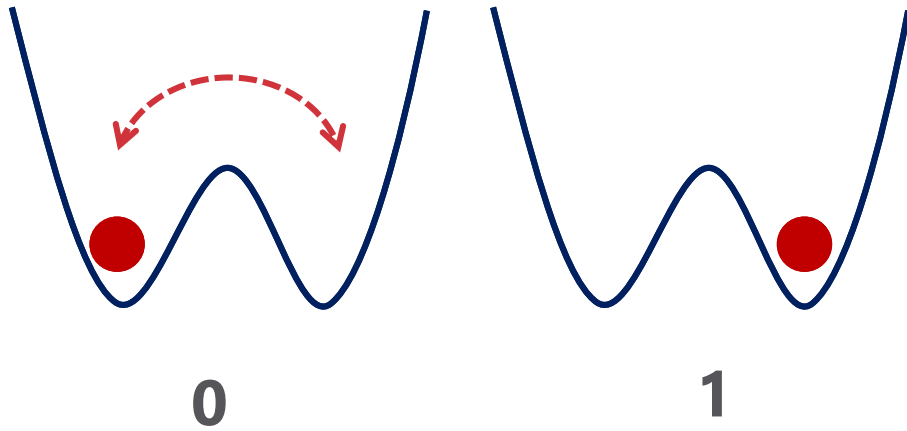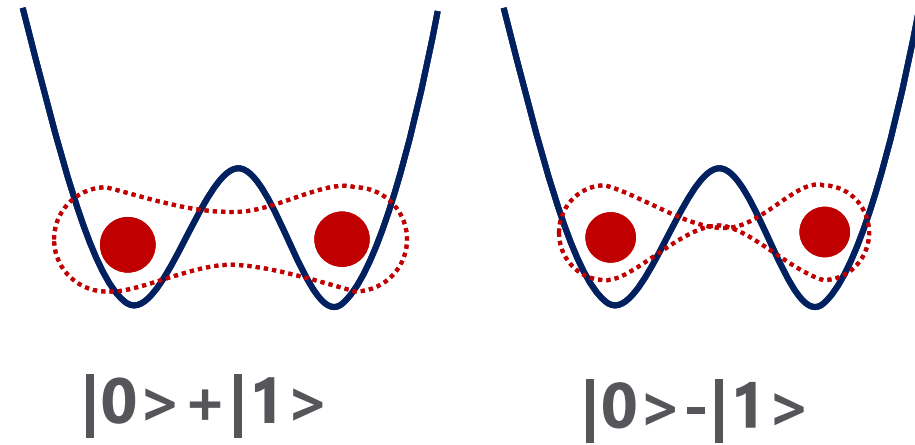March 2023

1 A New Paradigm for

Information Processing

Changing the Building Block: ...Of Bits and Qubits

Classical Computation: bits

Quantum Computation: qubits

0

1

$|0> + |1>$

$|0> - |1>$

Coherent superposition
of quantum states
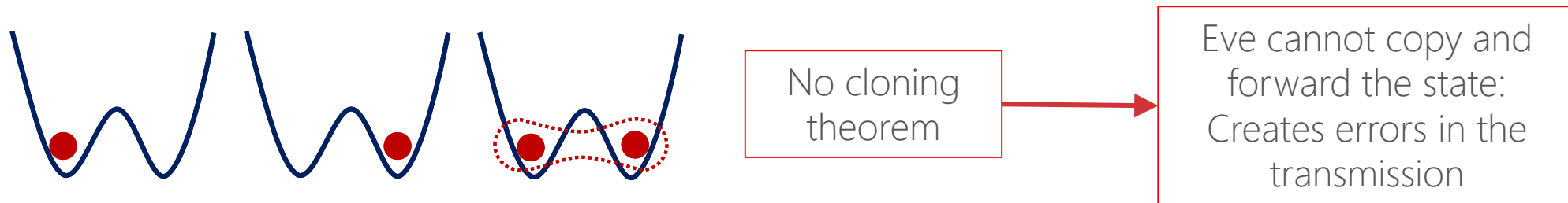
Computation with qubits is a paradigm change

Using the Qubits...

