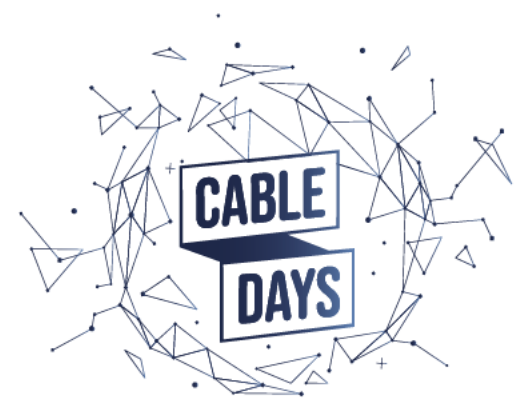


ZERO/3

LIVE ON AIR, SECURED BY QUANTUM PHYSICS

Lukas Helm, Head of Sales, zerothird

Design Center Linz, 09.10.2026



NETZE | PLATTFORMEN | KOMMUNIKATION



Telekom · Rundfunk

LIVE ON AIR, SECURED BY QUANTUM PHYSICS

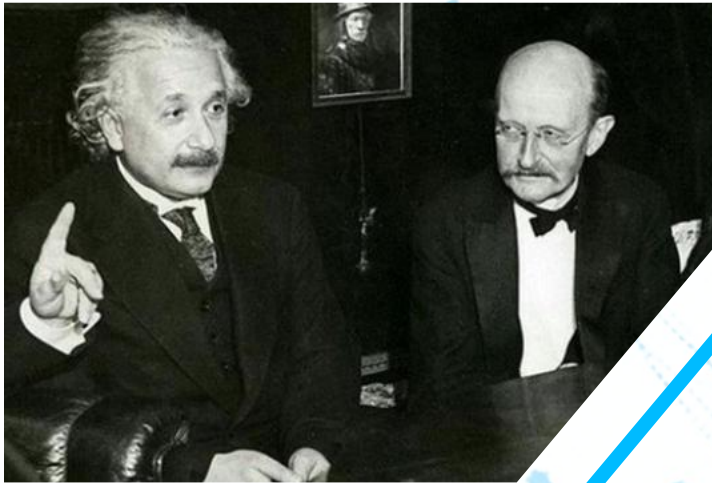


1

QUANTUM PHYSICS

QUANTUM PHYSICS — A MODERN SCIENCE

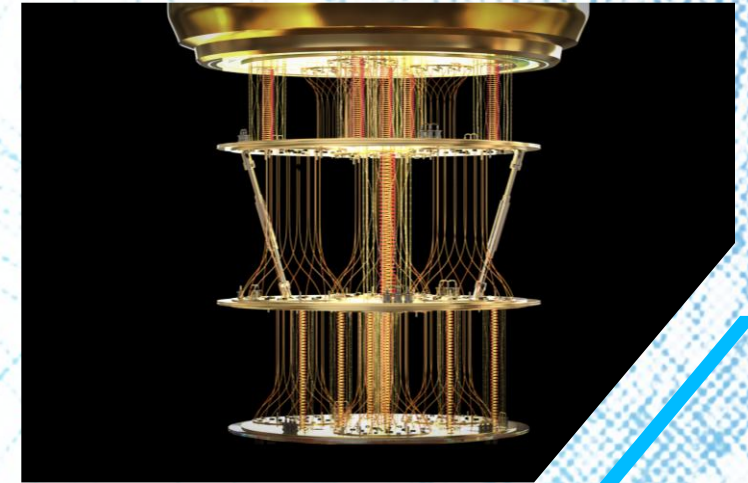
A century of proof. A future of innovation.



