YEARS
QUANTUM
INNOVATION

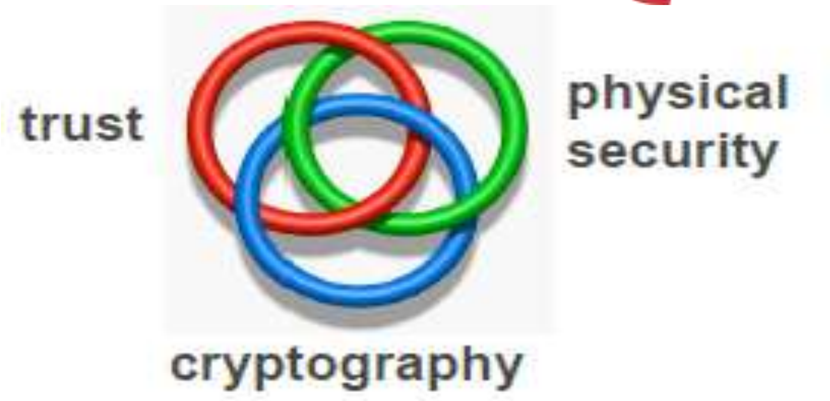
Deploying Future-Proof Secure National Networks

Quantum Communications Practical Applications

Grégoire Ribordy, CEO
ID Quantique SA

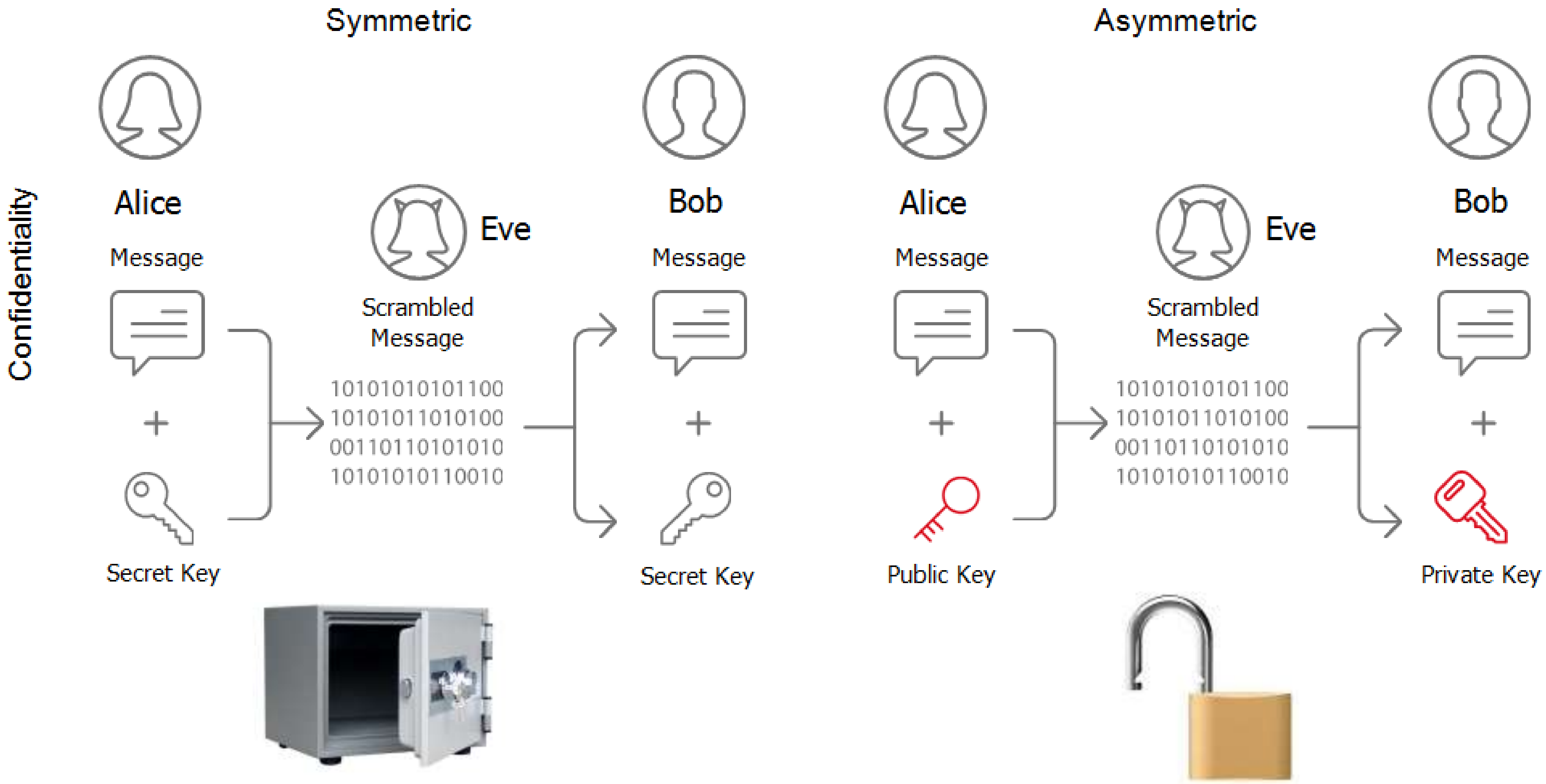
07/04/2025

Cryptography…



- … is a foundational pillar of cybersecurity
  - Cryptography allows us to achieve information security while using untrusted communication systems.
  - Example: Do you use e-banking? Why do you trust the system?
  - Information security requires
    - Confidentiality
    - Integrity
    - Authentication
    - Non-Repudiation

