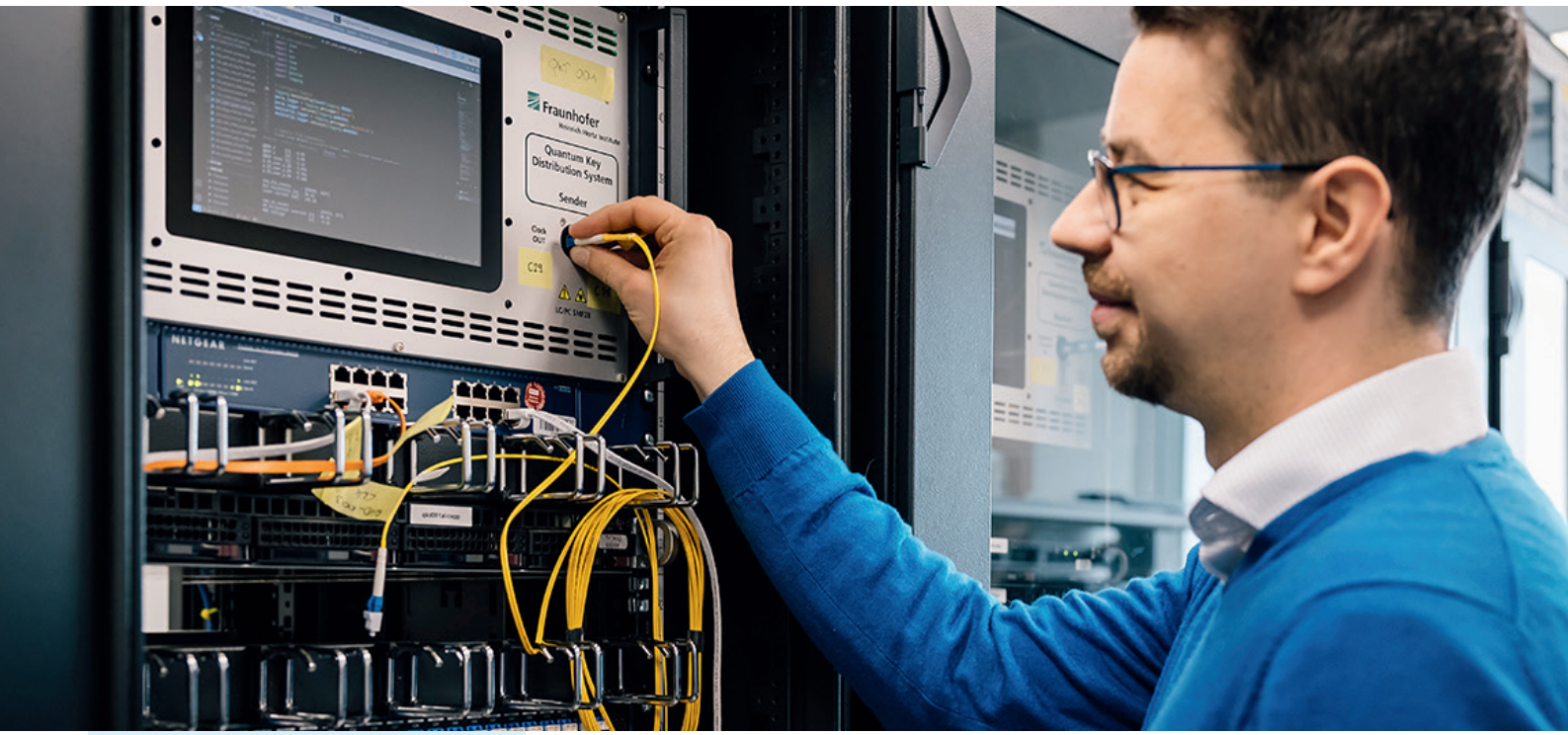
QUANTUM KEY DISTRIBUTION SYSTEM FOR FUTURE-PROOF SECURITY

Fraunhofer HHI



AT A GLANCE

Quantum Key Distribution (QKD) offers a robust and future-proof solution for the long-term protection of sensitive data transmissions and communication applications — even in light of the imminent threats posed by quantum computers.

Fraunhofer HHI has developed a turnkey QKD system that integrates seamlessly into modern telecommunication network infrastructures.

Specifications

- Autonomous startup and operation
- Continuous operation in dynamically switching and routing networks
- Instantaneous recovery after quantum channel interruptions
- No need for dedicated optical clocks or auxiliary channels
- Compatible with wavelength-multiplexing schemes
- ETSI-compliant key consumer and SDN monitoring interfaces
- 19" rack-compatible housing
- 625 MHz time-bin Decoy-BB84 QKD protocol

Background

Our information society depends on the constant availability of secure communication and data services. However, current encryption methods are increasingly at risk due to more advanced eavesdropping techniques, growing computational power, and the rapid advancement of quantum computing.

QKD counters these threats by using fundamental principles of quantum physics instead of complex mathematical algorithms. This approach guarantees long-term security for the generated and distributed keys — at high generation rates — and supports a broad range of cryptographic applications.

Fraunhofer HHI

Reference

Funded with in the German BMBF QuNET-Initiative

With funding from the:

Federal Ministry of Research, Technology and Space

QuNET

Applications

- Offsite data backup
- Secure backbone links
- High-security private networks
- Protection of SCADA systems in critical infrastructure
- Secure key distribution from central servers

Benefits

- Generation of highly secure symmetric keys for cryptographic applications
- Future-proof long-term protection of sensitive data
- Immunity to store-now-decrypt-later attacks
- Resilience against quantum-computer-based threats
- Quantifiable security guarantees
- High key generation rates

Description

The QKD system consists of a sender and receiver unit, both housed in 19" rack-compatible enclosures. Operating at a qubit rate of 625 MHz, the system implements time-phase encoding based on the 1-decoy-state BB84 protocol. A quantum random number generator (QRNG) provides the primary source of entropy.

The default quantum channel operates at 1546.92 nm but can be configured within the ITU DWDM grid. Uniquely, the HHI QKD system supports real-time optical switching and routing of the quantum channel and can resume operation within less than 500 ms following an interruption — a world-first feature enabling use in dynamic network environments.

All required classical communication occurs over standard routable TCP/IP channels. The system autonomously handles initial and continuous synchronization.

The receiver is compatible with various single-photon detectors, allowing optimization for specific use cases. Monitoring and control are possible via front panel displays and Ethernet interfaces. The QKD post-processing and key management software suite includes a complete post-processing stack and provides a key interface according to the ETSI QKD ISG 004 standard, ensuring interoperability with encryption devices and other applications.

Dr. Nino Walenta
Photonic Networks and Systems

Phone +49 30 31002-514 | -414
info-pn@hhi.fraunhofer.de

Fraunhofer Heinrich Hertz Institute
Einsteinufer 37, 10587 Berlin
Germany

www.hhi.fraunhofer.de/qkd

20250709