QUNET: MOBILE FREE-SPACE QUANTUM COMMUNICATION SYSTEM

C. Spiess[1], S. Töpfer[1], S. Sharma[1], A. Krzic[1], T. Grafenauer[2], R. Lieger[2], B. Ömer[2], S. Petscharnig[2], M. Warum[2], C. Pacher[2], G. Sauer[1], M. Goy[1], R. Berlich[1], T. Kopf[1], T. Peschel[1], C. Damm[1], A. Brady[1], D. Rieländer[1], F. Steinlechner[1]

[1]Fraunhofer Institute for Applied Optics and Precision Engineering, Jena, Germany

[2]AIT Austrian Institute of Technology GmbH, Vienna, Austria

OVERVIEW OF INFRASTRUCTURE

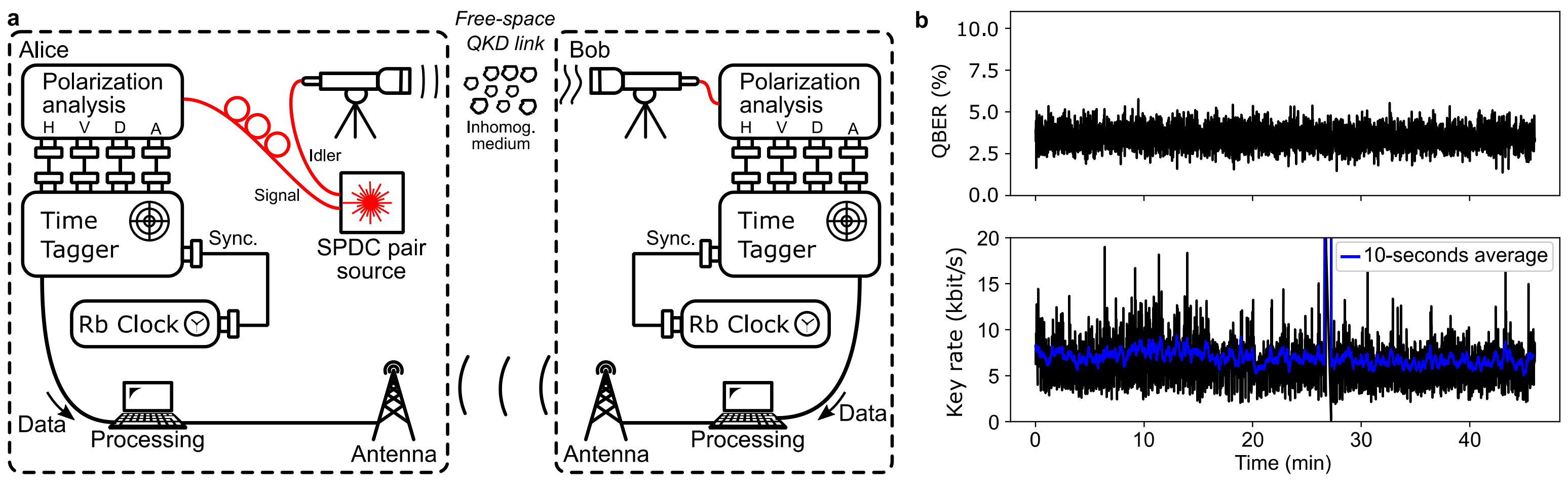


Fig. 1. Quantum key distribution setup **a**, including a spontanous parametric downconversion source, and telescopes with active tip-tilt beam stabilization. **b** Achieved key rates of 7.1 kbit/s on average and quantum bit error rates (QBER) during 50 min of key exchange on a 300-m free-space link.

Quantum Key Distribution (QKD) allows users to generate encryption keys, whose secrecy and randomness is founded in the laws of physics [1]. Here we report on the realization of a portable quantum communication platform and its validation in an intra-campus QKD session (Fig. 1 and 2). We outline the entire quantum-photonics process chain for efficient free-space quantum communication. Starting with the design and fabrication of an entangled photon source and mobile telescopes in-house, to finally integrating adapted QKD postprocessing software solutions from the Austrian Institute of Technology (AIT) to generate the information-theoretically secure key, which is used to encrypt a video call.