Cryptographic Primitives



Symmetric

Asymmetric

Confidentiality

Alice

Message

+

Secret Key

Eve

Scrambled Message

10101010101100
10101011010100
00110110101010
10101010110010

Bob

Message

+

Secret Key

Alice

Message

+

Public Key

Eve

Scrambled Message

10101010101100
10101011010100
00110110101010
10101010110010

Bob

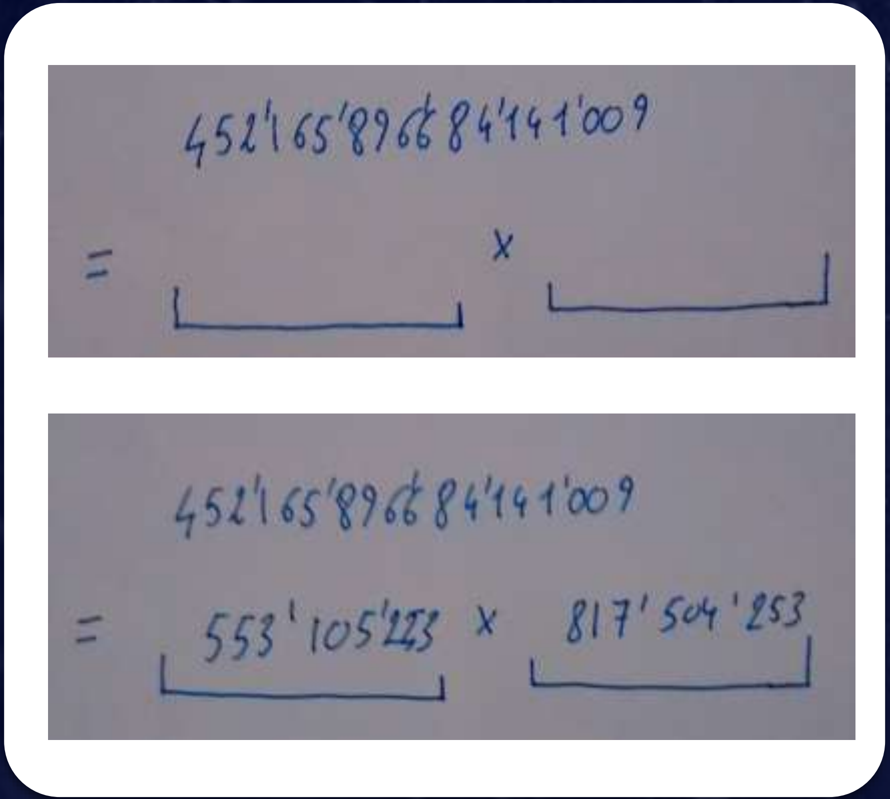
Message

+

Private Key

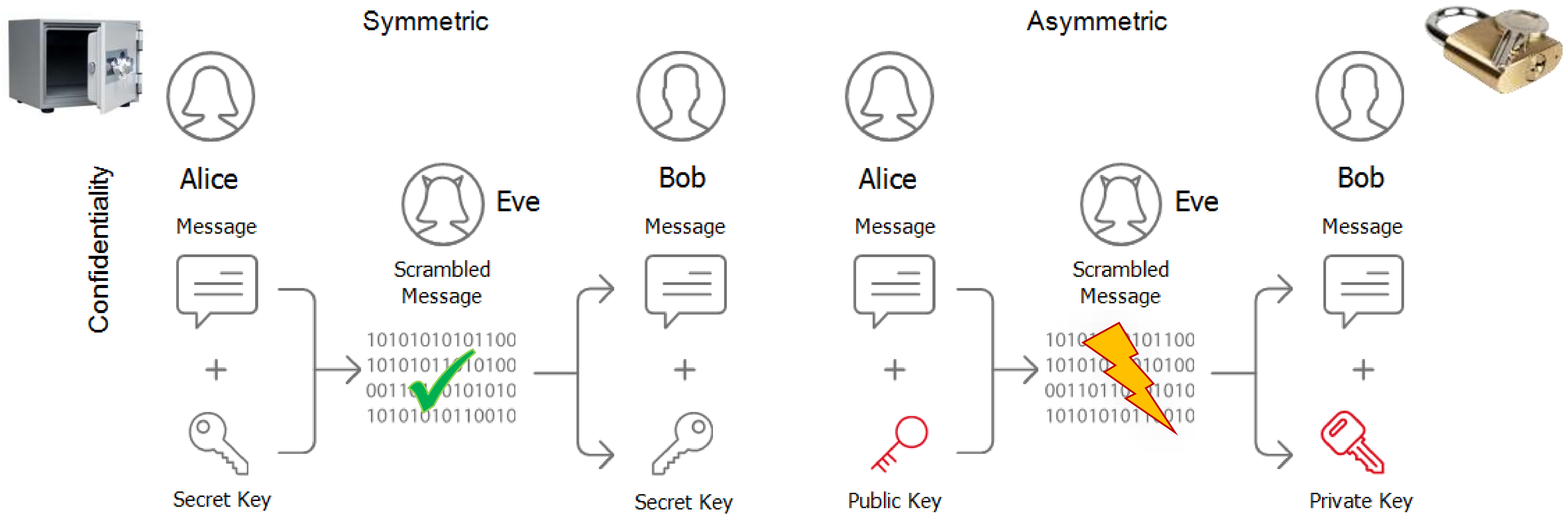
Quantum Computing Impact on Cryptography

Threat: Factoring becomes an **easy** problem; breaks current public key cryptography (DH, RSA, ECC…)



Shor's Algorithm, 1994

Cryptographic Primitives



Confidentiality

Symmetric

Alice

Message

+

Secret Key

Eve

Scrambled Message

Bob

Message

+

Secret Key

Asymmetric

Alice

Message

+

Public Key

Eve

Scrambled Message

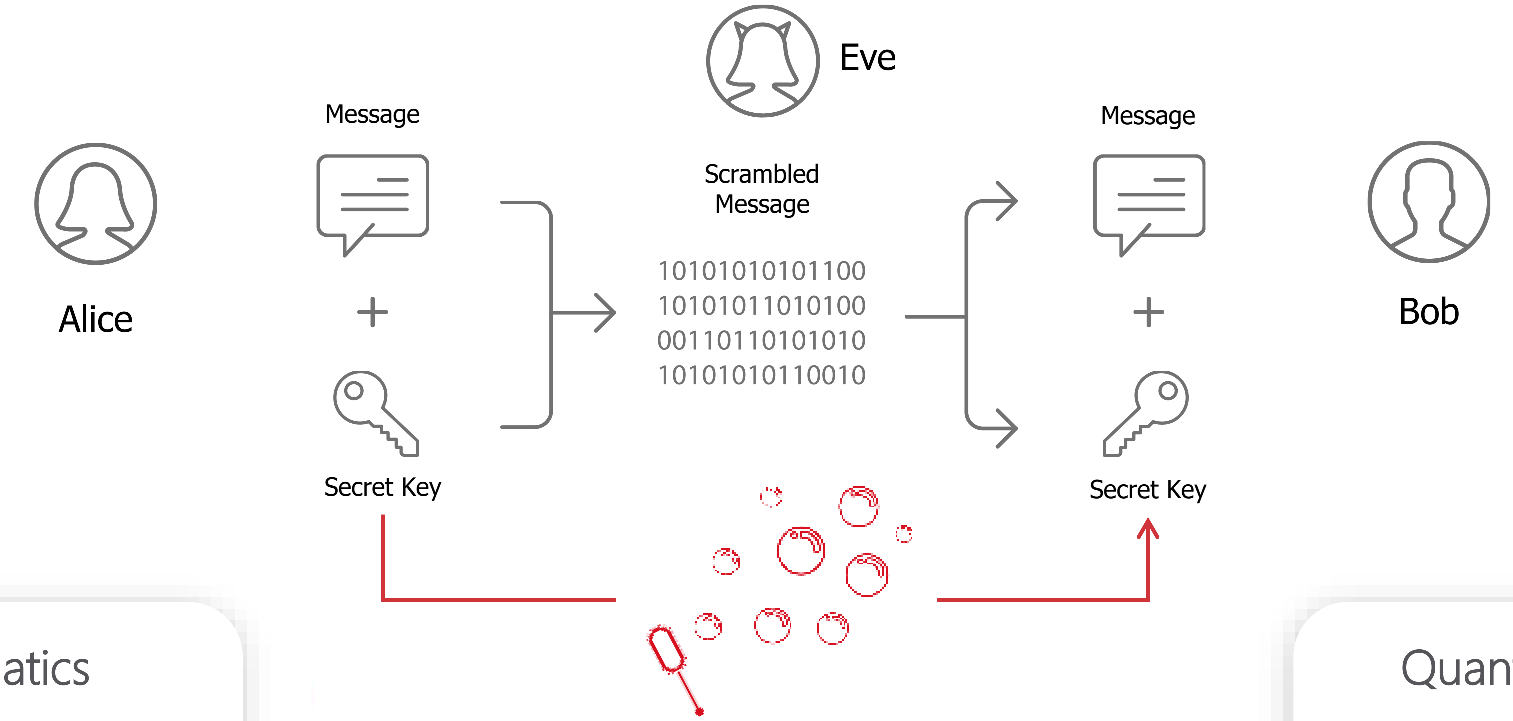
Bob

Message

+

Private Key

Quantum-Safe Cryptography



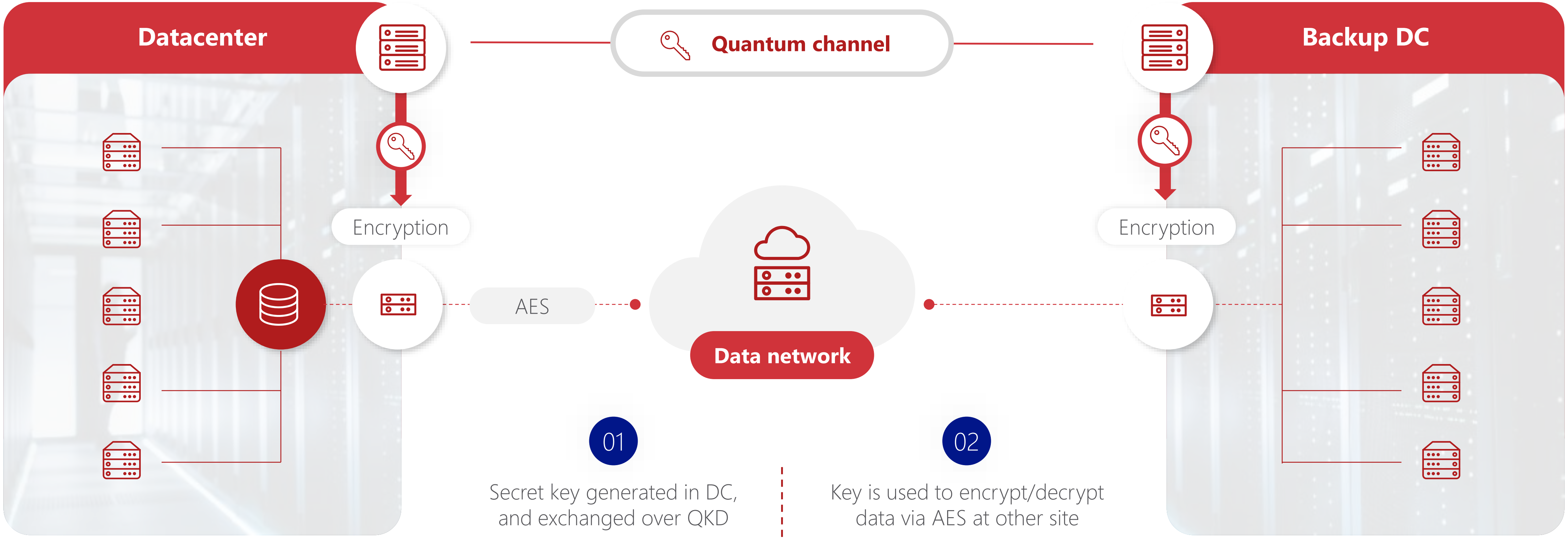
Mathematics

Post-Quantum Crytpography (PQC)

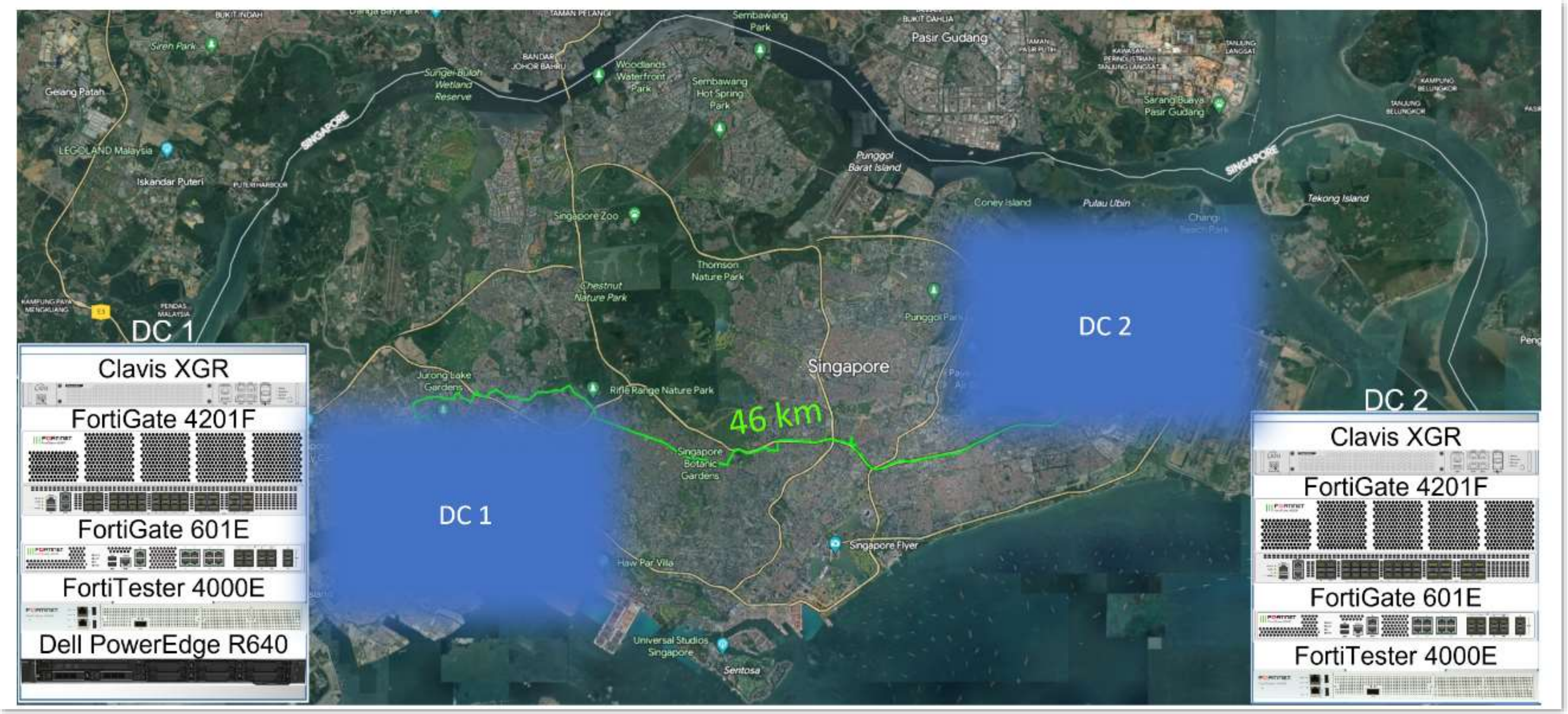
Quantum Physics

Quantum Key Distribution (QKD)

Long-Term Security with QKD


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

JPMorganChase establishes quantum-secured crypto-agile network



https://arxiv.org/pdf/2405.04415

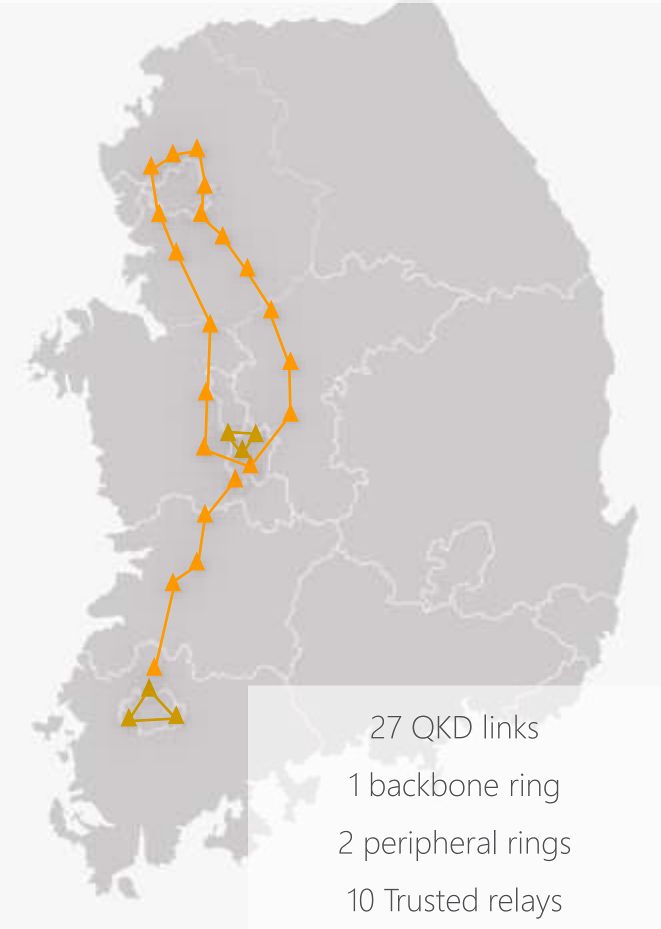
Korean National Convergence Network Project

2000 kilometers

48 government organizations

Security, stability & efficiency

QKD Physical Layer



27 QKD links

1 backbone ring

2 peripheral rings

10 Trusted relays

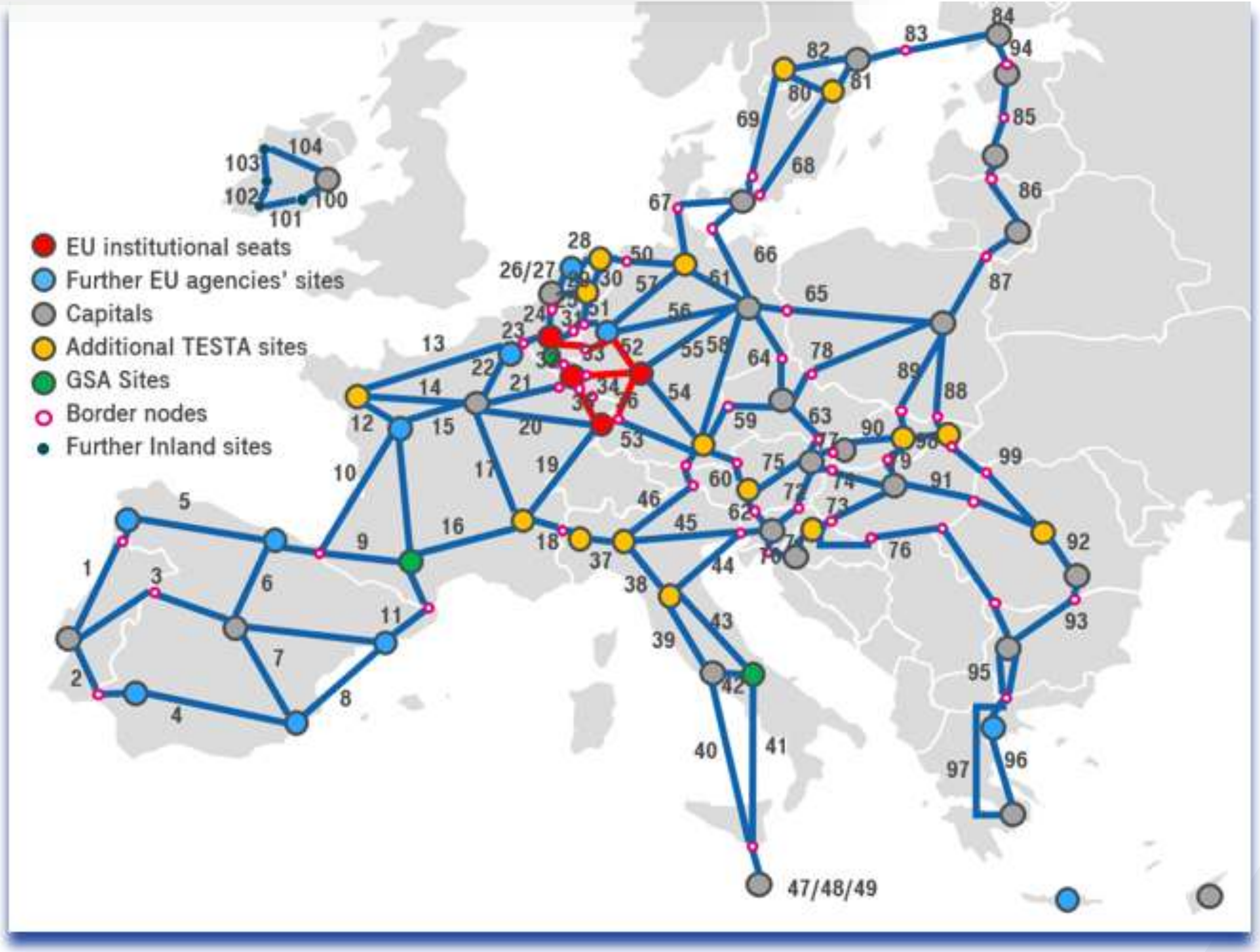
The EuroQCI Initiative

Cybersecurity Strategy for the coming decades.

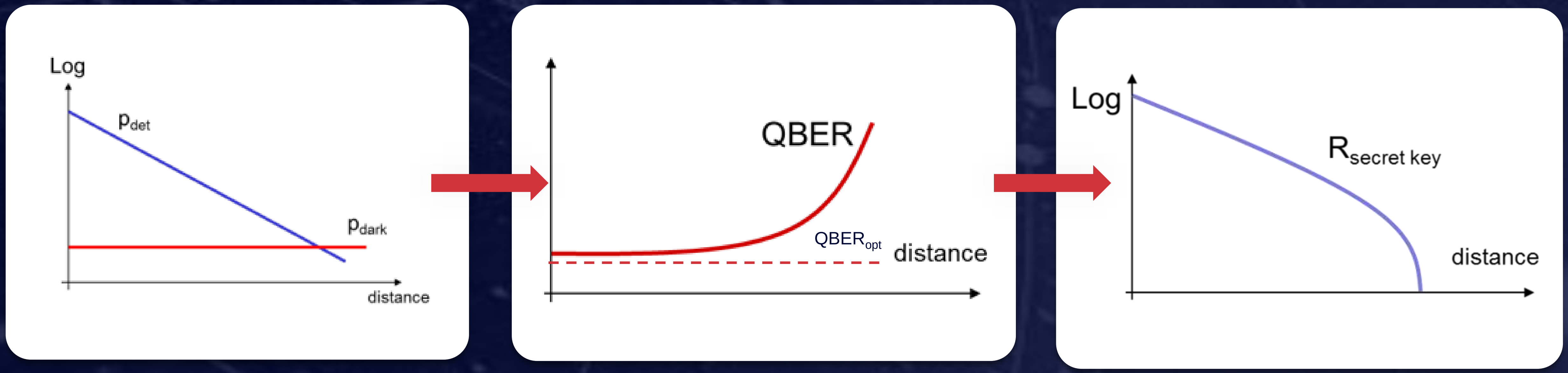
Aiming at safeguarding sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures.

- First phase 2022-2023 National Phases
- Second phase 2024 any beyond – roll out
- Fully operational by 2027

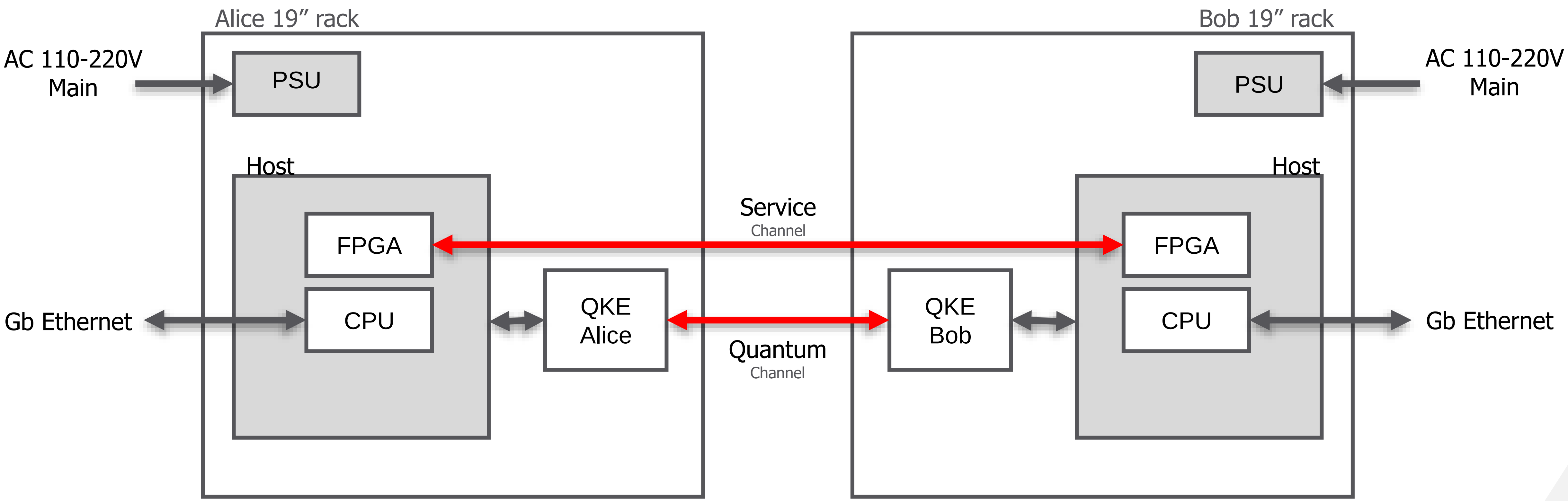
EU Quantum Communication Infrastructure



QKD Generic Performance



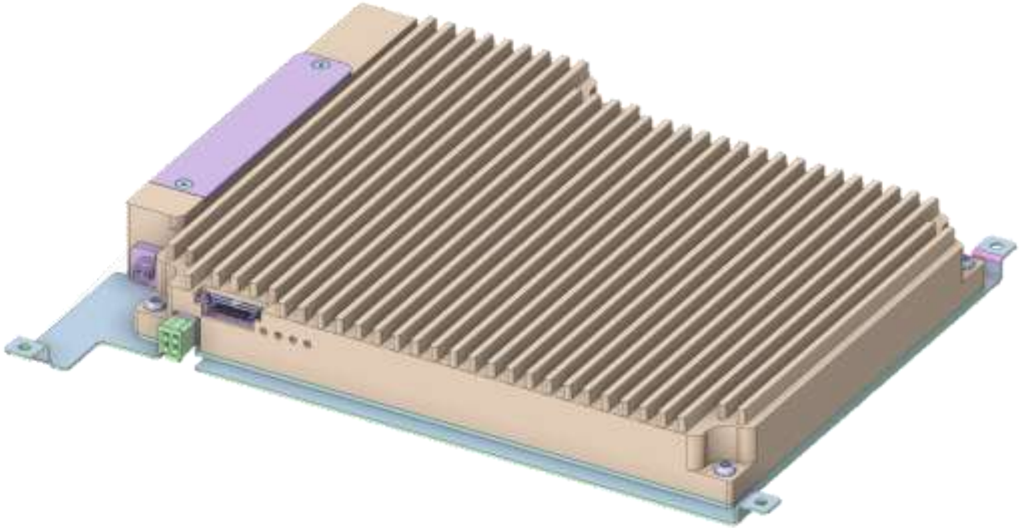
XG Series Block Diagram

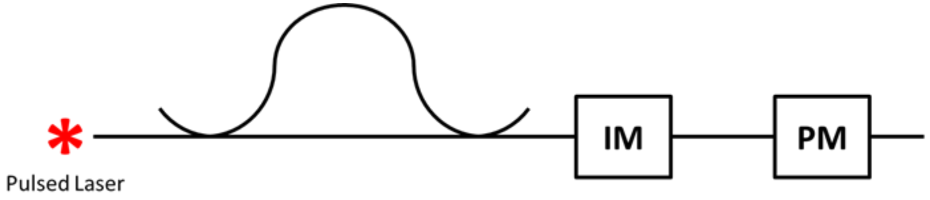


QKE Alice

MAIN SPECS:

- 4-state BB84 + 2 decoys
- Time-bin phase encoding
- Pulse frequency: 1 GHz
- Qubit Frequency: 500 MHz
- Integrated monitoring, filtering, IF stabilization and locking with Bob IFs



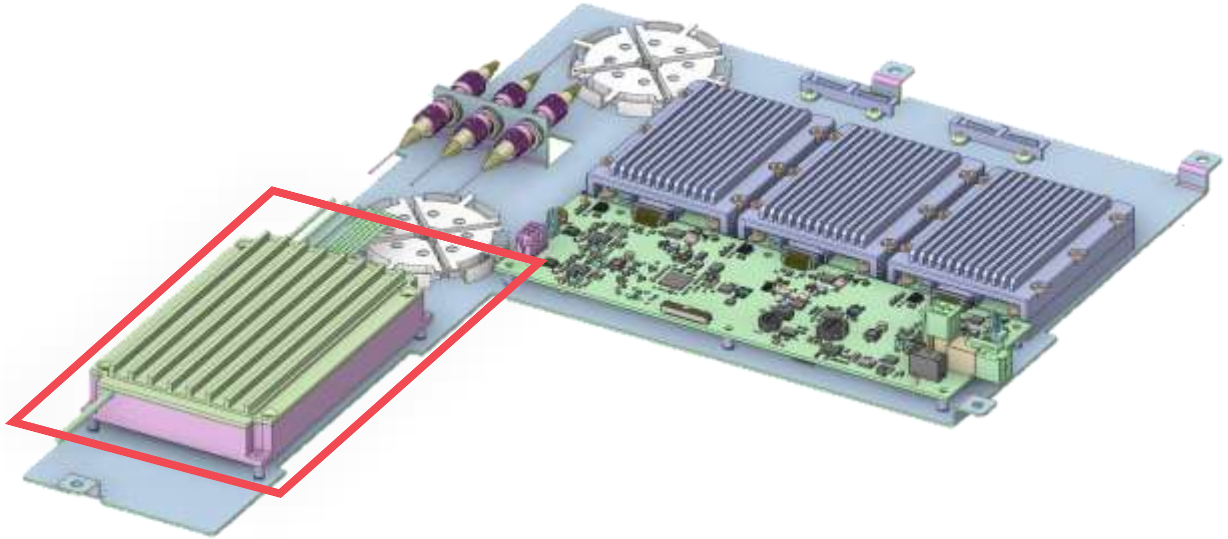


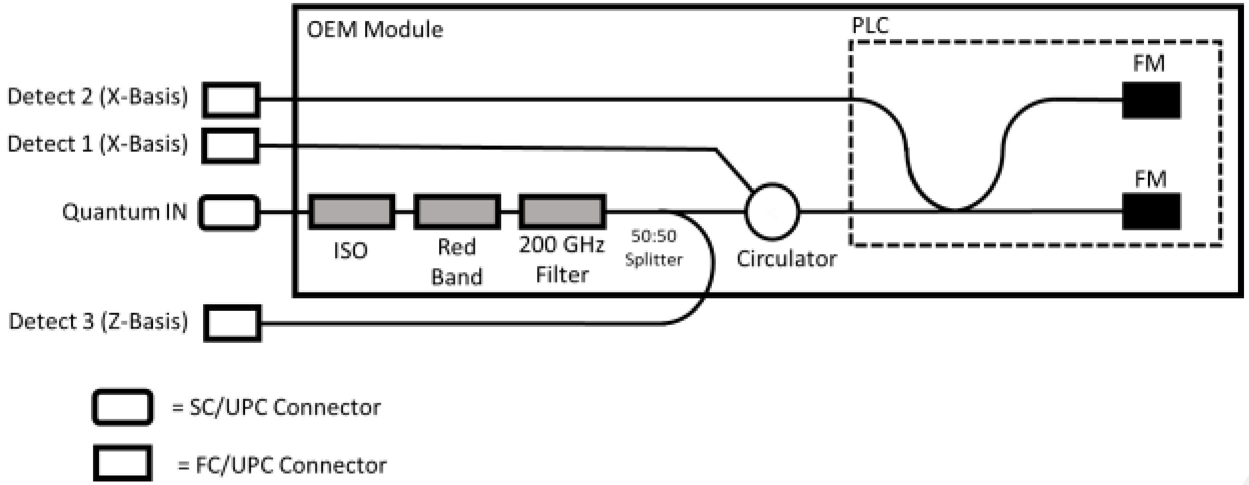
QKE Bob

MAIN SPECS:

- Fiber-based passive components + PLC interferometer (in a temperature stabilized package)
- Optical losses < 5-6 dB
- Temperature stability of IF <= +/- 0.001 °C

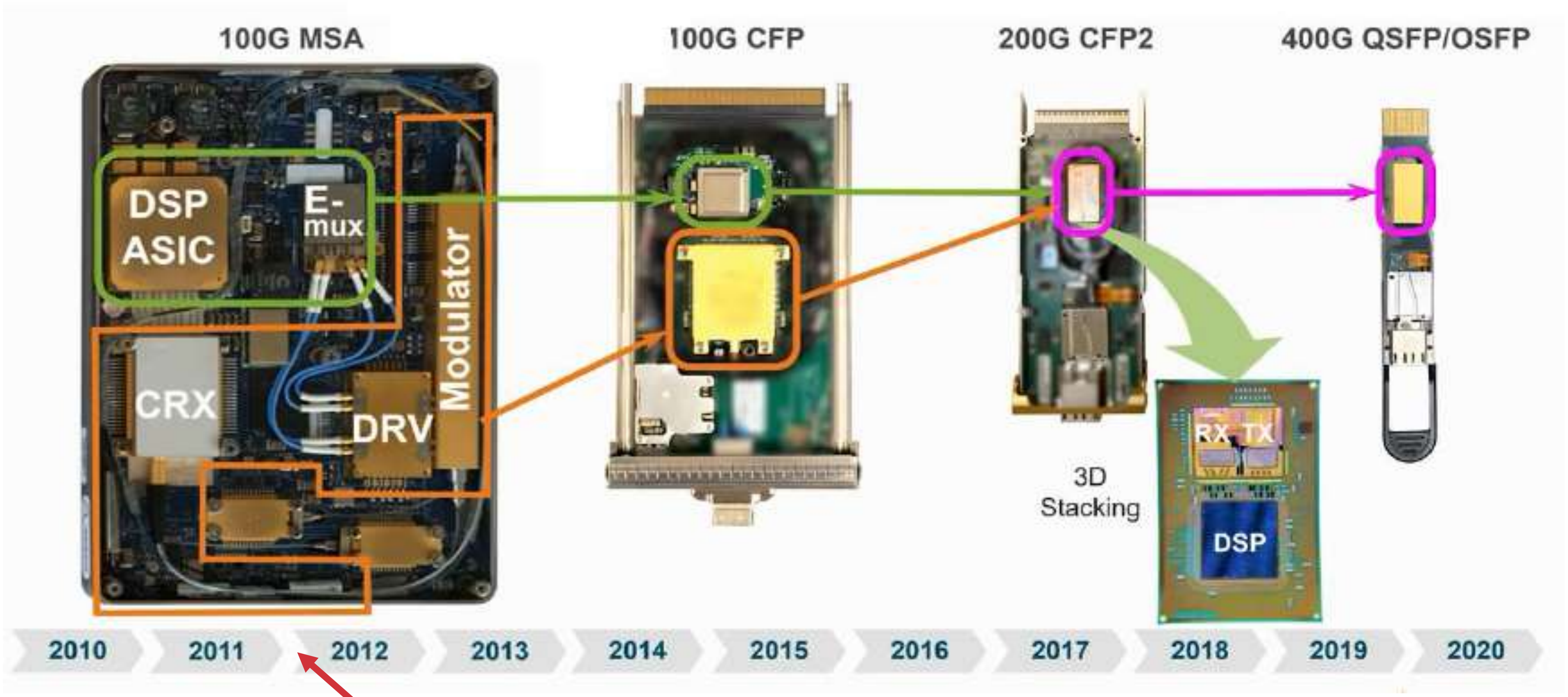
Visibility > 99.5 % for any input polarizations state





Datacom Analogy

50-100k$ → 5-10 k$ → 0.5 - 1 k$



QKD is here

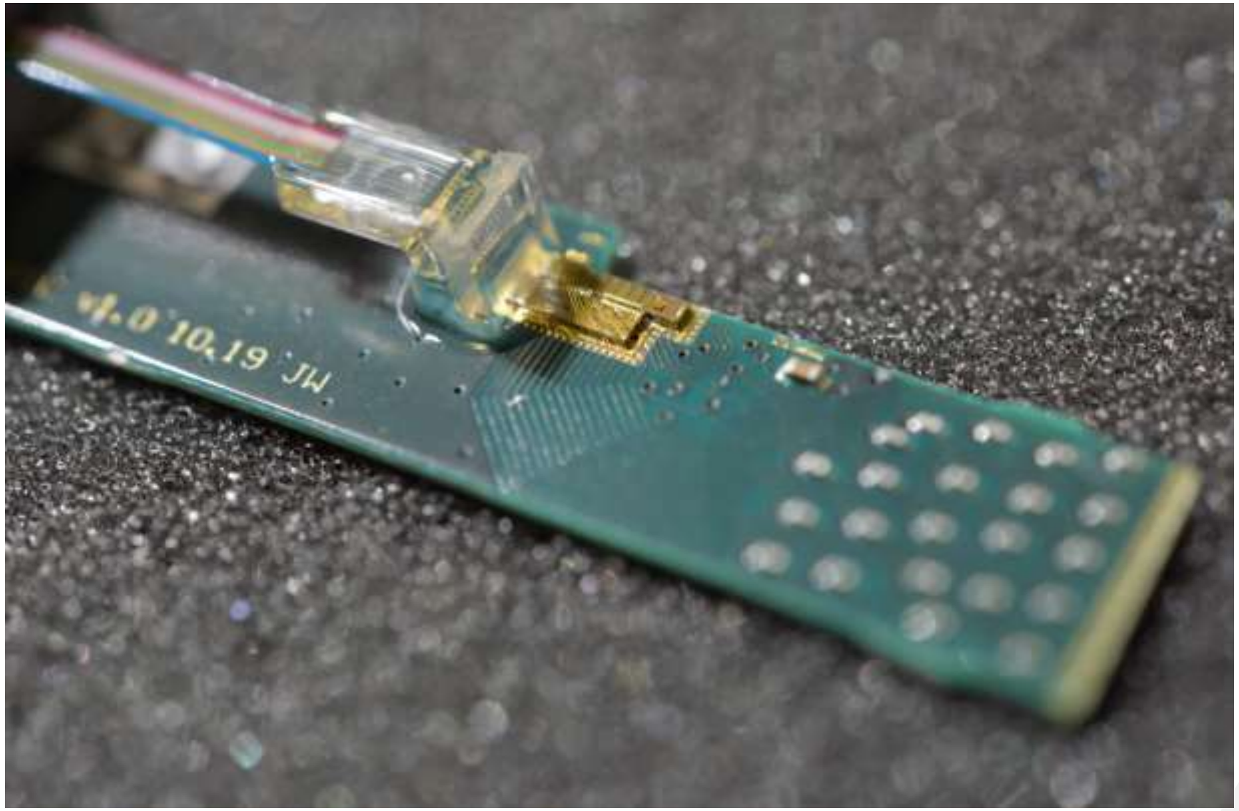
Silicon Photonics Based Transmitter (Alice)

Platform choice

Pros: Small footprint, PIC and IEC, fast modulation

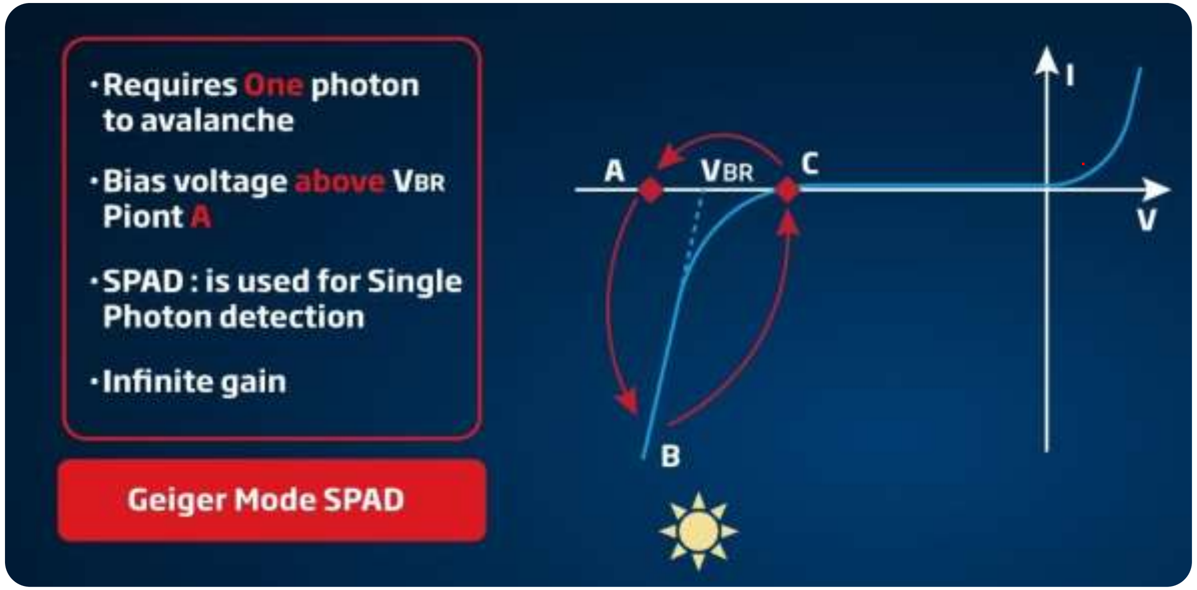
Cons: Cannot integrate laser

Footprint: 1.1 mm x 4.5 mm



Detecting Single-Photons

Single-photon avalanche detectors (SPAD)

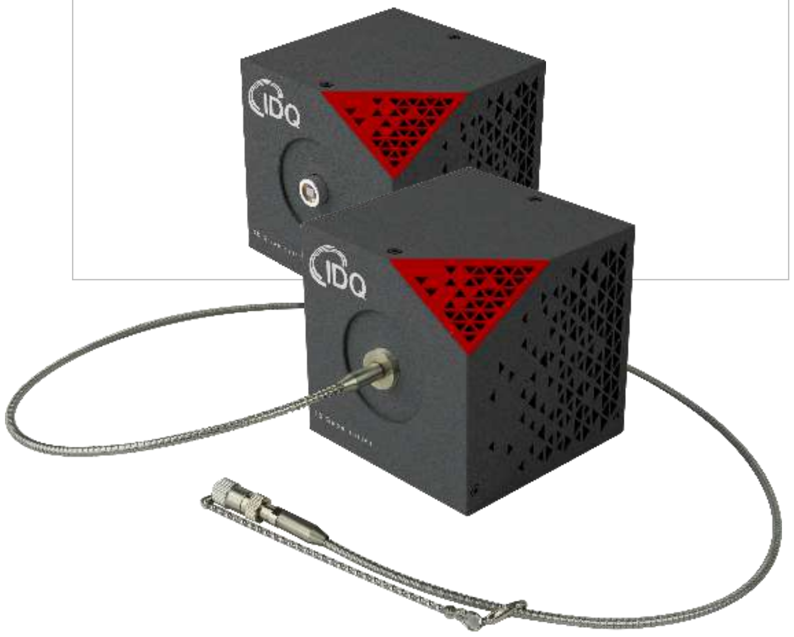


- Requires One photon to avalanche
- Bias voltage above VBR Piont A
- SPAD : is used for Single Photon detection
- Infinite gain

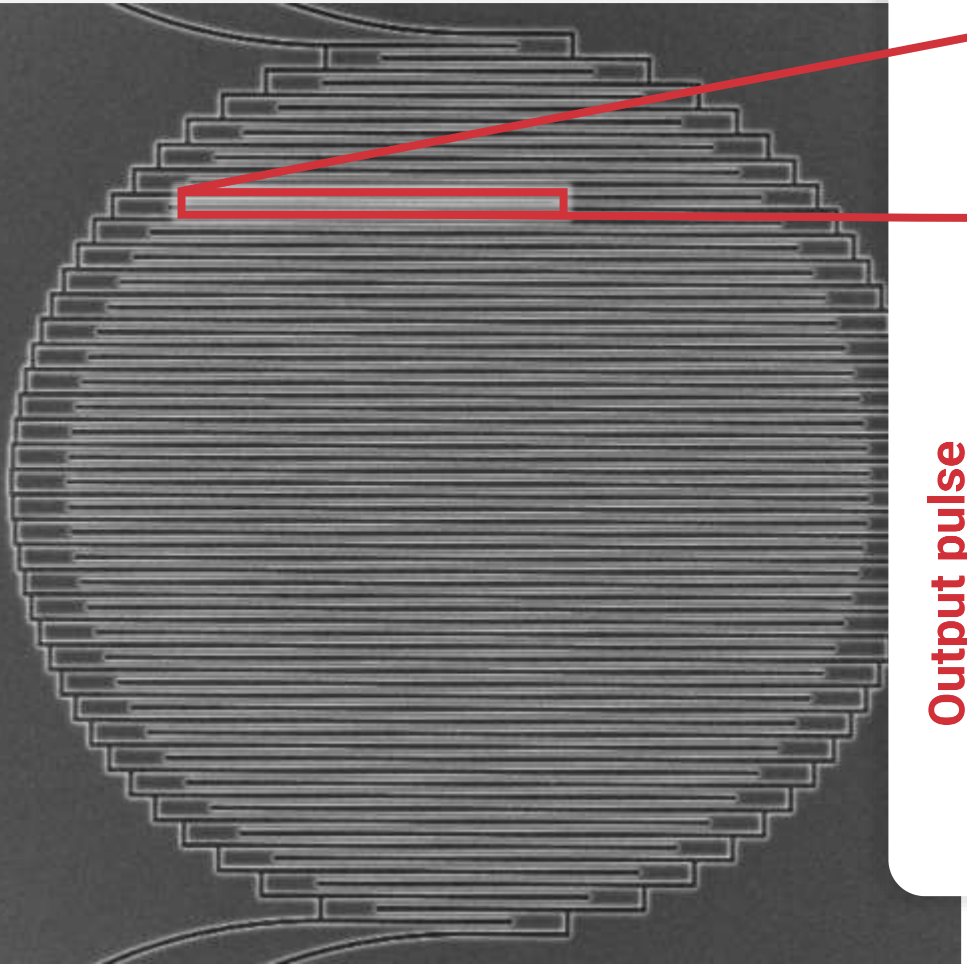
Geiger Mode SPAD

Performance	Si	InGaAs
Detection Efficiency :	80% (vis)	25% (NIR)
Dark Counts :	~10-100Hz	~1KHz
Counting Rate:	1-10MHz	<10MHz

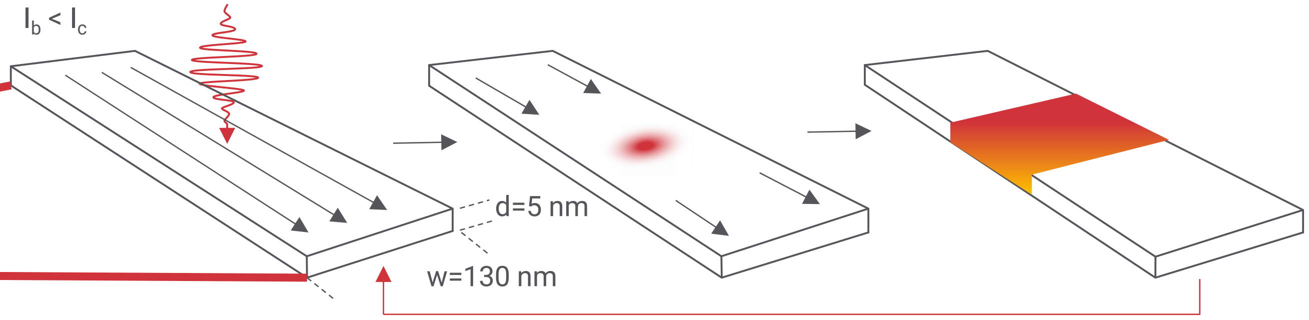
ID Qube



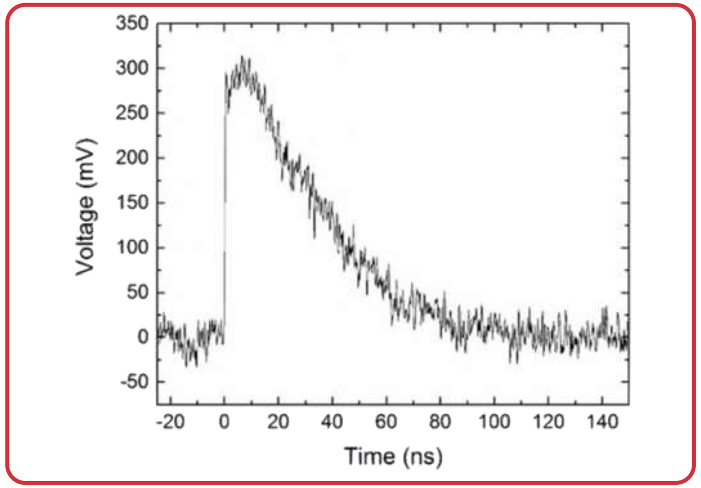
Superconducting nano(wire/strip) single-photon detectors (SNSPD)



Operating principle



Output pulse



Operating mode

Free-running: the operating circuit yields passive resetting

Asynchronous

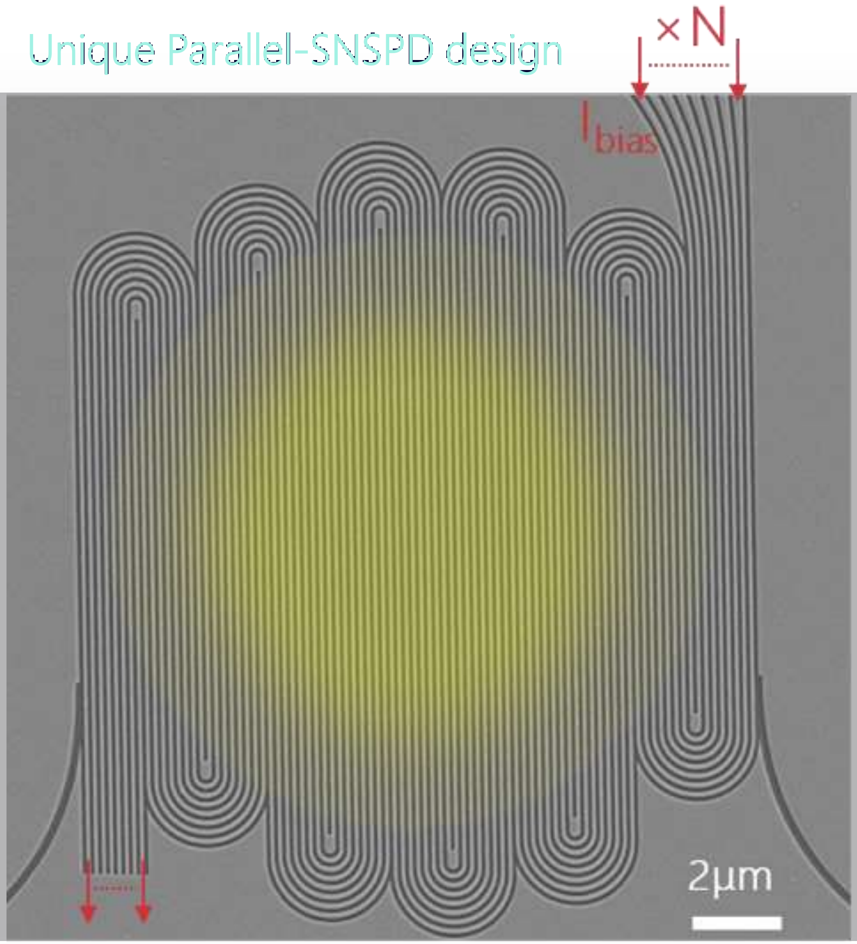
Ultrafast and photon-number-resolving SNSPDs

INNOVATION AWARD

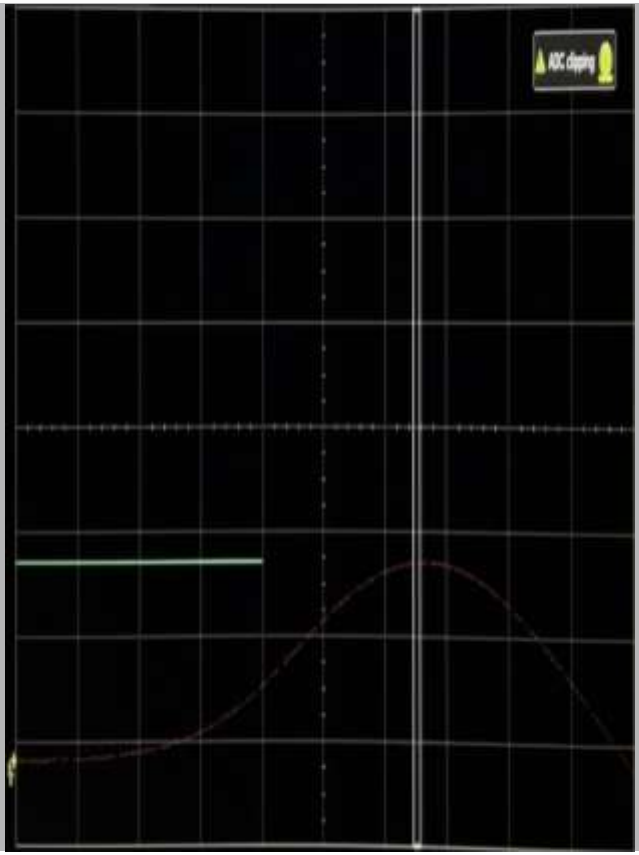
LASER PHOTONICS

EUROPA SCIENCE

Unique Parallel-SNSPD design



Pure PNR performance



Optimized photon-number identification

Photonic quantum computing

Detection at more than 250 Mcps

Ultra-high key rate QKD

Enterprise-ready SNSPD system - introducing the ID281 Pro

Let the Pro create some magic

- Rack mountable, fully automatic cooldown and operation
- With IDQ's Clavis XGR : QKD over hundreds of km made easy
- Perfect for a Satellite-QKD ground station
- Easy fit in a quantum computing or quantum networking rack

ID Quantique

Quantum.
Trust enabled for the future

Q & A

info@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