- 120+ years since Planck and Einstein
- Verified in every experiment, every day

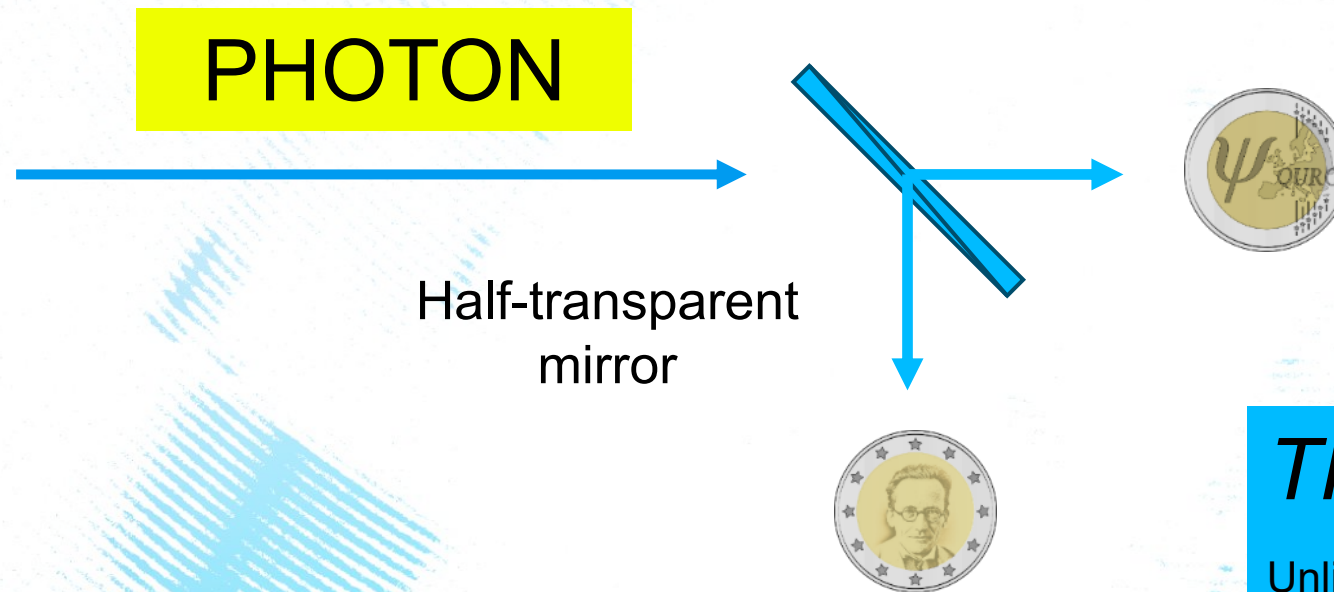


- 3 out of the last 4 nobel prizes about Quantum Physics
- Vienna: Anton Zeilinger (2022) – zerothird's background



- Now shaping Today
 - Q-Computing
 - Q-Sensing
 - Q-Communication

QUANTUM RANDOMNESS — NATURE'S TRUE COIN TOSS



TRUE RANDOMNESS!

Unlike a dice roll, it's not just complexity —
there is *no* physical reason why it goes one way
or the other.

HEISENBERG'S UNCERTAINTY PRINCIPLE



- You can know a particle's **position or momentum** — but not both exactly.
- **Measurement** itself disturbs the system.



- In Star Trek, teleportation faced the same issue.
- The writers invented the **Heisenberg Compensator** to “solve” it.



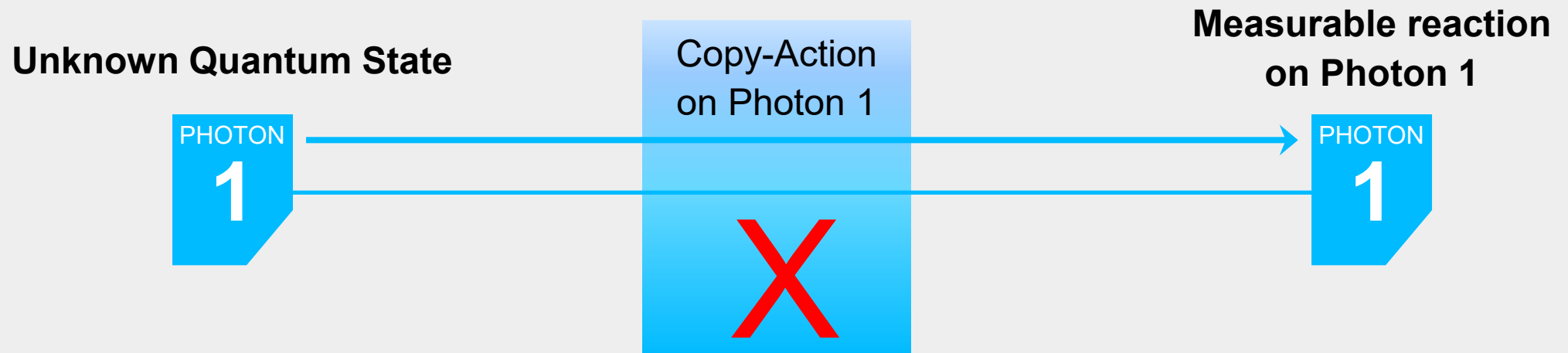
- Asked how the compensator works, Michael Okuda (Star Trek Designer) answered:
- “It works very well, thank you.”

NO-CLONING — YOU CAN'T COPY THE UNKNOWN



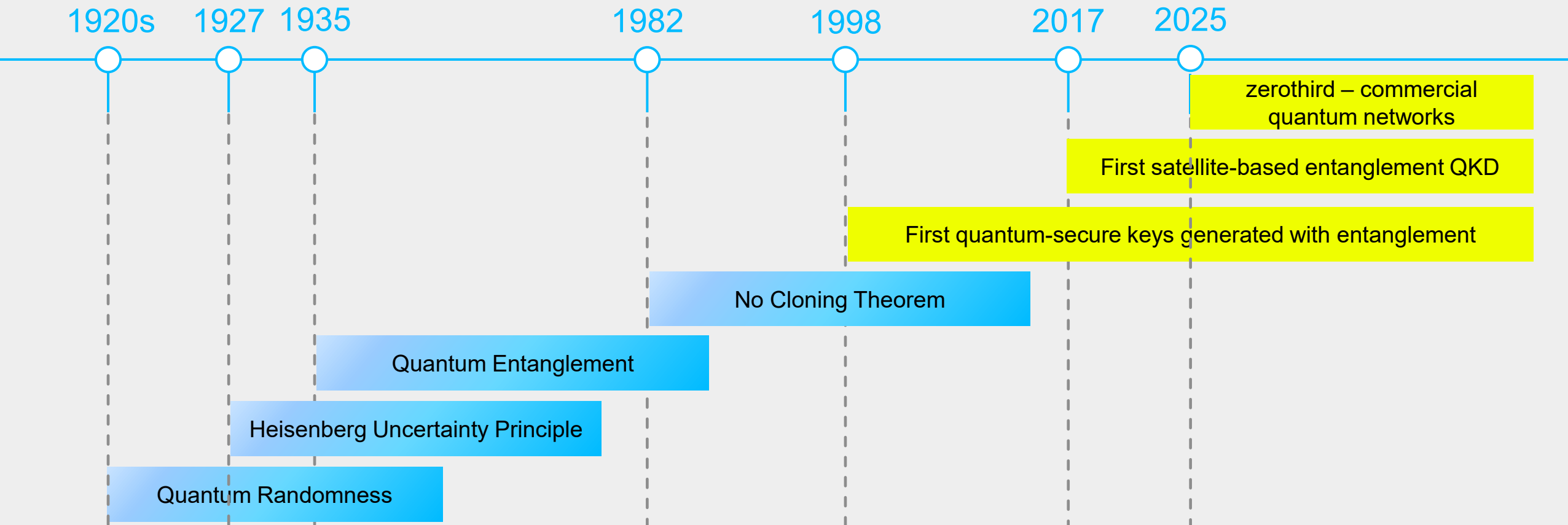
// *An unknown quantum state cannot be copied — any attempt changes or destroys it.*

Wootters & Zurek 1982



FOUR KEY QUANTUM PHENOMENA

From paradox to protection — physics becomes security.

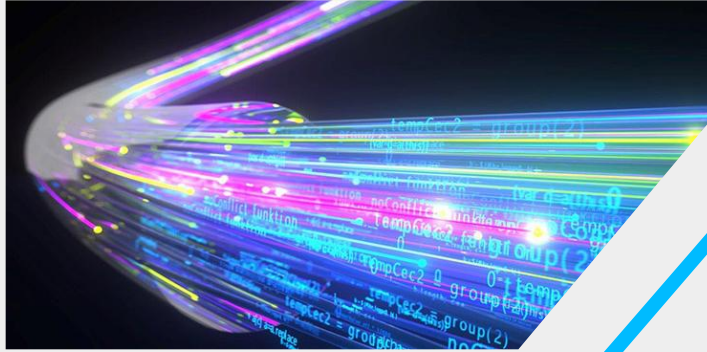


QUANTUM TECHNOLOGIES AT A GLANCE



QUANTUM COMPUTING

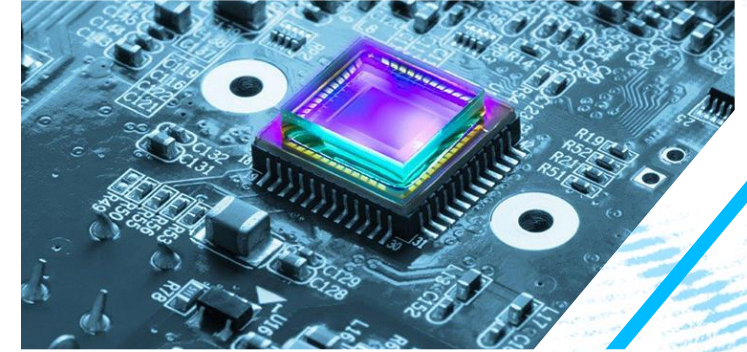
... uses quantum bits to perform calculations that are exponentially faster than classical computing. This includes machine learning, drug discovery, financial modelling and hacking of cryptographic systems using e.g. Shor's algorithm.



QUANTUM COMMUNICATION

... uses the principles of quantum mechanics to transmit information in a secure and crack-proof way. Major application is Quantum Key Distribution ("QKD")/cryptography.

ZERO/3



QUANTUM SENSING

... aims to measure physical quantities with higher precision and to surpass classical sensors' limits. Applications include imaging, navigation, and environmental monitoring.

/2

THE QUANTUM THREAT

THE HISTORIC CRYPTOSYSTEMS



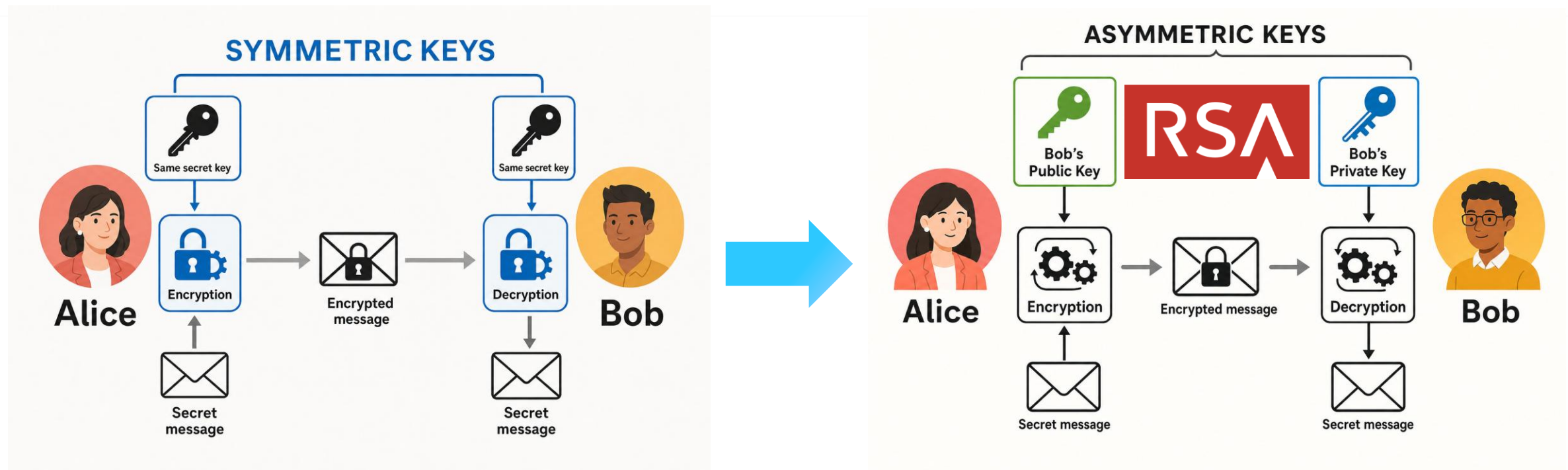
500 BC – Greek Cypher Wheel



1944 AC – “Navajo Code Talker”

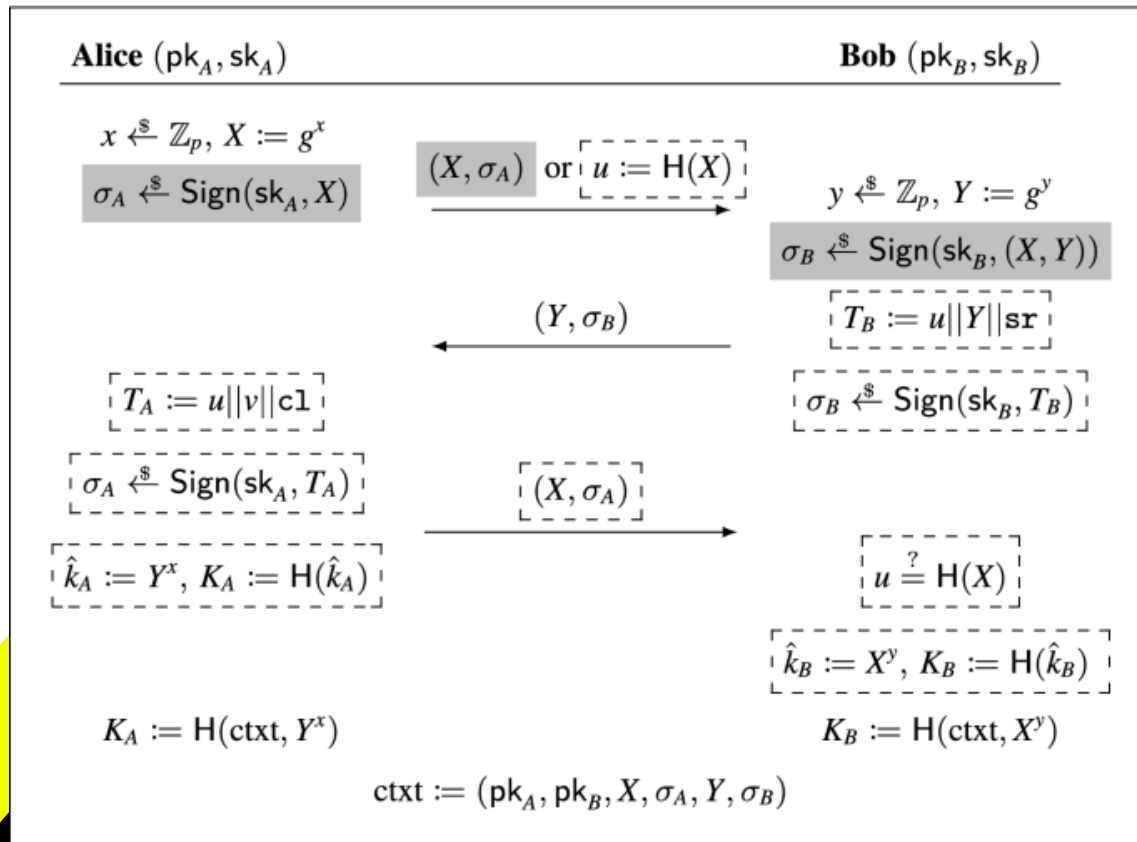
FROM SYMMETRIC TO ASYMMETRIC

How do you share that secret key over a network where attackers can always listen?



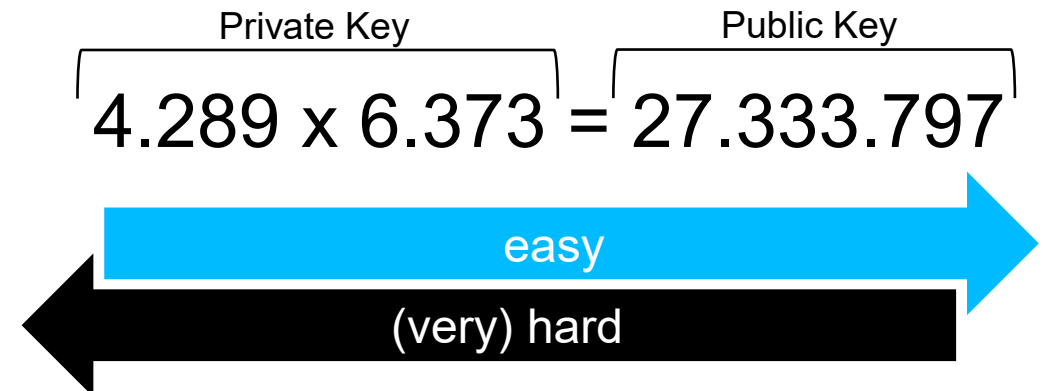
MATH BASED ASYMMETRIC ENCRYPTION

How do you share that secret key with someone over a **network** where **attackers can always listen**?



Asymmetric cryptography solved the key-distribution problem. Its security is **based on hard mathematical problems for class. computers**:

Easy to compute **in one direction**. Practically **impossible to reverse** without the private key

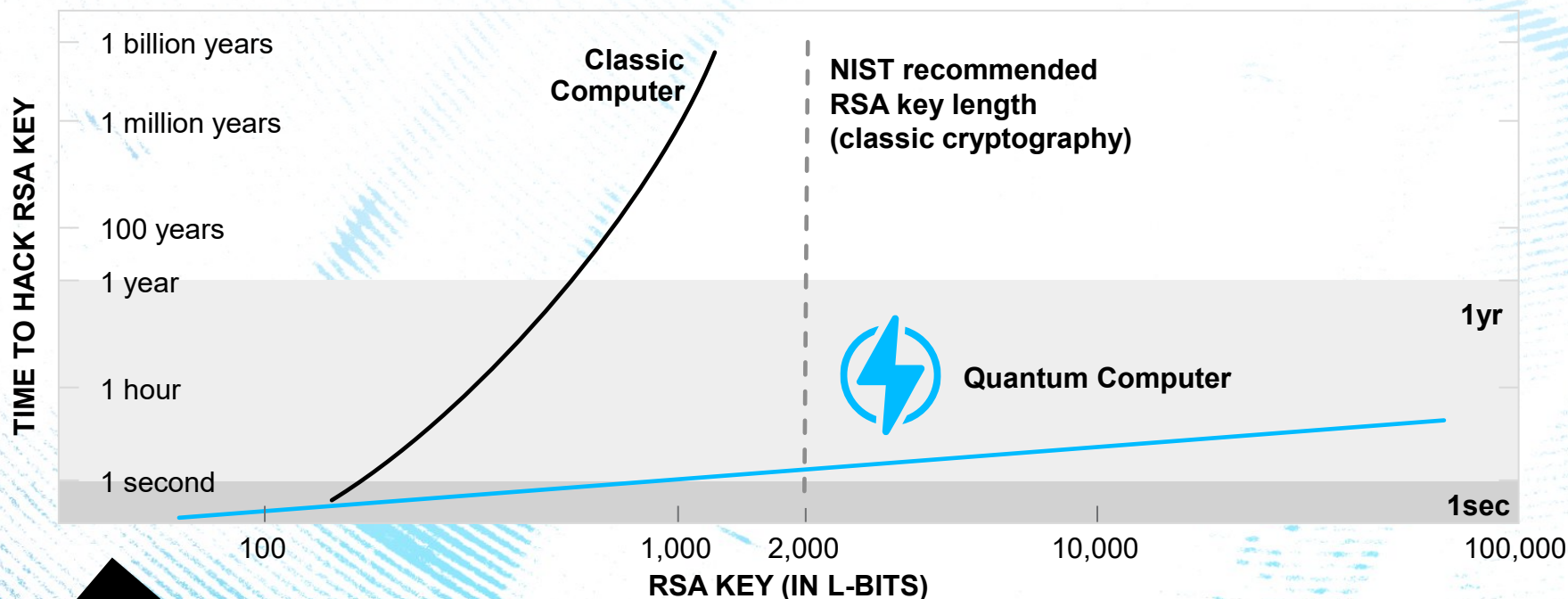


THE QUANTUM COMPUTER



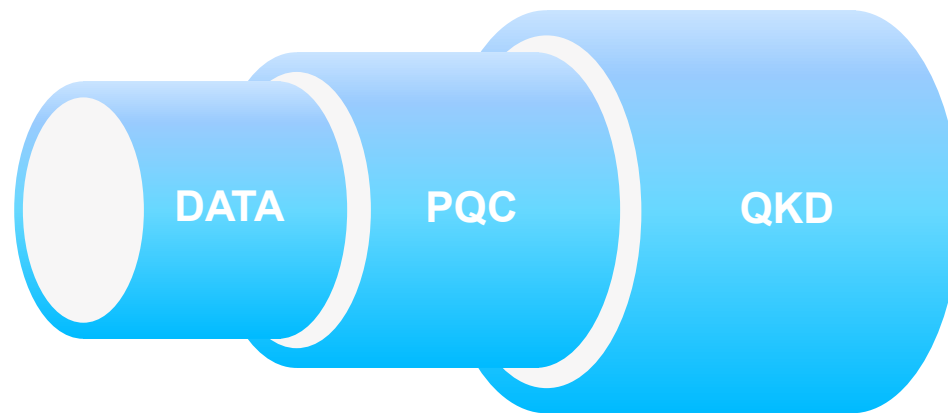
ENCRYPTION AS WE KNOW IT WILL FAIL WITHIN THE DECADE

Time for factoring classic computers vs. Quantum computers (simplified)



QKD + PQC: DEFENSE IN DEPTH

A Combination of QKD and PQC will be required to face the threat.



PQC

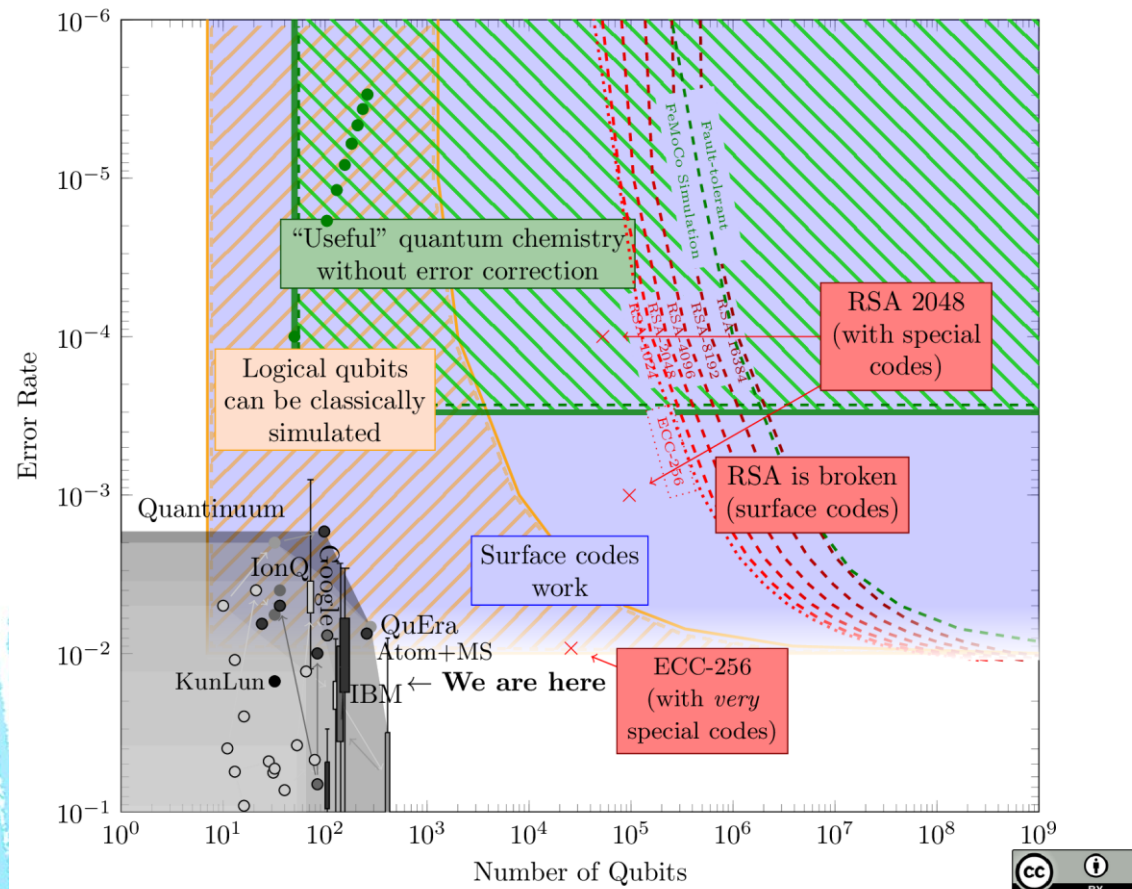
- Harder maths
- Assumption that even Quantum Computers can't break it

QKD

- Security based on the laws of physics
- Resistant even to computationally unlimited adversaries

THE CLOCK IS RUNNING OUT: QUANTUM COMPUTERS ARE CLOSING THE GAP TO RSA/ECC FAST

Landscape of Quantum Computing in 2026



2026

FEWER QUBITS NEEDED
TO BREAK RSA-2048

vs 2021 estimates:
from ~20m to ~100k
(QLDPC Codes)

2024

GOOGLE WILLOW: FIRST
LOGICAL QUBIT BELOW
ERROR THRESHOLD

Surface codes operational,
the theoretical barrier is
crossed

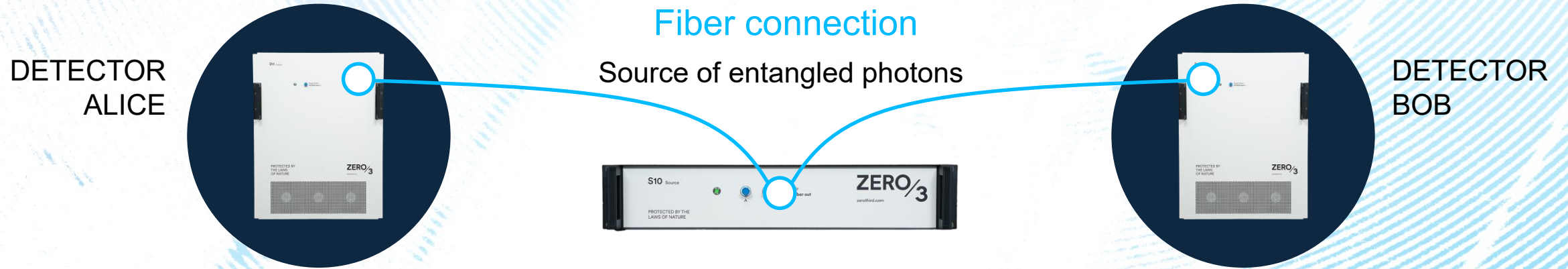
HARVEST NOW, DECRYPT LATER

Adversaries are already collecting encrypted traffic today – waiting for Q-Day to decrypt it. Data encrypted now with RSA or ECC is already at risk

/3

QUANTUM CRYPTOGRAPHY

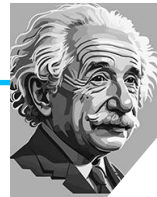
THE ENTANGLEMENT OF QUANTUM STATES



Quantum Entanglement State:
two photons behave identical at distance

PHOTON
1

Action on
Photon 1



“Spooky action at distance”

PHOTON
2

Measurable reaction
on Photon 2

PHOTON SOURCE AND DETECTOR DEVICES



eQKD ADVANTAGES

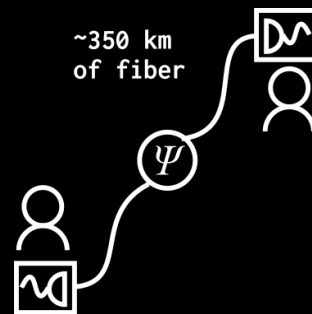
1

ENTANGLED



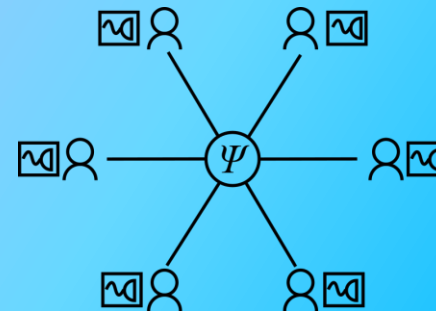
2

LONG DISTANCE



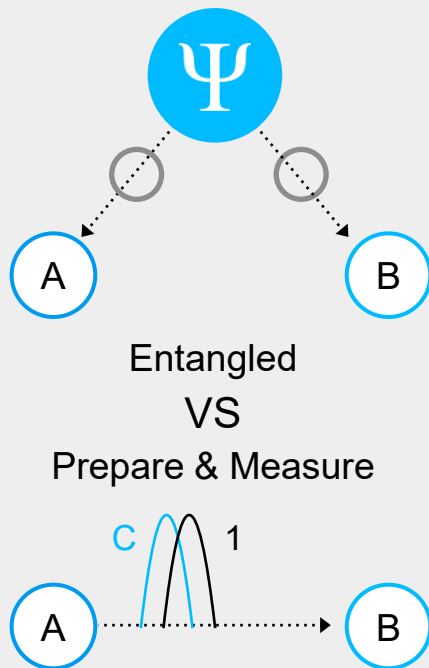
3

NETWORKS

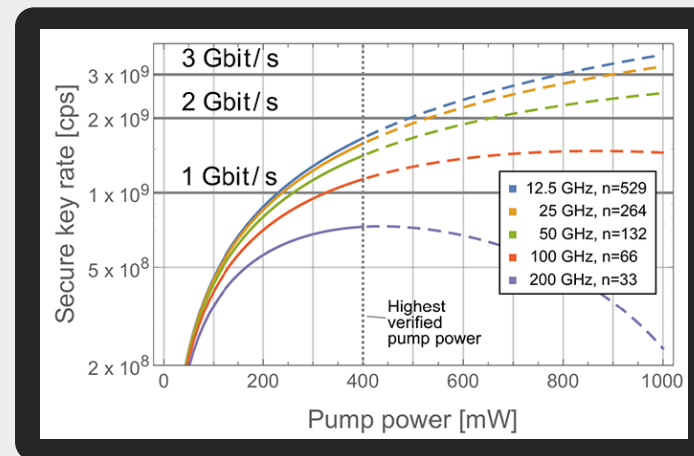


ADVANTAGES OF ENTANGLEMENT-BASED QKD (“eQKD”)

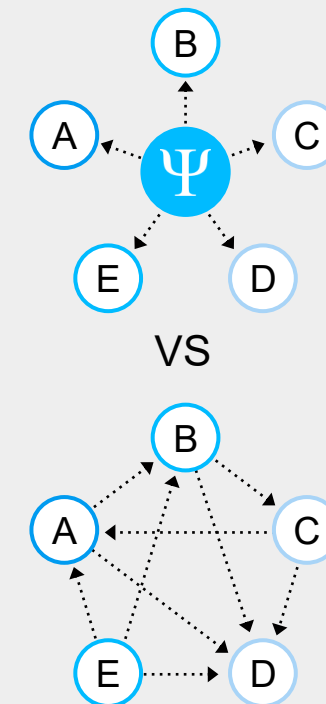
- 1** Maximum security due to “Monogamy of Entanglement” intrinsically preventing any leak of information



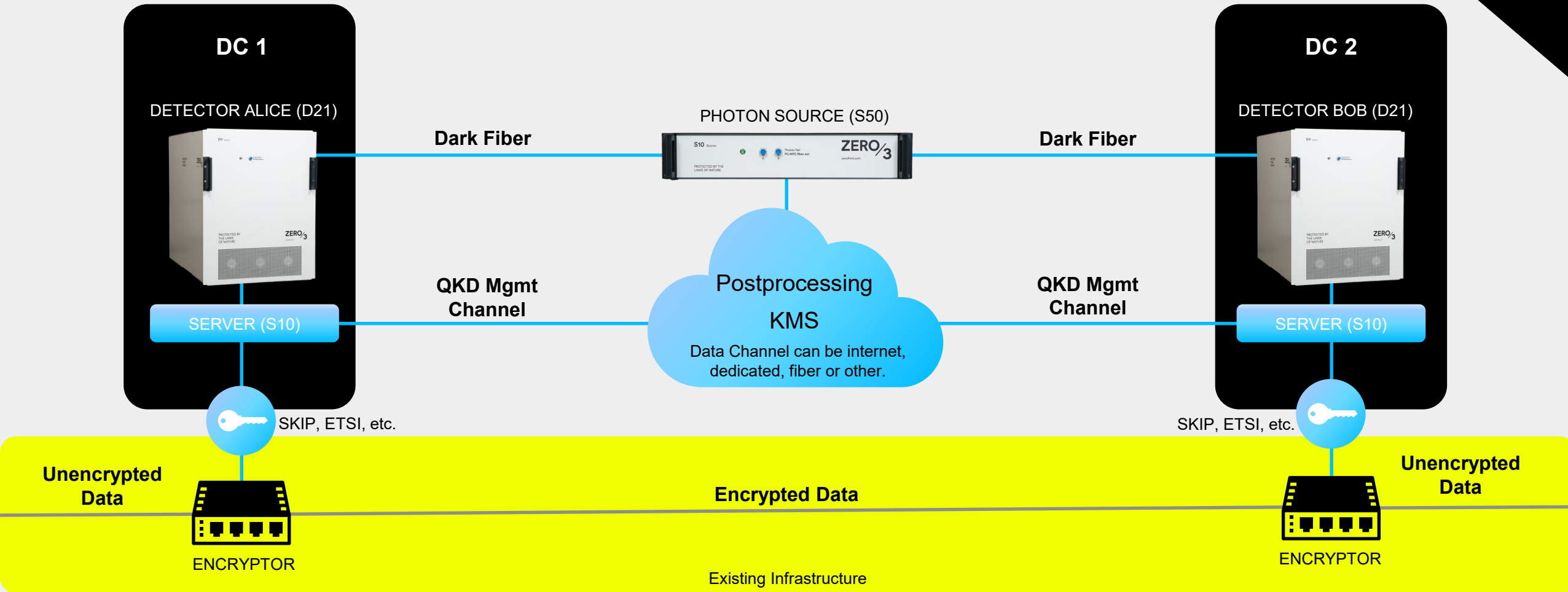
- 2** Very high key rates and long distances >350km only limited by detector jitter due to efficiency of eQKD source



- 3** Fully connected networks with all WDM complexity in one location and only one detection system per communication partner



POINT TO POINT SETUP



/4

SECURING A LIVE SIGNAL

ORF & AUSTRIAN PARLIAMENT

Austrian Parliament & ORF: world's first quantum-secured live broadcast (May 2026). Protects integrity of democratic content against manipulation & deepfakes

Source: [Quantenkryptografie: Erstes absolut sicheres TV-Signal aus Parlament - science.ORF.at](https://www.sciencemag.org/news/2025/05/austrian-parliament-secure-live-broadcast)



REPUBLIK ÖSTERREICH
Parlament

Facts

- 10km Fiber between Parliament and ORF
- 3-month pilot to establish framework for critical infrastructure deployment
- Usecase is the encryption of a live broadcast signal (world premiere)
- S10, D11, C10

Partners

- ORF
- Austrian Parliament (Parlamentsdirektion)
- Big Blue Marble



ZERO/3
ONE SENDER,
ONE RECEIVER,
ZERO THIRD