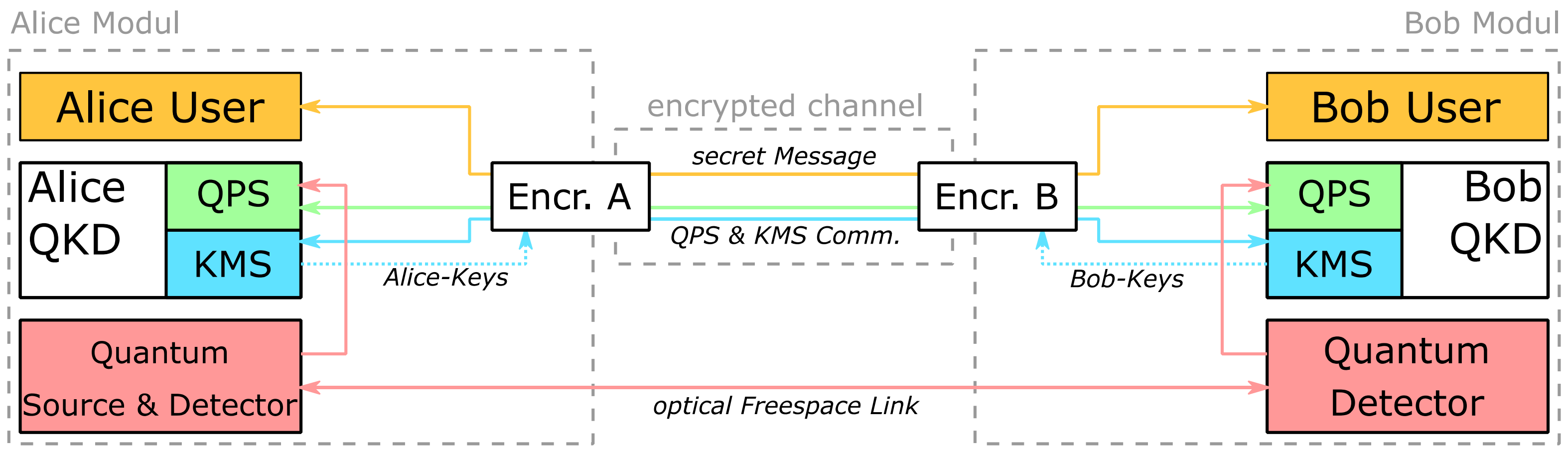


Fig. 2. The two QKD-modules are connected by an optical freespace link for transmission of the quantum signal, as well as through an encrypted classical channel for Quantum-Postprocessing (QPS), Key-Management (KMS) and user communication. The QPS retrieves quantum events and generates the secure key, which is stored in the KMS. The KMS feeds the key to the encryptor (Encr. A/B), which then uses it to encrypt the classical channel.

ENTANGLED PHOTON SOURCE

- Based on type-2 spontaneous parametric down conversion (SPDC).
- Polarization encoding engineered through Sagnac interferometer design [2], Fig. 3.
- Entangled photons, signal and idler created at 810 nm.
- One photon sent over free-space link to Bob and the other one sent to Alice through fiber.
- Field-deployable, 19 inch rack compatible (Fig. 4).