- **To provide randomness:** Quantum Random Number Generator (QRNG)

Measurement → 0

Measurement → 1

$|0>+|1>$

- **To secure communications:** Quantum Key Distribution (QKD) and Quantum Networks

No cloning theorem → Eve cannot copy and forward the state: Creates errors in the transmission

- **To enhance computing power:** Quantum Computer

Based on Entanglement: coherent superposition of multiple qubits
Quantum Computer can process an exponential number of input states in one step

Quantum Communications

2

- Point-to-point QKD
- QKD Networks
- Quantum Networks
- The Quantum Internet

What are we talking about?
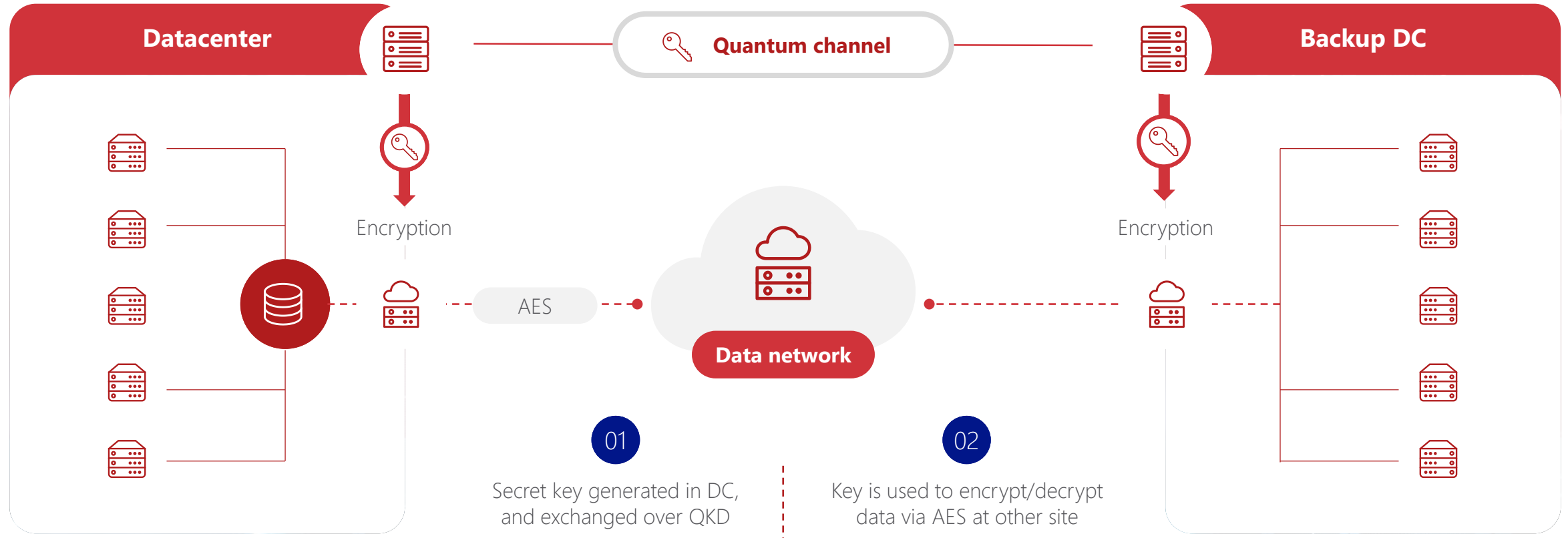
>1 Billion photon/second

60 km

1 photon/second

Adding QKD to your infrastructure: Point-to-Point Key Distribution

Datacenter — **Quantum channel** — **Backup DC**

Encryption — Encryption

AES — **Data network**

01 Secret key generated in DC, and exchanged over QKD

02 Key is used to encrypt/decrypt data via AES at other site
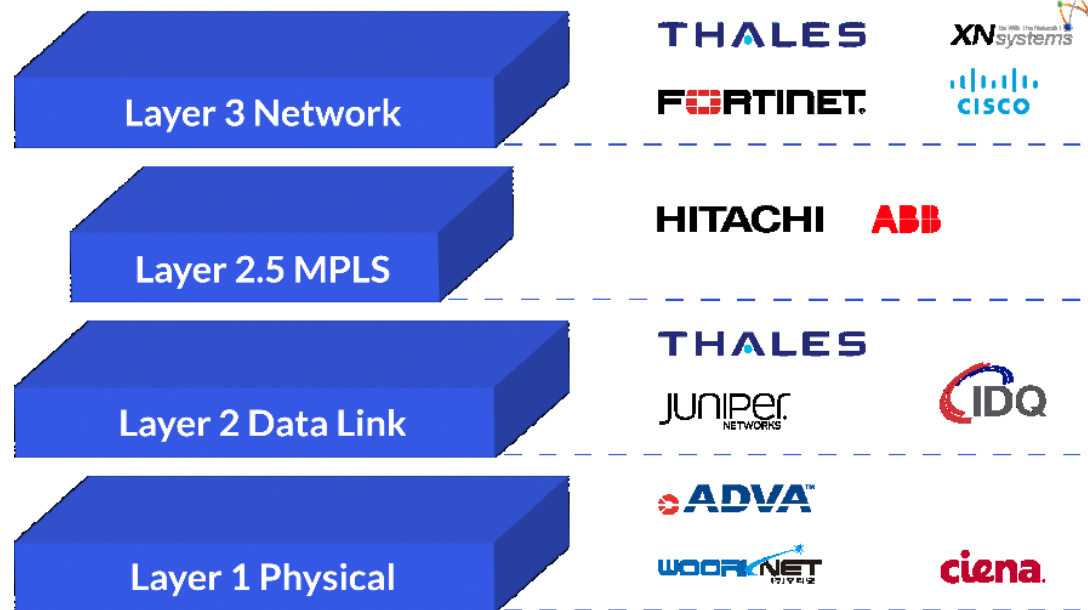
Integrating QKD with existing encryption solutions

IDQ works with different network encryption solutions which may be upgraded with QKD to be Quantum-safe

Benefits of overlaying QKD:

1. Securing your organization in the post-quantum era
2. Reaching long-term confidentiality and aiding data integrity
3. Improving the TCO & ROI of your incumbent encryption solution
4. Acting as a 'value-add', demonstrating your cybersecurity commitments to stakeholders

Supported/PoC Vendors

Layer 3 Network

THALES
FORTINET
XN Systems
cisco

Layer 2.5 MPLS

HITACHI   ABB

Layer 2 Data Link

THALES
JUNIPER NETWORKS
IDQ

Layer 1 Physical

ADVA
WOORINET
ciena

Current limitations of QKD...and how to overcome them

Limitations

Physical infrastructure

Point-to-point
physical connection

No standards

Cost

Requires authentication

Distance

Solutions

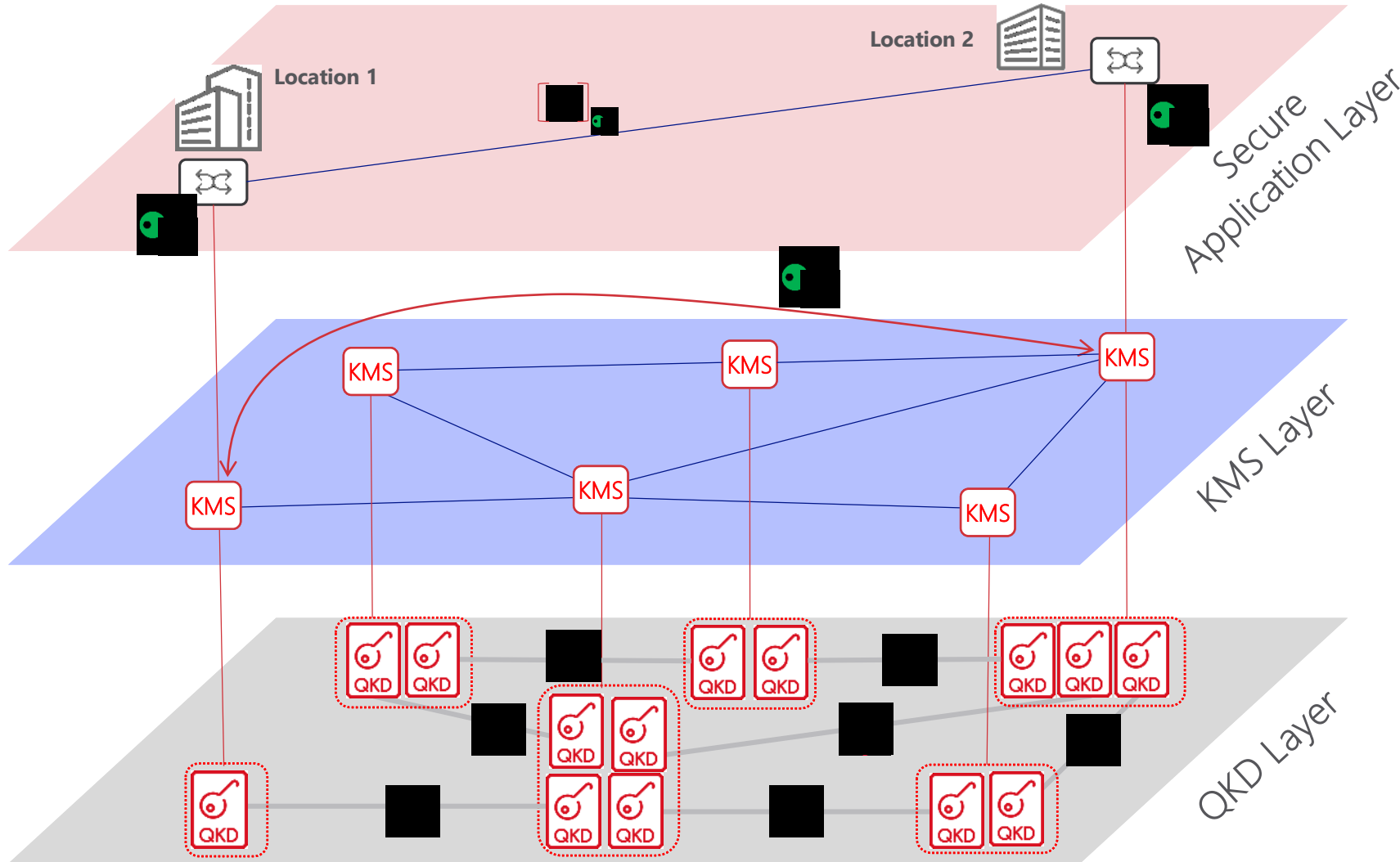None: same as internet!

QKD Networks

Work In Progress

QKD on chip

Pre-shared key OR
QR algorithms

Trusted Nodes
Satellites
Quantum Repeaters

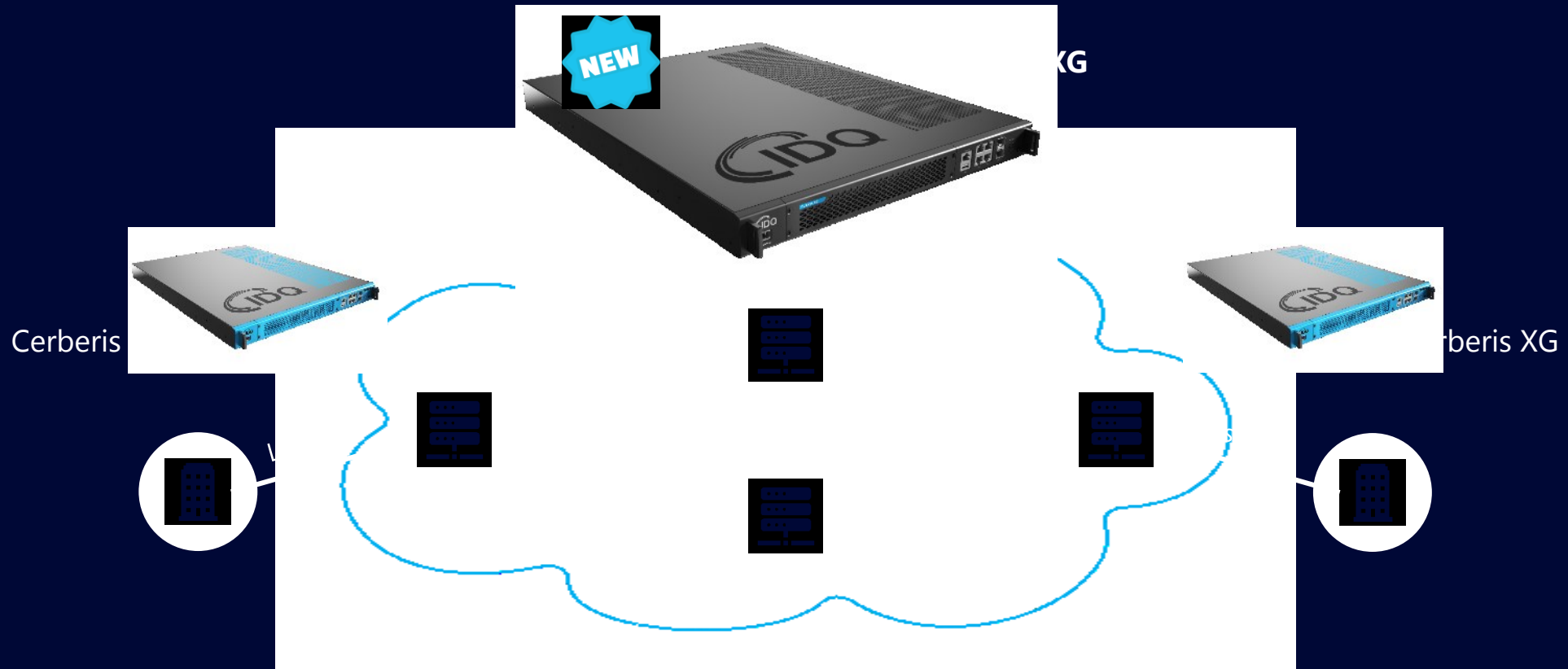# QKD Networks with Trusted Nodes

KMS is the glue of the QKD network

It ensures QKD keys are synchronized through QKD network

The first comprehensive range of Quantum Key Distribution solutions

✅ Proven and highly reliable technology

✅ Designed for complex topologies and large-scale deployments

Cerberis XG

Cerberis XG

QKD Networks: Korean National Convergence Network Project

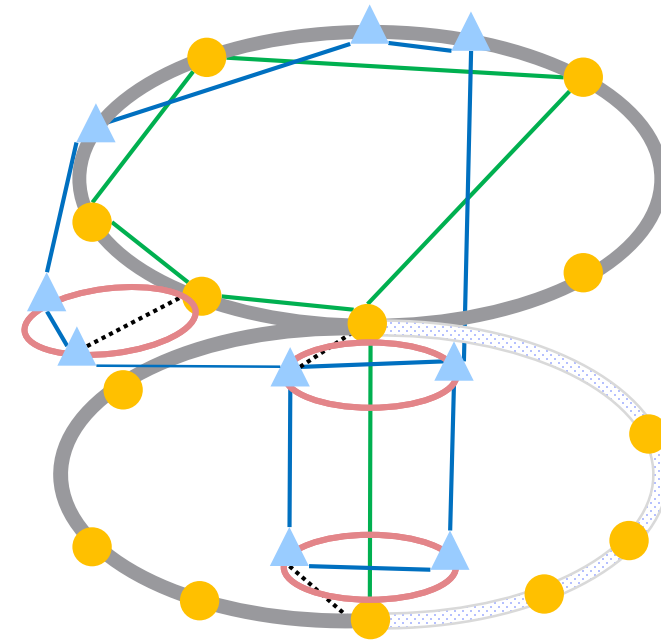IDQ and SK Broadband selected for the construction of the first nation-wide QKD network in Korea

2000 kilometers

48 government organizations

Security, stability & efficiency

[QKD & KMS Network]

▲ Gov. regional office		⬭ Customer ring	
● SKB regional office		⬭ SKB backbone	
▬ Customer KMS link		▪▪▪ Ext. key	
▬ SKB KMS link			

QKD Networks in the EU: the Euro-QCI Initiative

Part of EU Cybersecurity Strategy for the coming decades.

Quantum Communication Infrastructure
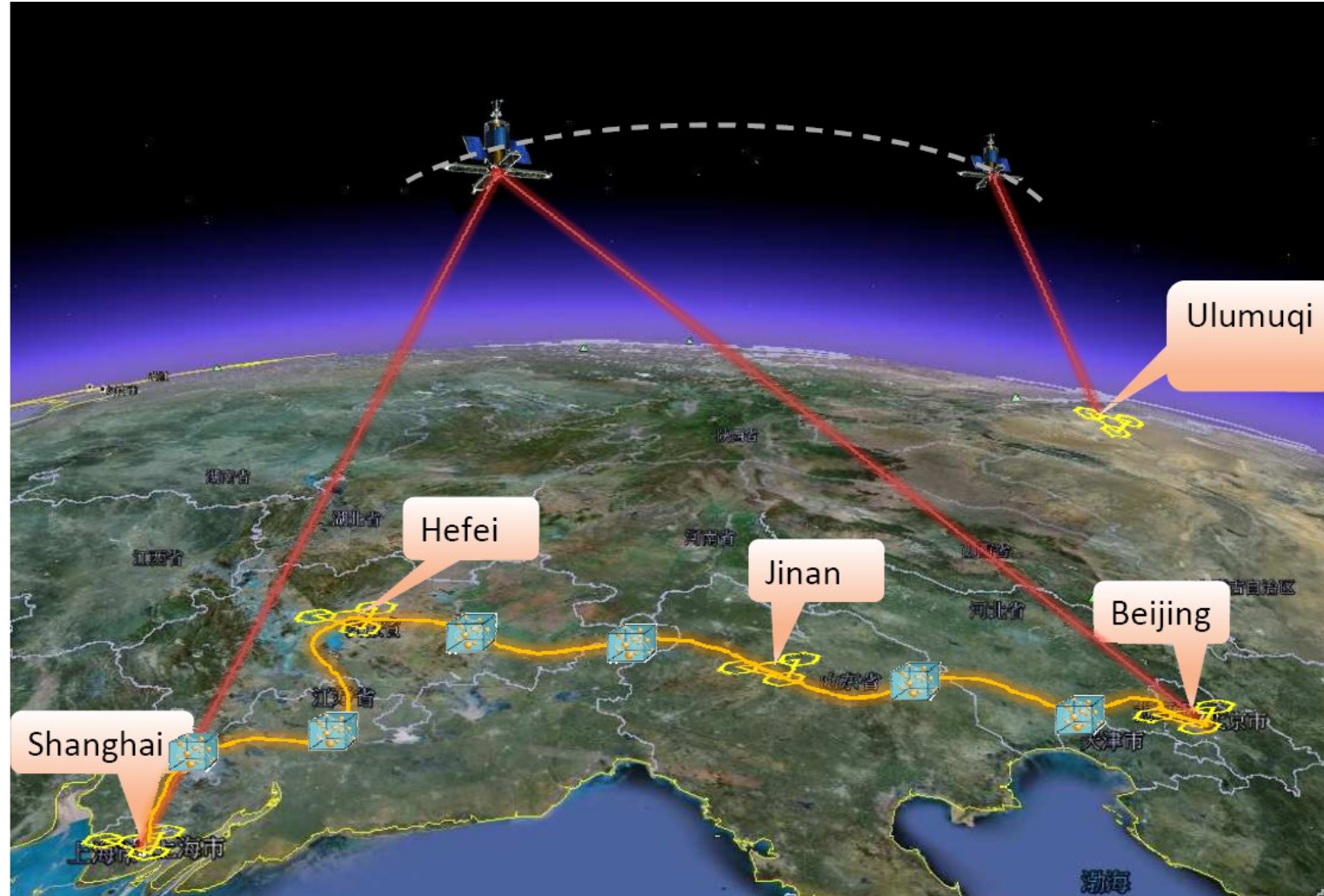
Aiming at safeguarding sensitive data and critical infrastructures by
integrating quantum-based systems
into existing communication infrastructures.

- Preliminary stage (2020-2022): OpenQKD consortium and QKD Testbeds

- First phase (2022-2023): National Phases

- Second phase (2024 any beyond): Roll out

- Fully operational by 2027
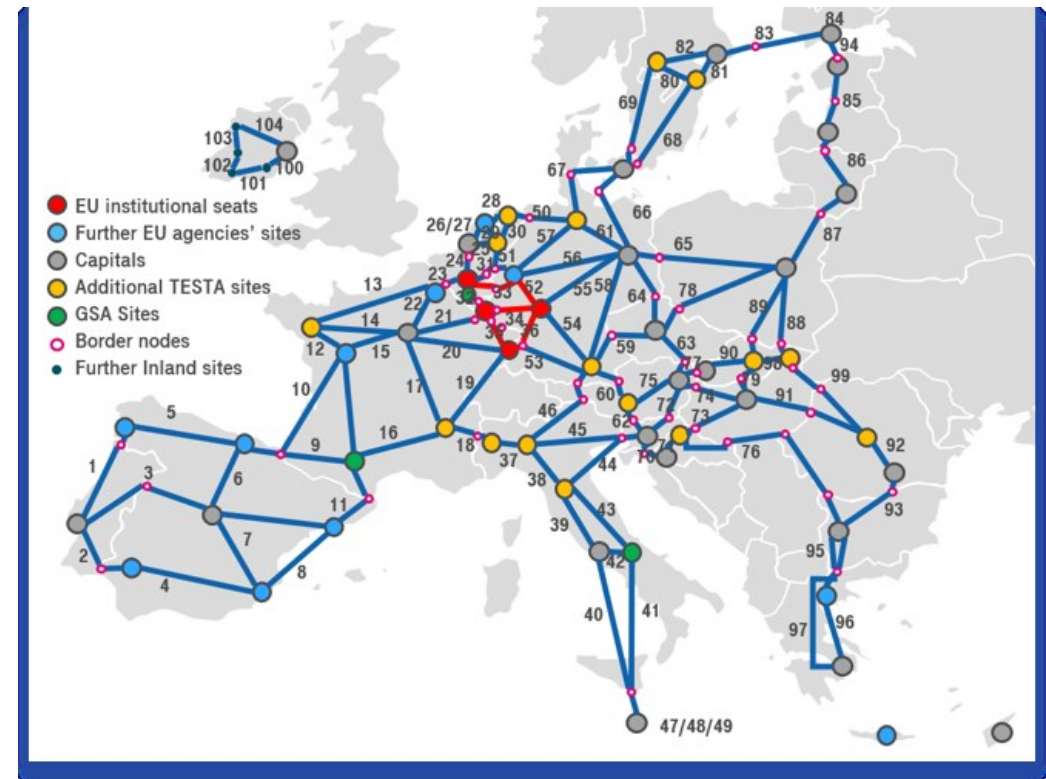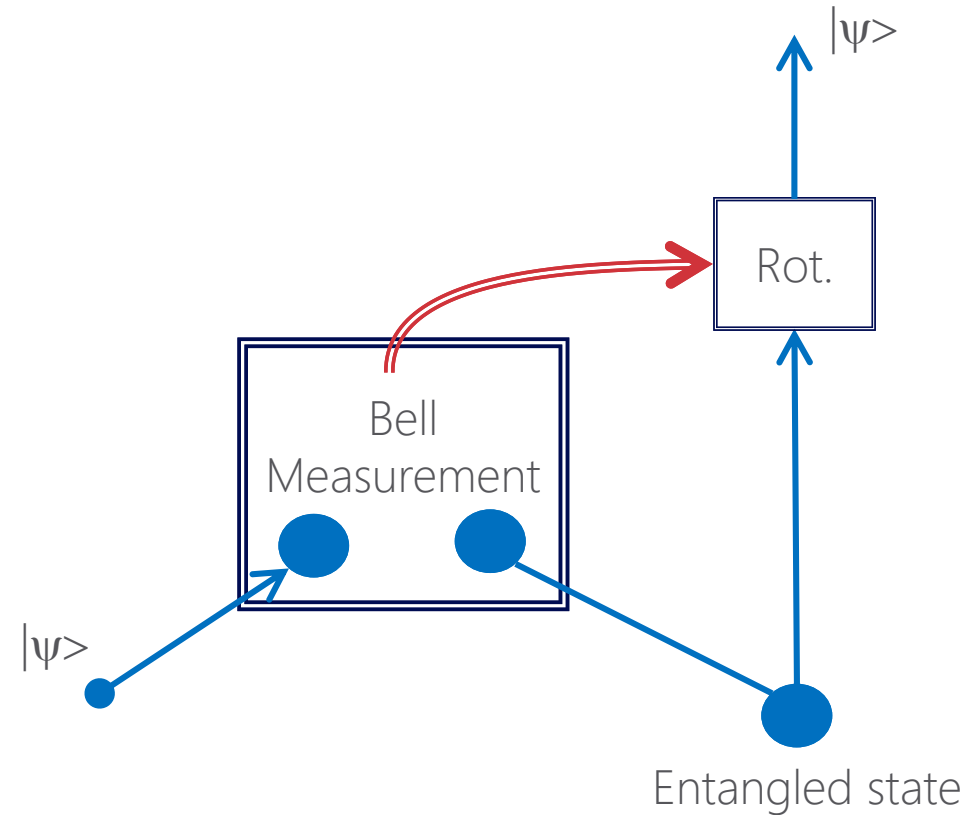
A hybrid Chinese QKD network

The building blocks for Quantum Networks

- Entangled States
- Bell Measurements
- Quantum Memories
- Teleportation

$\Rightarrow$ **Transfers quantum states across the network**

Quantum Internet: A world-wide Quantum infrastructure

- Build a quantum infrastructure

- Each node stores and exchanges qubits with the others

- Can be used as a global QKD network

- ... and much more!

Summary: Key points

1 Quantum Era is at our door

2 We need to revamp our Network Security

3 Quantum Communication is required for Quantum-Safe Security

4 Start today with point-to point QKD and QKD Networks

5 … And continue tomorrow with
Quantum Networks and the future Quantum Internet

ID Quantique

Quantum.
Trust enabled for the future

Q & A

bruno.huttner@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity