A real-time experimental QKD platform for quantum-secure telecom infrastructures

Jan Krause, Benedikt Lezius, Richard Schilling, Jonas Hilt,
Stefan Weide, Nino Walenta, Nicolas Perlot, Ronald Freund

Fraunhofer Institute for Telecommunications,
Heinrich Hertz Institute, Einsteinufer 37,10587 Berlin, Germany
Email: jan.krause@hhi.fraunhofer.de

Fraunhofer HHI

INTRODUCTION

The German initiative QuNET [1] aims to prepare secure, robust and future-proof solutions for a quantum-secure IT infrastructure. It focuses on quantum key distribution (QKD) and covers three application scenarios:

I. Point-to-point links
- Individual solutions, e.g. datacenter backups, direct links between agencies.

II. Multi-user networks
- Solutions for critical infrastructure, e.g. energy, health

III: Large multi-user networks
- Access to end-to-end encryption for small entities / individual users with a strong focus on scalability.

Project scope
- Concepts development of overall networks and system architectures.
- Components development.
- Interoperability with post-quantum cryptographic solutions.
- Encouragement of private sector participation.
- Close cooperation with government authorities regarding standardization and certification.

DESIGN

As part of QuNET, we present our first-generation experimental real-time QKD platform that enables the study of different protocols, mainly targeting scenario I.

Selected features
- Optimized for short- and mid-range high data rate applications.
- ETSI GS QKD 004 interface allows for flexible key usage / different commercial encryptors.
- Implementation of the 1-decoy timebin-phase BB84 protocol [2].

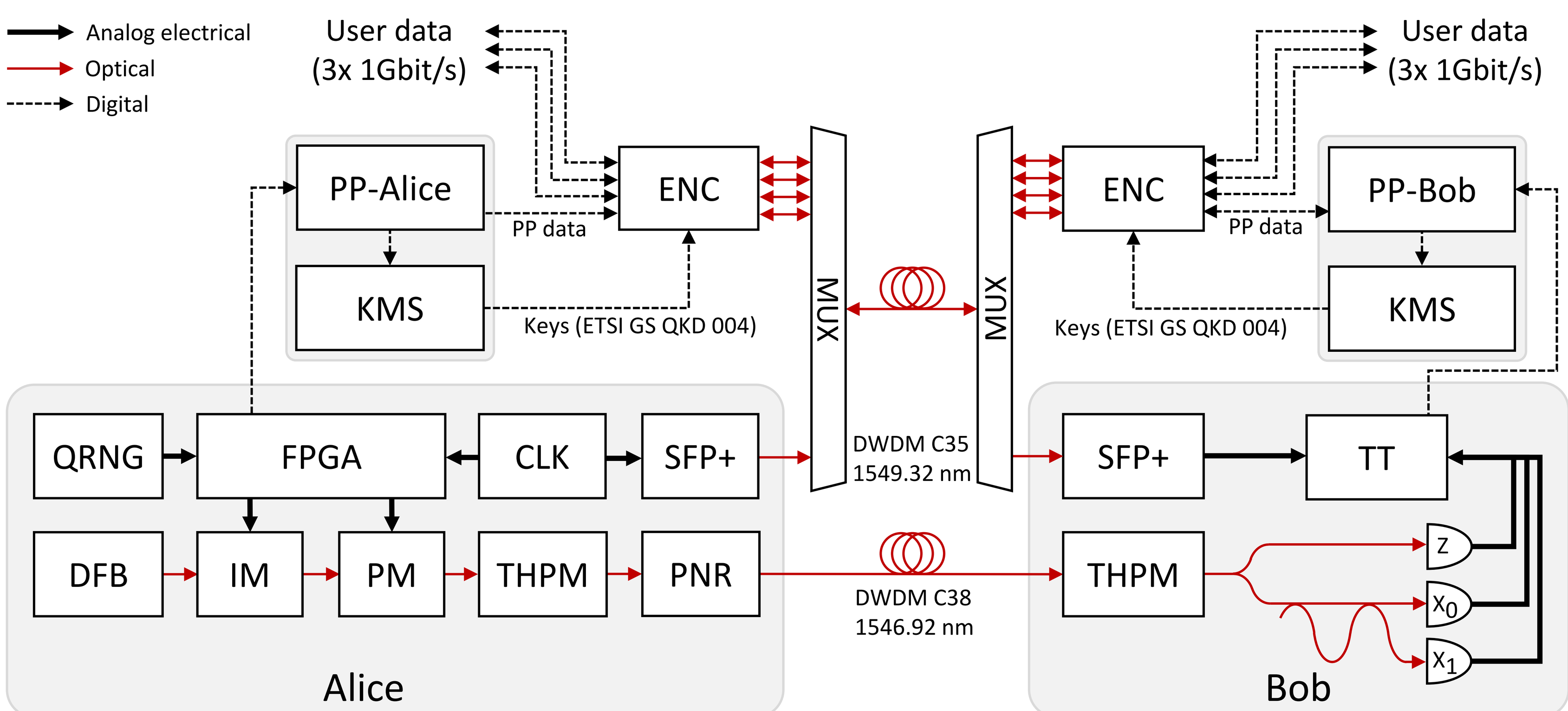

Figure 1: System design. Architecture allows for flexible protocol usage. ETSI GS QKD 004 protocol enables interchangeability of the commercial encryptors. All classical channels multiplexed over one fiber. QRNG: commercial quantum random number generator chip, FPGA: field-programmable gate array, CLK: clock, DFB: distributed feedback laser, IM: intensity modulator, PM: phase modulator, THPM: Trojan horse protection module, SFP+: enhanced small-form factor pluggable transceiver, PNR: active photon-number regulation, TT: Time tagger, PP: post-processing, KMS: key-management service, ENC: layer-2 AES encryptor.

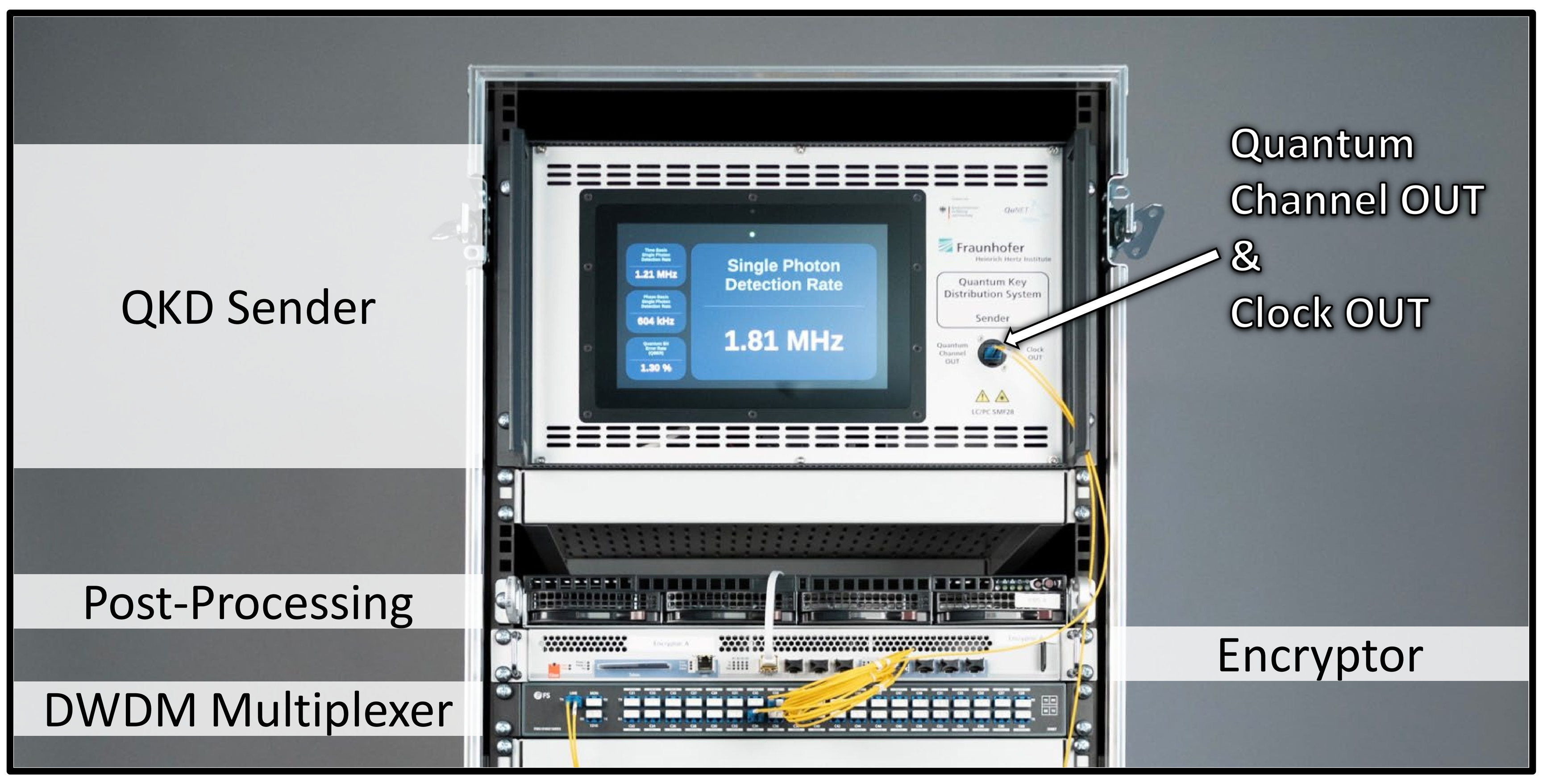

Figure 2: Sender setup including QKD sender, post-processing server, commercial encryptor and DWDM multiplexer.

RESULTS & SUMMARY

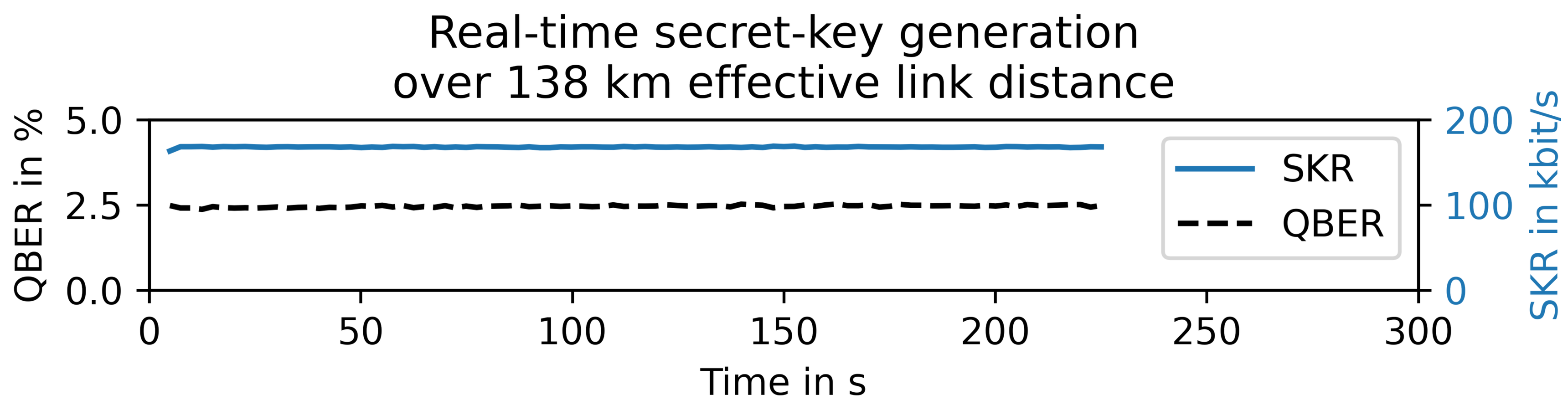

Figure 3: Results of a real-time measurement. We achieved a quantum bit error rate (QBER) of 2.46% and a secret-key rate (SKR) of 168 kbit/s, using superconducting nanowire single-photo detectors. Qubits were generated by Alice at a rate of 625 Mqbit/s.

- **Real-time QKD system demonstrated successfully over fiber and free-space links.**
- **Whole system (except for detectors) integrated into 19“ rack housings (Figure 2).**
- **Active stabilization loops enable uninterrupted use.**
- **Keyrate of 168 kbit/s over 138 km effective link distance achieved.**

OUTLOOK

- Further system integration, simplification and reduction of required components.
- Miniaturized photonic integration based on the HHI PolyBoard hybrid photonic platform.
- Increased focus on standardization and certifiability by Germal Federal Office for Information Security (BSI).

REFERENCES

[1] https://www.qunet-initiative.de/
[2] D. Rusca et al., „Finite-key analysis for the 1-decoy state QKD protocol“, Appl. Phys. Lett. 112, 171104, (2018)
[3] ETSI GS QKD 004 Quantum Key Distribution (QKD) Application Interface, V2.1.1 (2020-08)

Fraunhofer HHI

QuNET

SPONSORED BY THE
Federal Ministry of Education and Research

This research was conducted within the scope of the project QuNET, funded by the German Federal Ministry of Education and Research (BMBF) in the context of the federal government's research framework in IT-security “Digital. Secure. Sovereign.”.