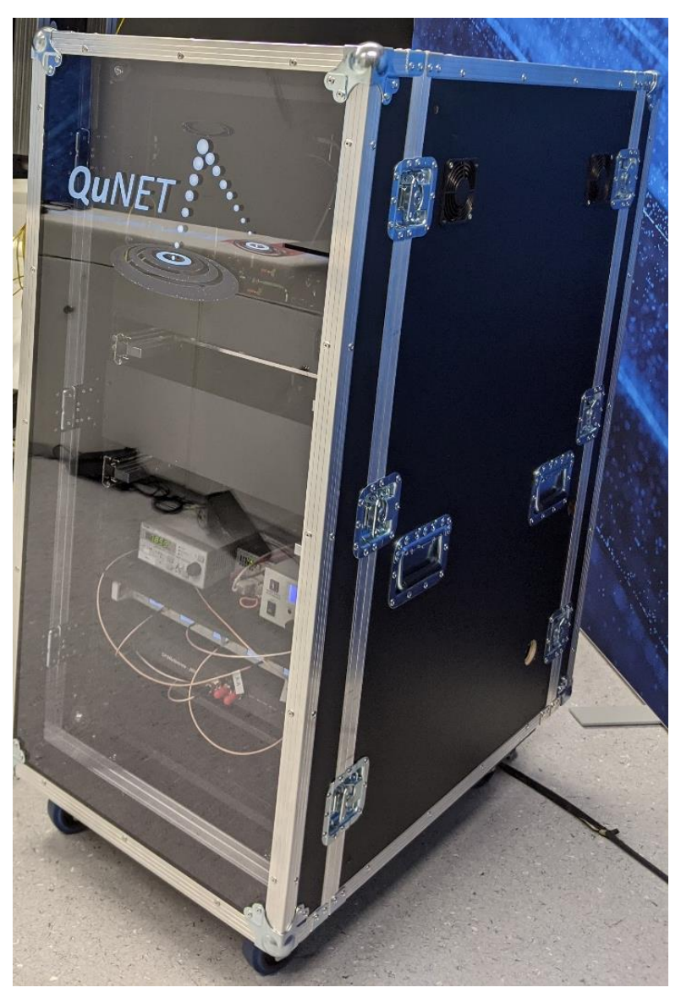
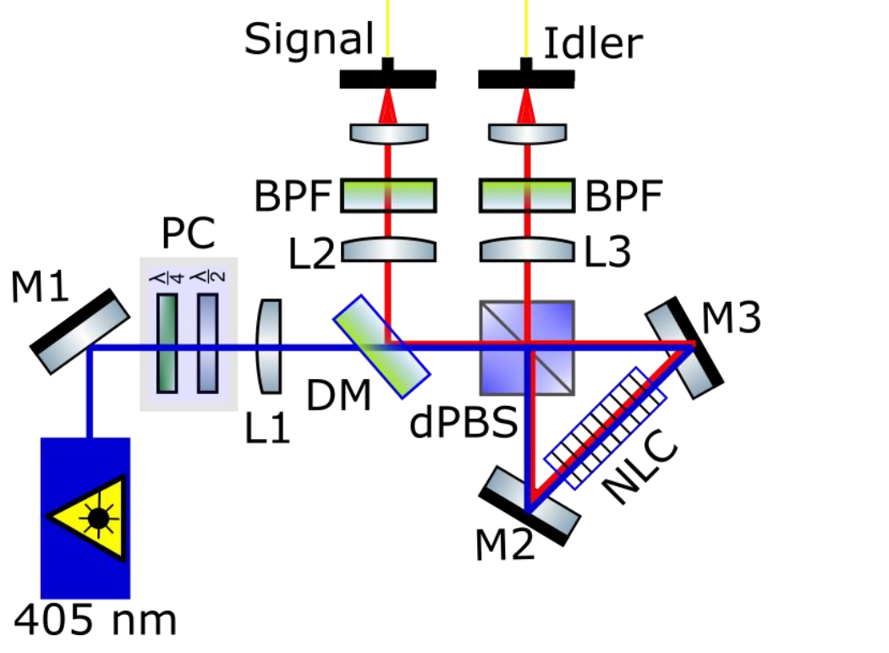


Fig. 4. Rack-integrated EPS with time-tagging and synchronization electronics



Property	Value
CWL_{SPDC}	810 nm
Brightness	1 Million pairs/s
Visibilty H/V	99.5 %
Visibility A/D	97.4 %

Fig. 3. EPS optical design. Non-linear crystal (NLC) is pumped bidirectionally with 405 nm in a sagnac configuration, generating entangled photon pairs at dual-wavelength polarization beam splitter (dPBS). The SPDC photons are then separated using a dichroic mirror (DM). SPDC photons are then collected in single mode fibers.

MOBILE OPTICAL TERMINALS

We developed two highly versatile mobile terminals (Fig. 5) for ad-hoc free-space quantum communication link, with the following features (Fig. 6):

- Off-axis mirror-based transmitter and receiver telescopes with 200 mm primary apertures and no central obscuration
- Communication channels at 810 nm and 1550 nm
- Forward (1064 nm) and backward (980 nm) beacon channels
- Visible (VIS) camera for rough alignment of the terminals
- Fine alignment and active beam stabilization with beacon lasers and fast steering mirrors (FSM)

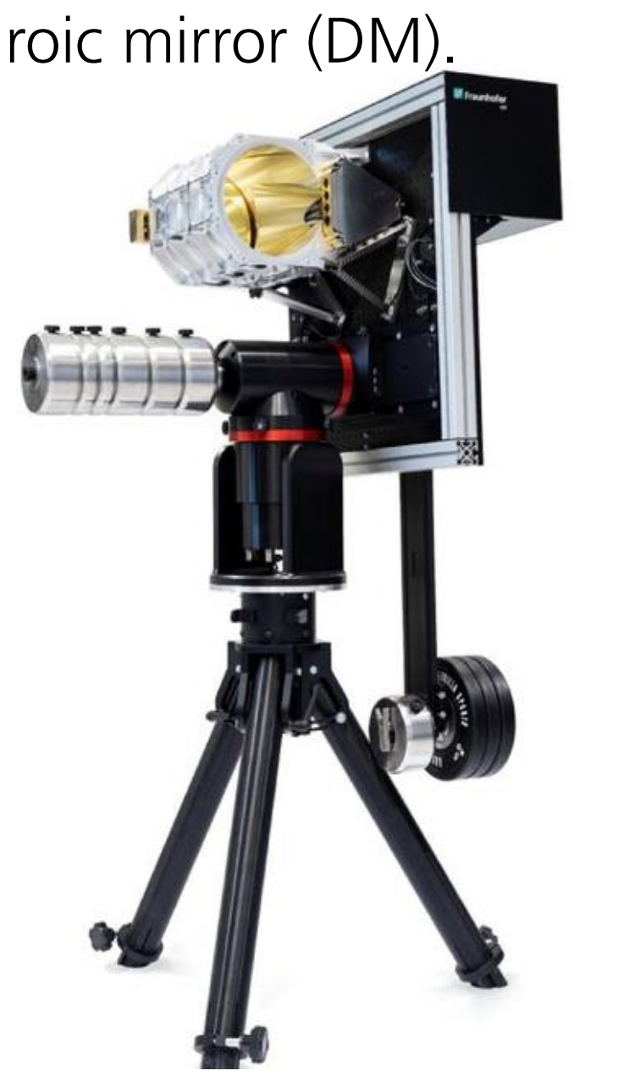


Fig. 5. Mobile terminal

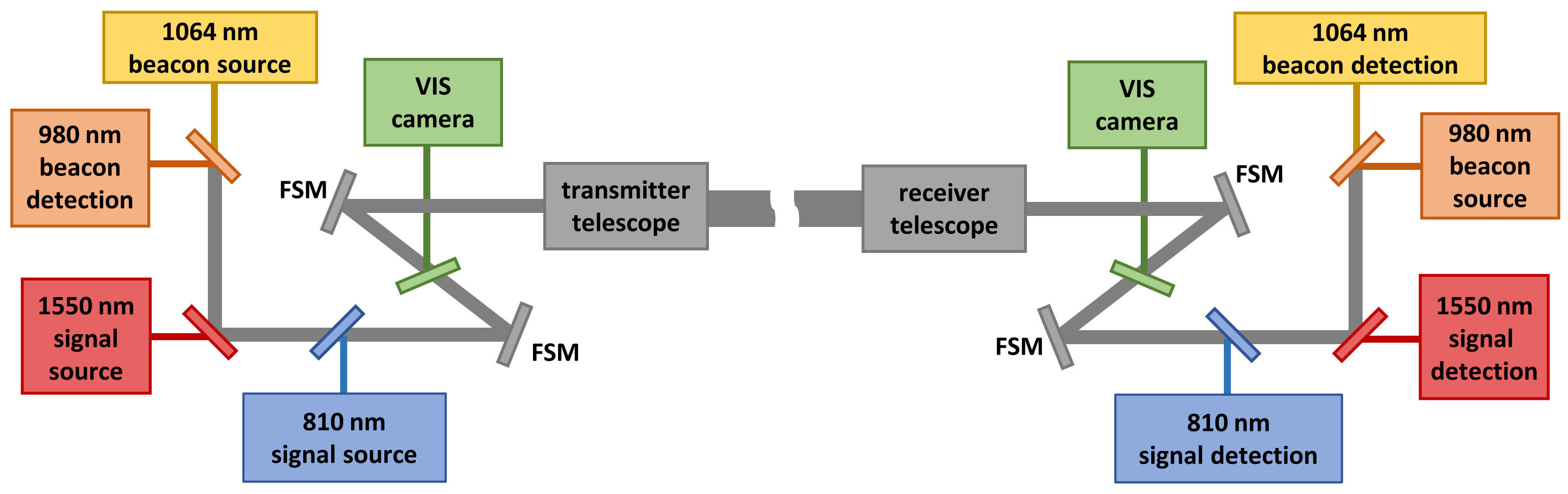


Fig. 6. Optical link architecture.

SYNCHRONIZATION WITH CORRELATED PHOTONS

Quantum communication schemes usually incorporate dedicated synchronization hardware, like GPS signal, Rubidium clocks or pulsed laser [3]. Here we show reliable operation of a potential quantum communication session, where entangled photon pairs serve as mediator to synchronize receiver and sender with synchronization jitters root-mean squares of smaller than 50 ps (Fig. 7). The computer-aided post-processing can be easily and immediately applied to wide range of quantum communication scenarios and may pave the way for secure time transfer.

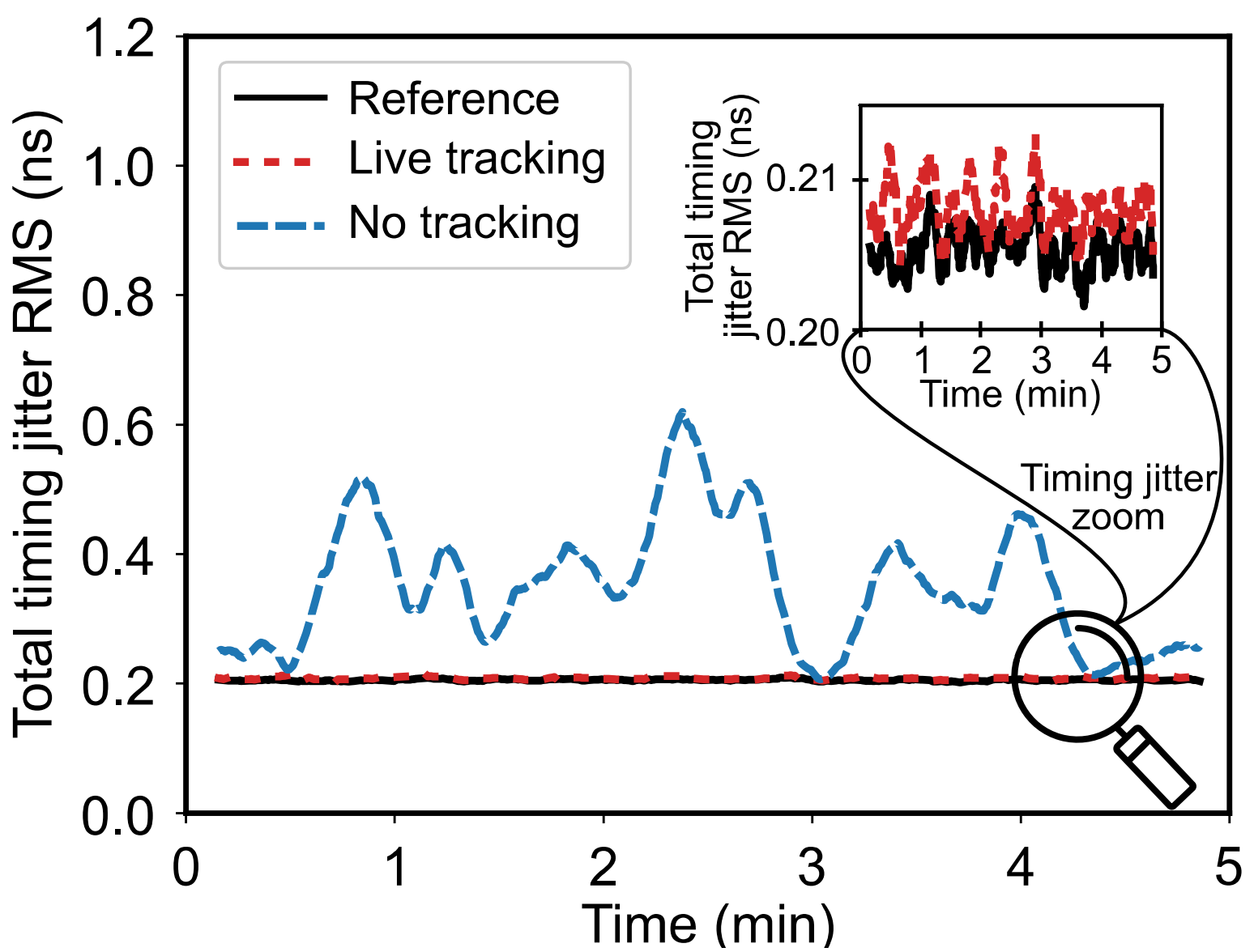


Fig. 7. Comparison of total system jitter with correlated photons and reference for 100 ms data package size and 600 ms feedback loop time. Live tracking of the correlation peak clearly reduces the jitter.

KEY GENERATION SOFTWARE (AIT)

Quantum key processing software consists of two major components (Fig. 8). The post processing stack transforms transmitted raw key material into keys which could successfully be received and validated on both key sharing entities. To perform this the raw key material gets processed in several modules where each prepares the key material for the next one. Most of the modules communicate to their corresponding peer module and their transmitted messages must be authenticated. Therefore a delayed authentication is in place which collects, after initialization, all transmitted messages per key and verifies their authenticity just before storing the key into a key management system which is the second major component of the software. It orchestrates the storage, synchronization and provision of keys to client applications. After new processed key material arrives at the KMS it will be split into smaller fixed size chunks, mapped with a new key identifier and synchronized with its peer. Clients like the crypto box are then able to request keys from the KMS which uses synchronization to ensure that the same key is provided to the corresponding peer crypto box based on a key stream session identifier.

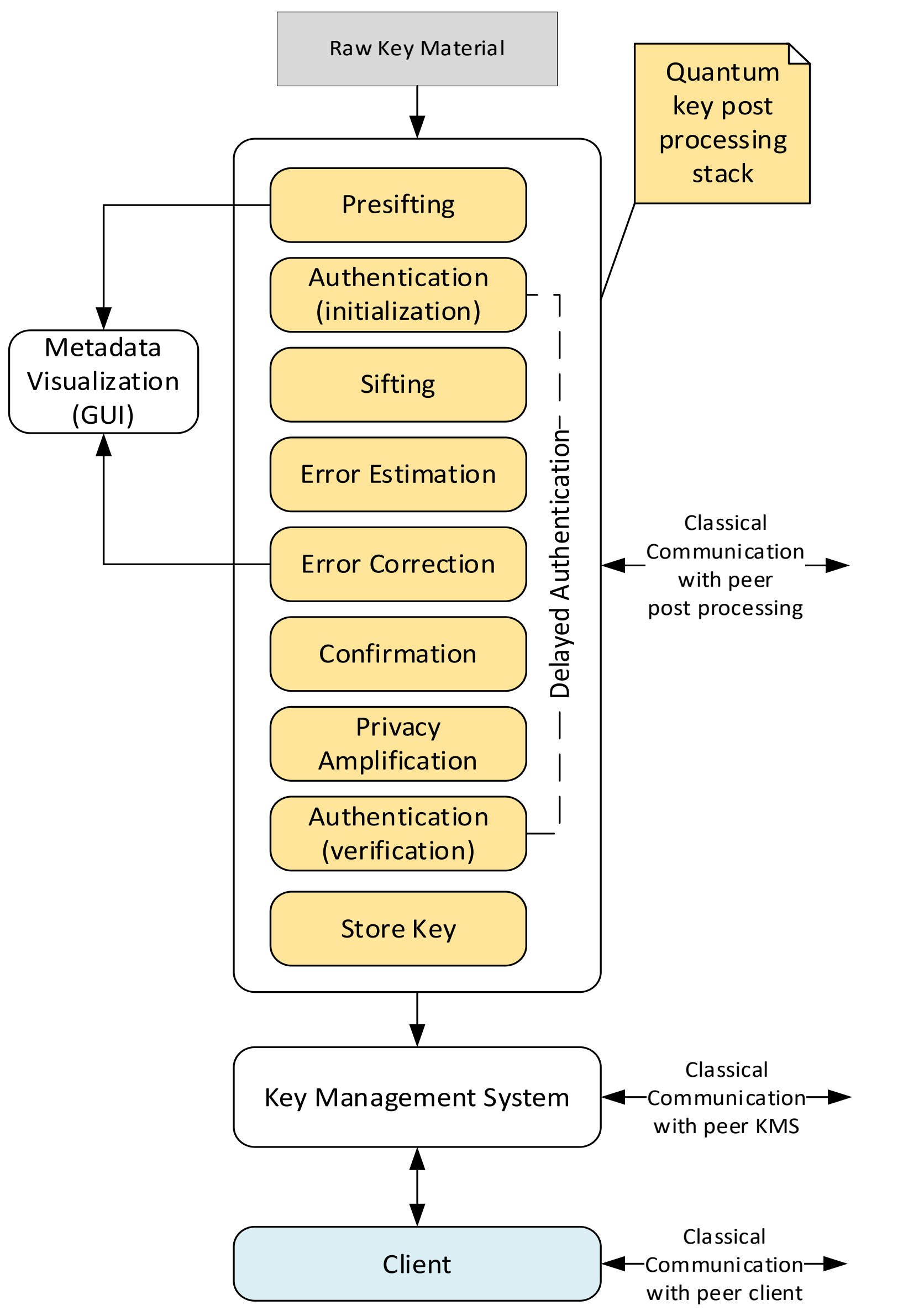

Raw Key Material
Quantum key post processing stack
Presifting
Authentication (initialization)
Sifting
Error Estimation
Error Correction
Confirmation
Privacy Amplification
Authentication (verification)
Store Key
Delayed Authentication
Metadata Visualization (GUI)
Classical Communication with peer post processing
Key Management System
Classical Communication with peer KMS
Client
Classical Communication with peer client

Fig. 8. Illustration of the quantum key distribution software components and their interaction.

In order to provide metadata information on the transmitted quantum bits there is a timeline based visualization realized with Grafana and InfluxDB. The first visualizes quantum bit error rates (QBER) and coincidences based on the stored metadata in the latter.

REFERENCES

[1] Bennett, Charles H.; Brassard, Gilles; Mermin, N. David (1992): Quantum cryptography without Bell's theorem. In: Phys. Rev. Lett. 68 (5), 557–559.

[2] Kim, Taehyun; Fiorentino, Marco; Wong, Franco N. C. (2006): Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. In: Phys. Rev. A 73 (1), 012316.

[3] Chen, Yu-Ao; Zhang, Qiang; Chen, Teng-Yun; Cai, Wen-Qi; Liao, Sheng-Kai; Zhang, Jun et al. (2021): An integrated space-to-ground quantum communication network over 4,600 kilometres. In: Nature 589, 214–219.

Bundesministerium
für Bildung
und Forschung

QuNET

Fraunhofer IOF

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY