



Mit Sicherheit ein Quantensprung

Verschlüsselung mit verschränkten Photonen

Dr. Kevin Füchsel

Quantum Optics Jena GmbH

Hall 7 – Booth 7-242

Everything Starts with WHY?



QUANTUM OPTICS
JENA

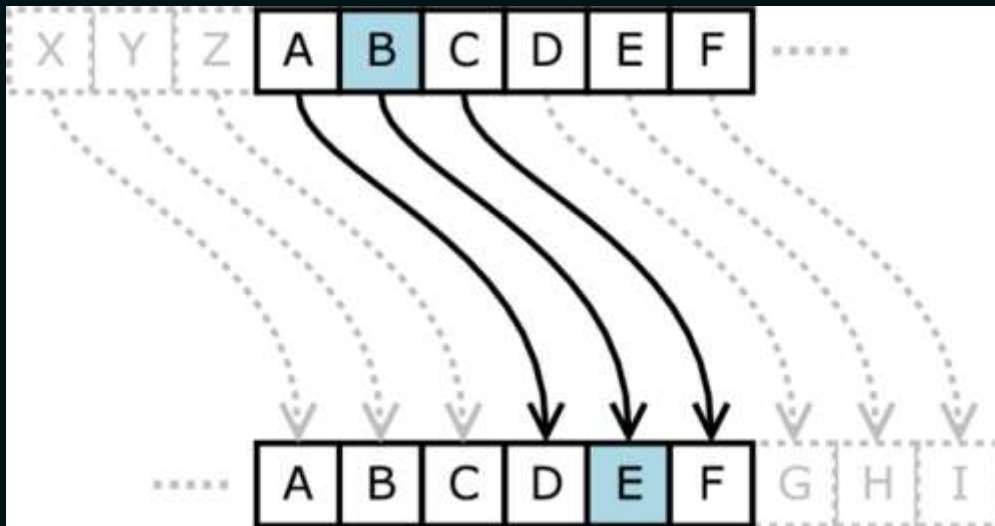


<https://www.flickr.com/photos/alfredofoto/15381212999>

Everything Starts with WHY?

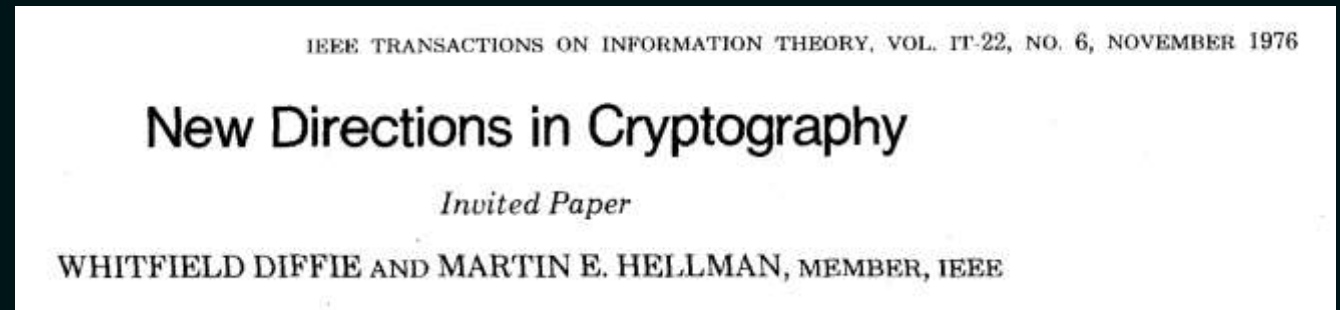


Caesar's cipher



https://en.wikipedia.org/wiki/File:Caesar_substitution_cipher.png

Public-key cryptography



<https://ee.stanford.edu/~hellman/publications/24.pdf>

Algorithms / Mathematics

Key Exchange
Mechanism

From Theory to Application



The Nobel Prize in Physics 2022



Ill. Niklas Elmehed © Nobel Prize Outreach

Alain Aspect

Prize share: 1/3



Ill. Niklas Elmehed © Nobel Prize Outreach

John F. Clauser

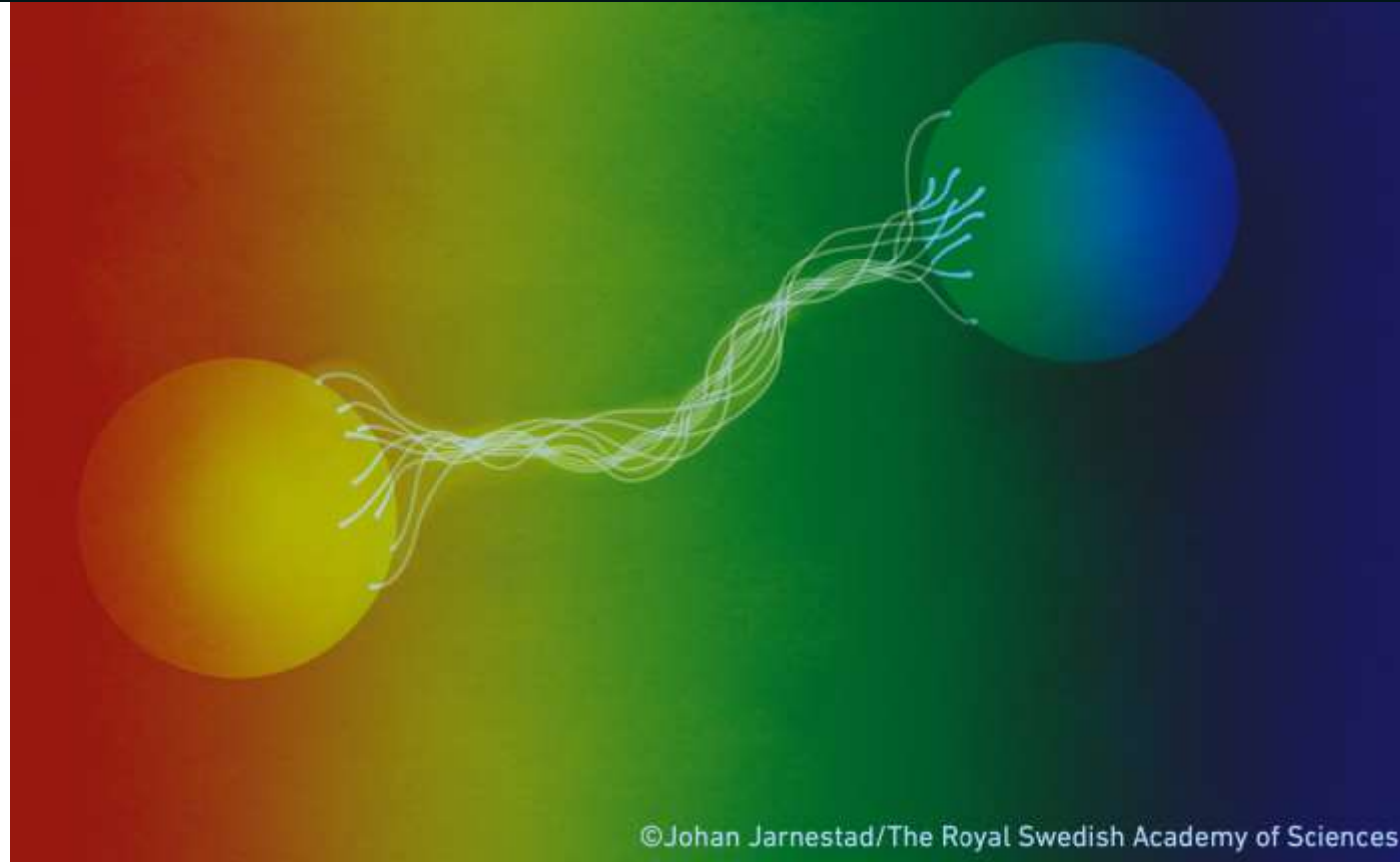
Prize share: 1/3



Ill. Niklas Elmehed © Nobel Prize Outreach

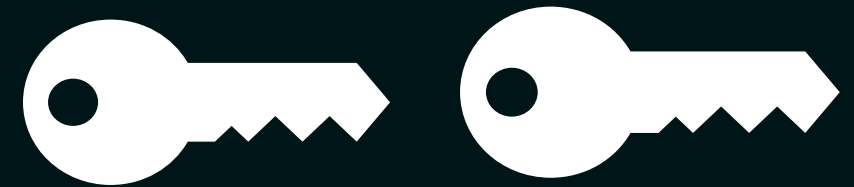
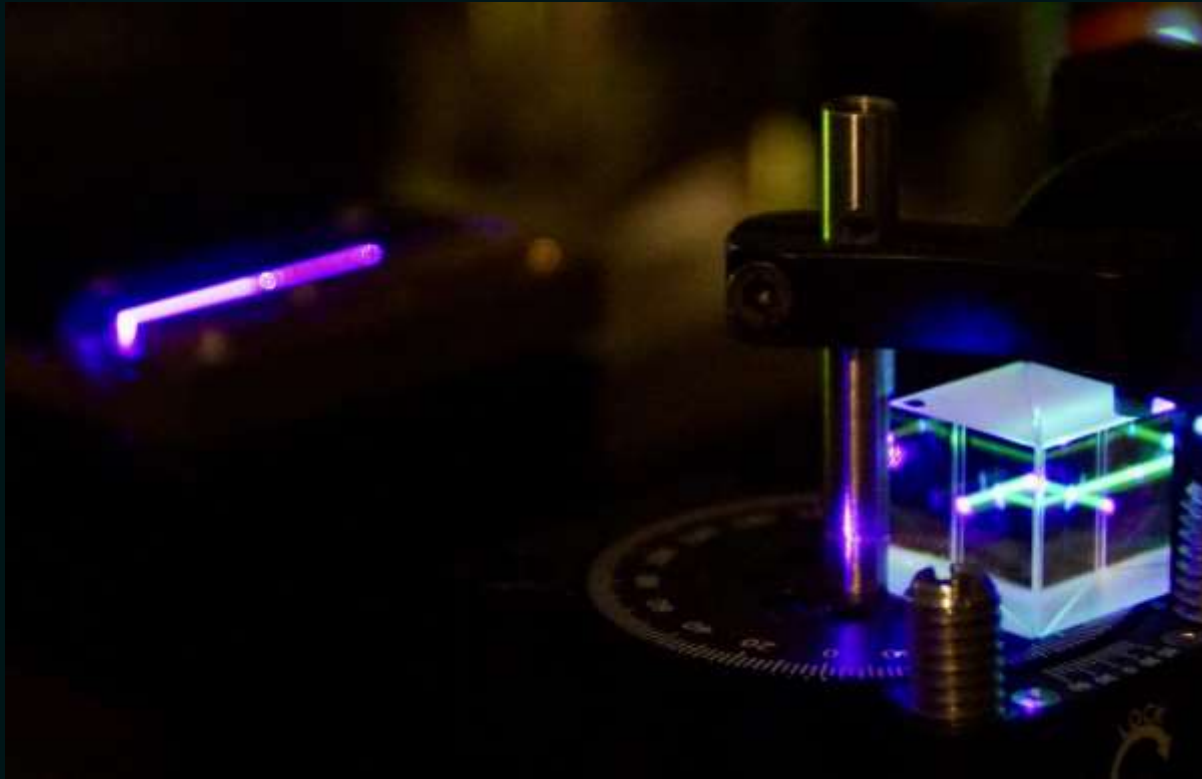
Anton Zeilinger

Prize share: 1/3



©Johan Jarnestad/The Royal Swedish Academy of Sciences

<https://www.nobelprize.org/prizes/physics/2022/summary/>



Symmetric Keys

no algorithms

Quantum-Safe

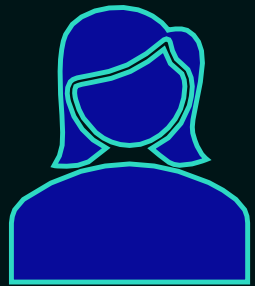
Our Solution



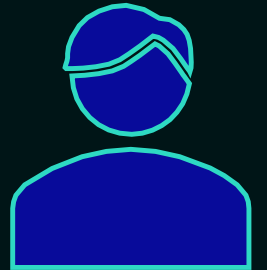
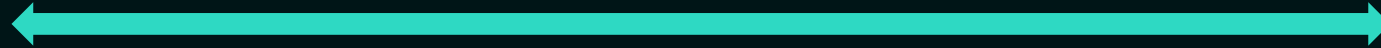
QKD-Systems with Entangled Photons



QUANTUM OPTICS
JENA



Communication Layer



Q-Layer

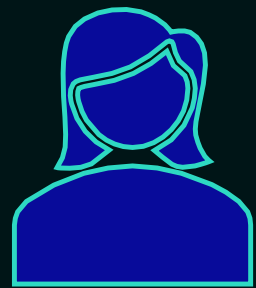


EPS
QKD

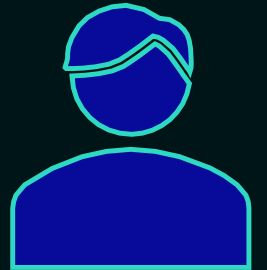
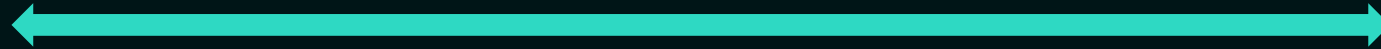
QKD-Systems with Entangled Photons



QUANTUM OPTICS
JENA



Communication Layer



Q-Layer

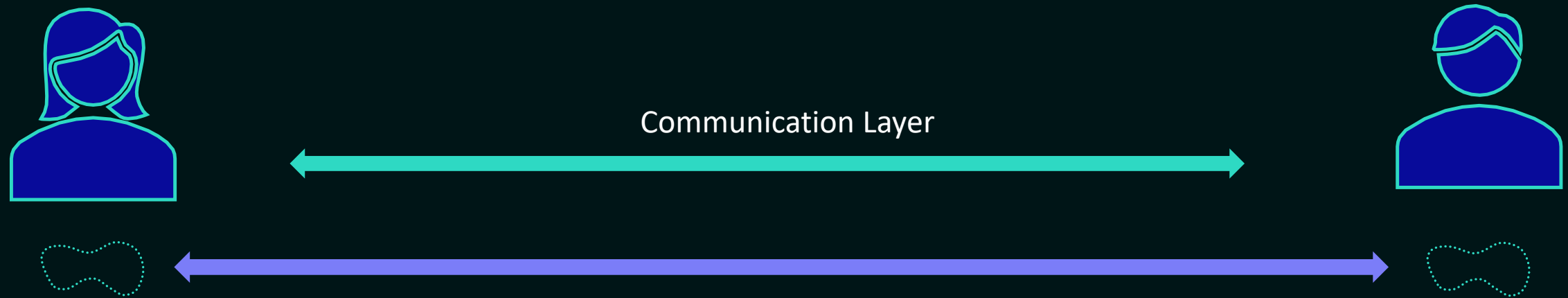


EPS
QKD

QKD-Systems with Entangled Photons



QUANTUM OPTICS
JENA

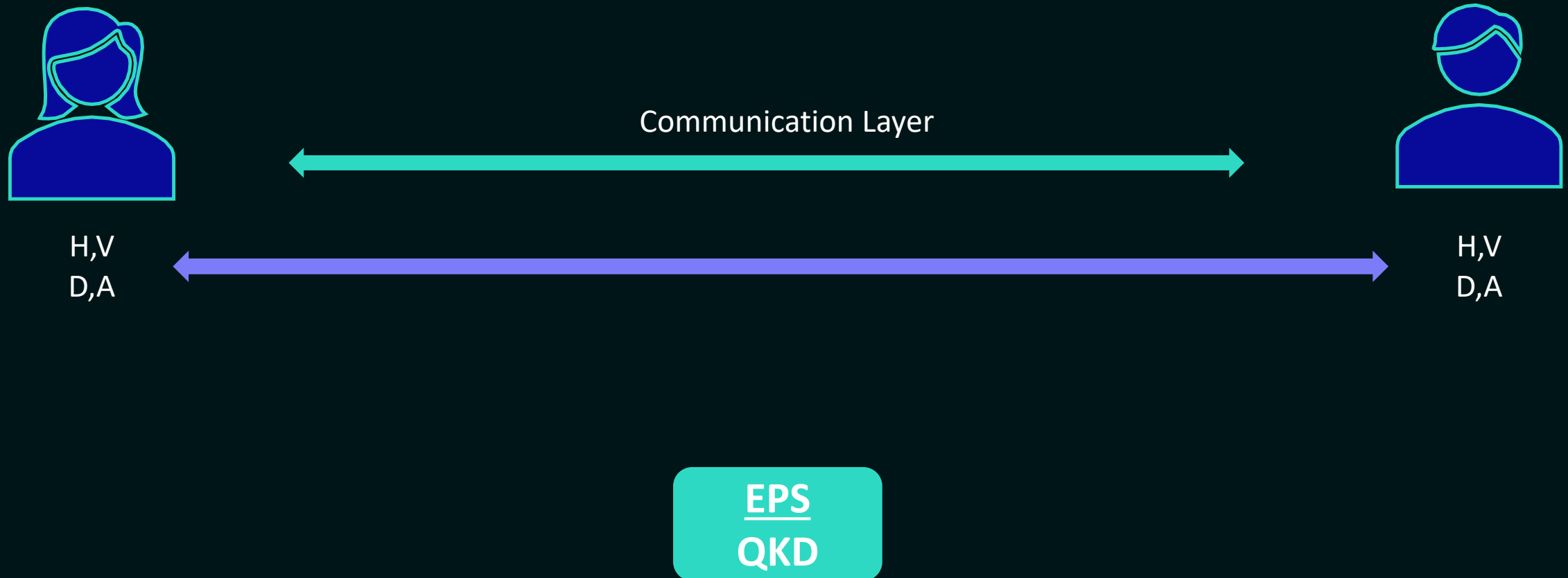


EPS
QKD

QKD-Systems with Entangled Photons



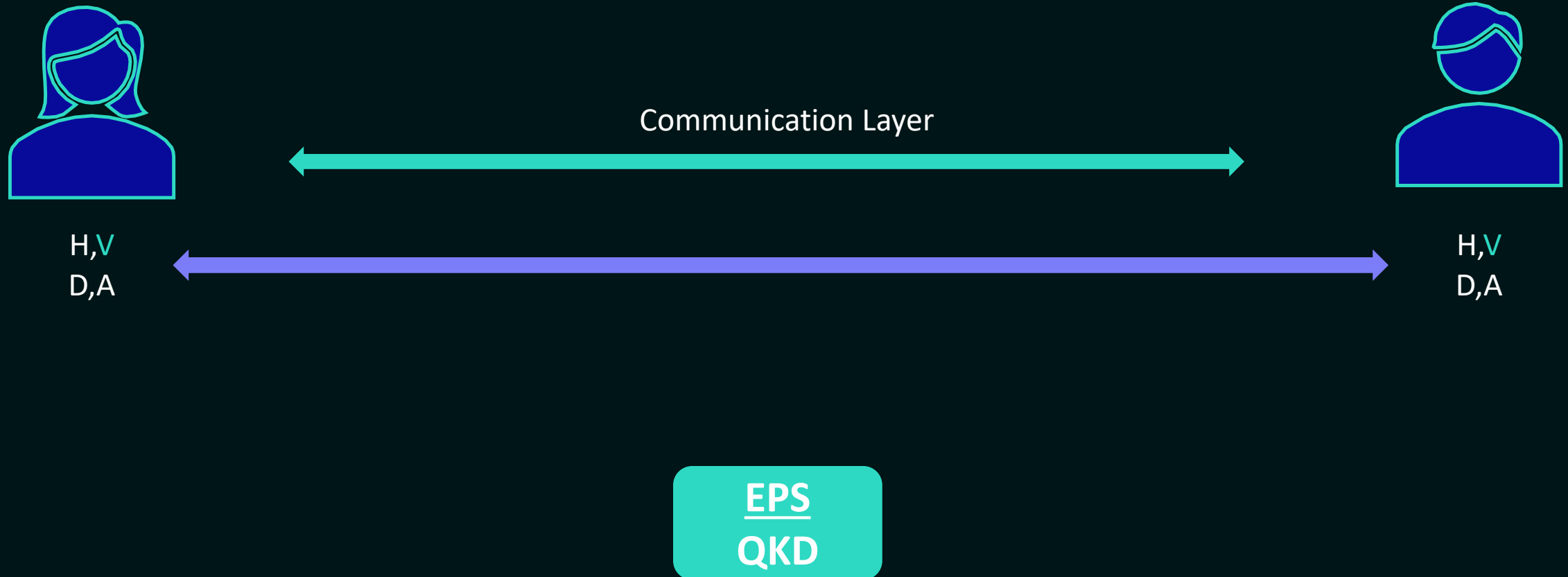
QUANTUM OPTICS
JENA



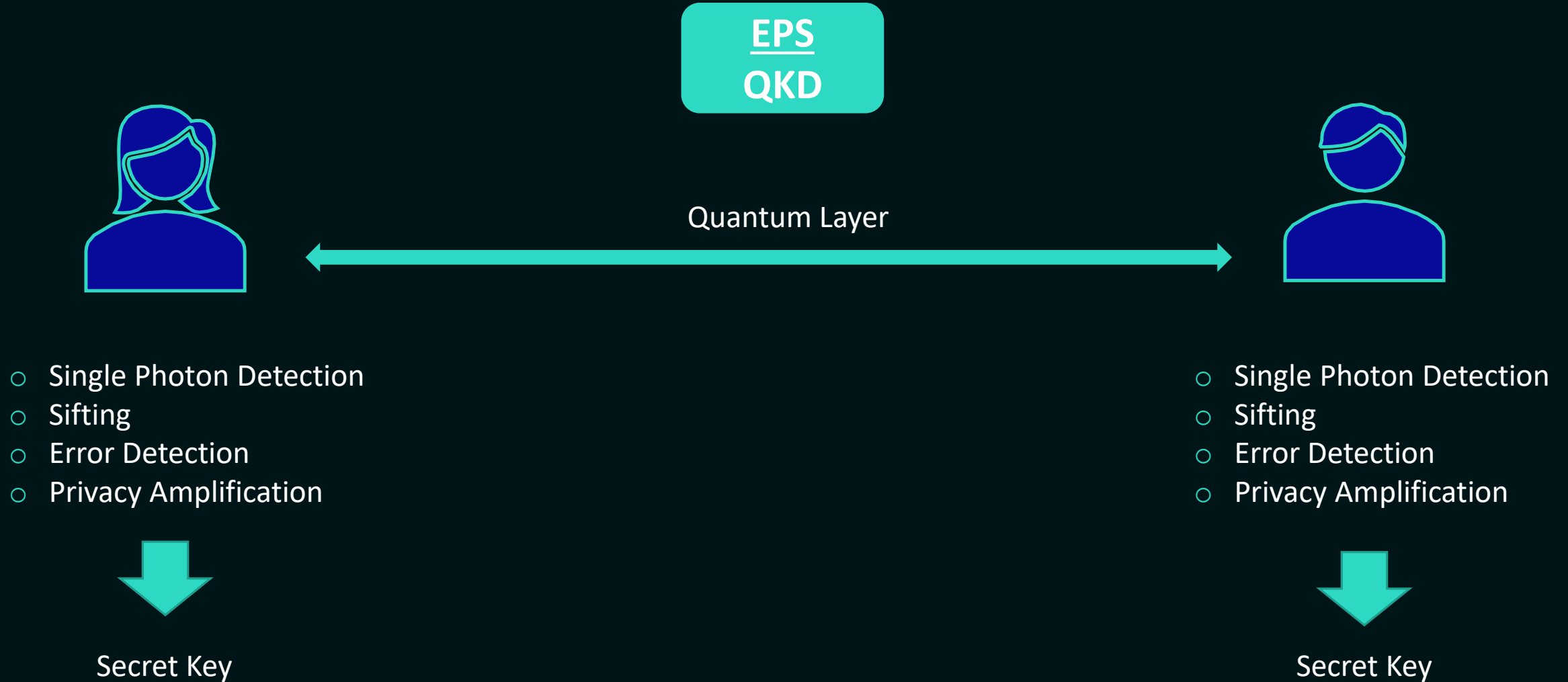
QKD-Systems with Entangled Photons



QUANTUM OPTICS
JENA



QKD-Systems with Entangled Photons



QKD-Systems with Entangled Photons

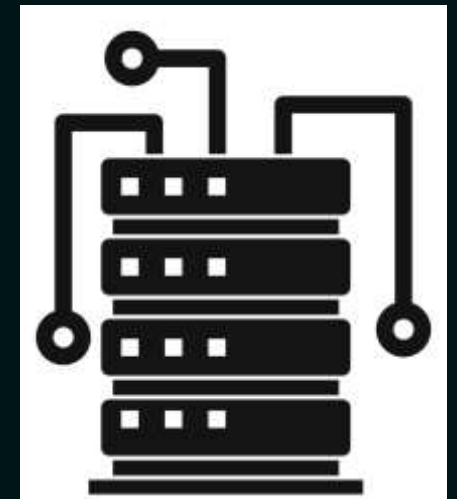
Customized photon
sources

Quantum State
Analyzer

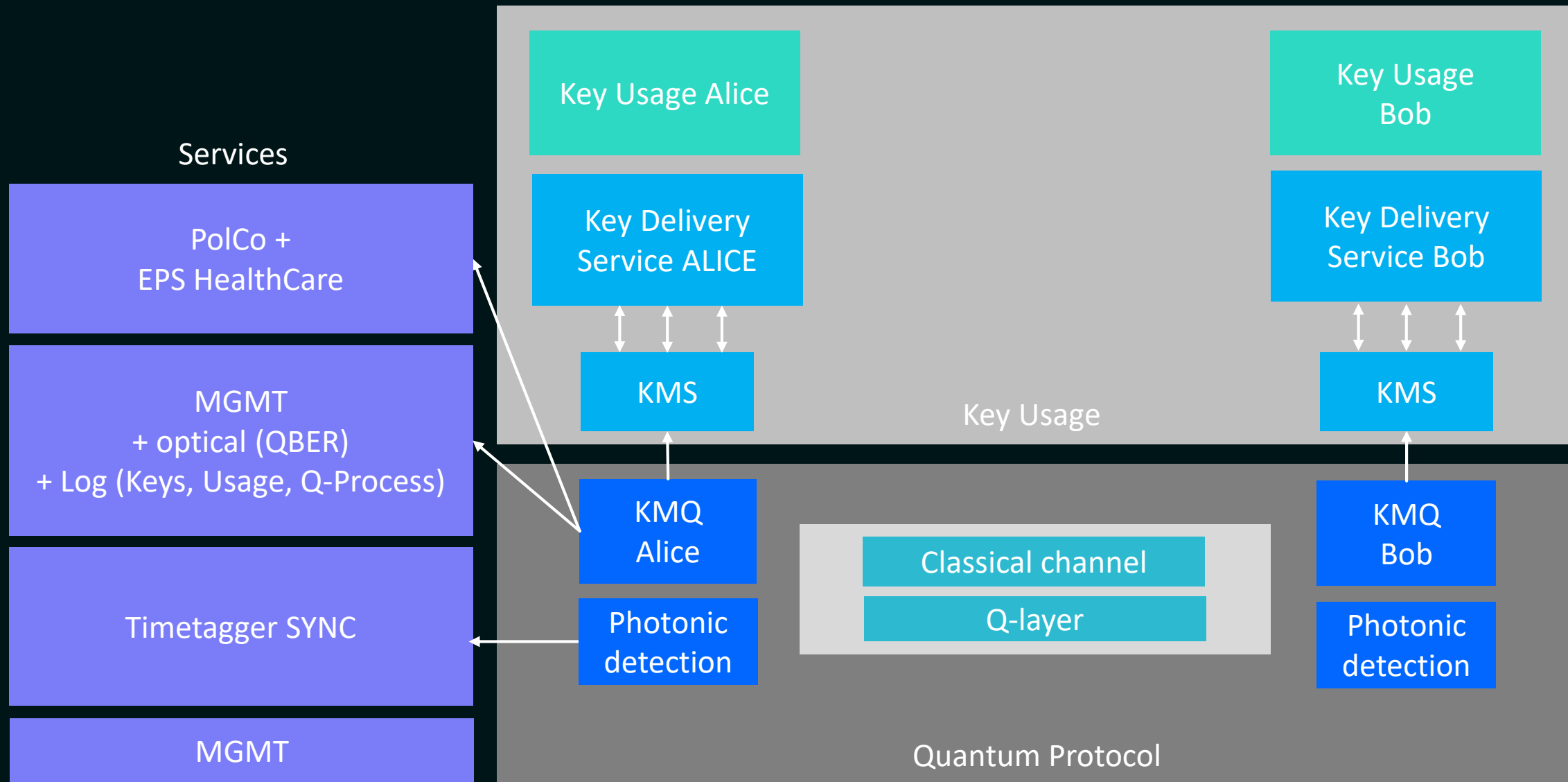
Key Management
System



Crypto Box /
Network



System Architecture





QUANTUM OPTICS
JENA

EVALUATION INTERFACE

Version 1.1a

Overview

Singles &
Coincidences

Protocol

Help & Support

pause

developed by

QUANTUM OPTICS
JENA

Classical Channel



Quantum Channel

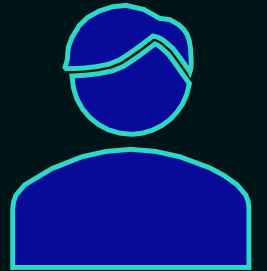
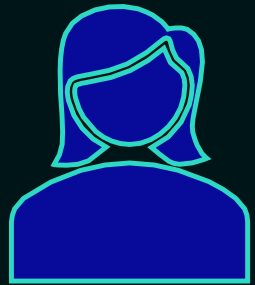


$$l \leq nq - \underbrace{n_x h_2(\delta_x) + n_z h_2(\delta_z)}_{\text{QBER}} - leak_{EC} - \underbrace{\log \frac{2}{\epsilon_{cor}} + 2 \log \frac{1}{2\epsilon_{sec}}}_{\text{Verify correctness \& security}}$$

Secure Key Length $\leq$ Number of Photons Uncertainty $-$ QBER $-$ Public Information $-$ Verify correctness & security



$$\text{QBER} \leq 11\%$$



Quantum Layer

25 dB loss = 50 km fiber + 13 dB

PAM

EPS
Source

PAM

Demonstration



QBER [%]

QBER

teal



15.0

secure Key Rate [bps]

secure Key Rate

green



1

9

6

3

180

S

90.0

0

Sat 27.08.22 01:00

Sat 27.08.22 09:00

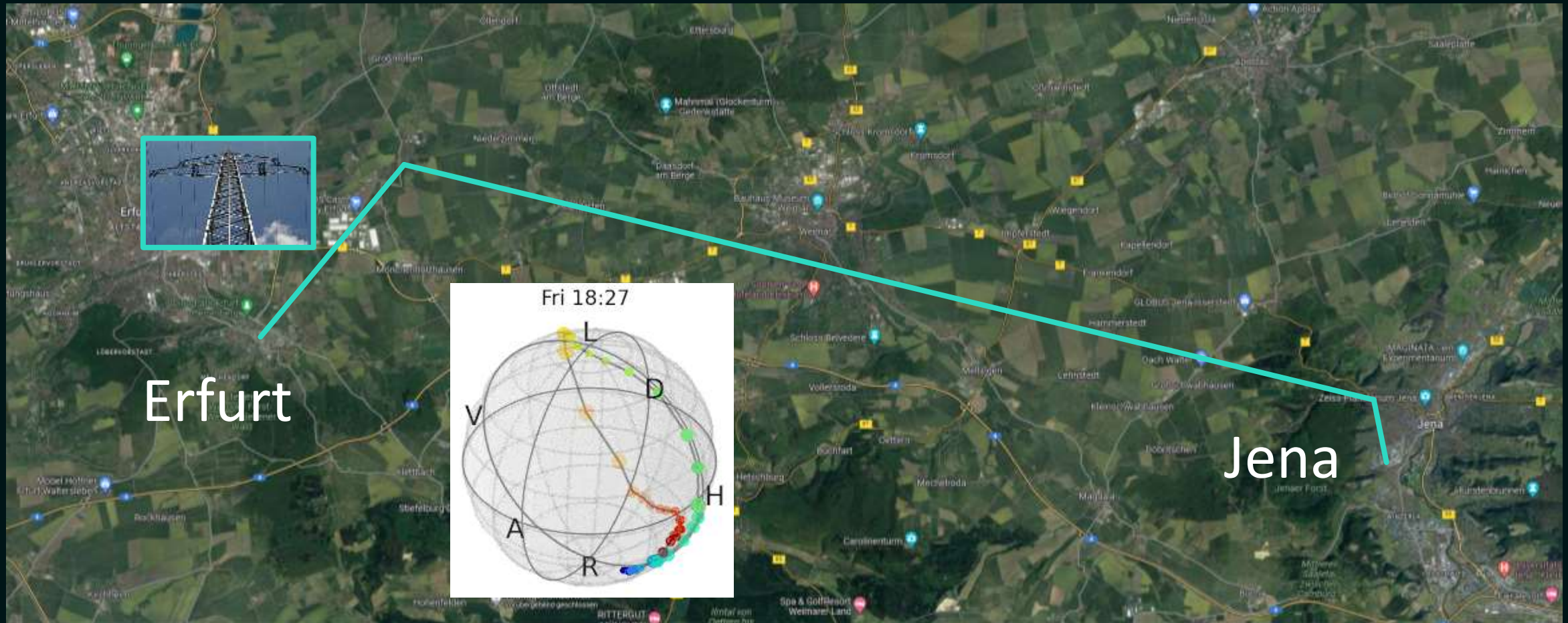
Sat 27.08.22 17:00

Sun 28.08.22 01:00

Sun 28.08.22 09:00

Sun 28.08.22 17:00

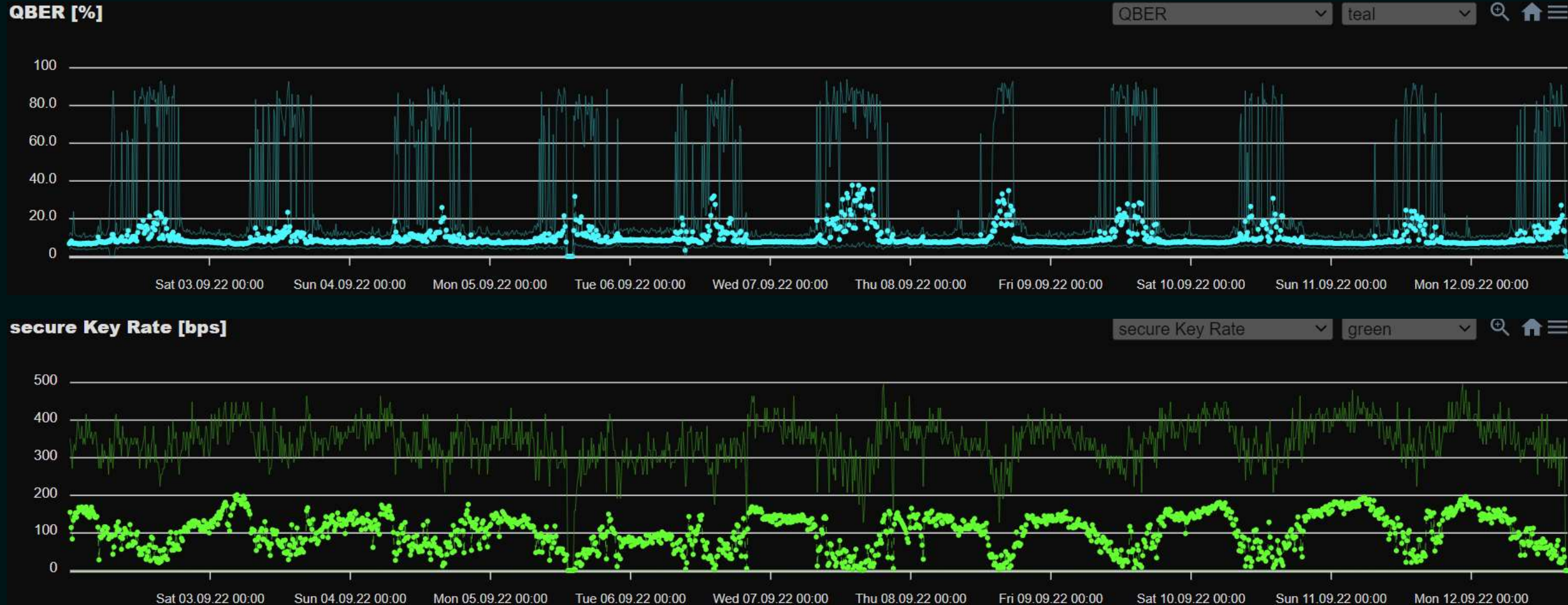
75 km, optical loss 20 dB @ 1550 nm



(c) Fraunhofer IOF Jena: Measurement of polarization fluctuations of Jena-Erfurt Link

Demonstration

30.000 keys (256 bit) per day, 20 keys per minute



Get in touch with us



QUANTUM OPTICS
JENA



ATHENE
National Research Center
for Applied Cybersecurity



www.qo-jena.com



k.fuechsel@qo-jena.com