QUANTUM KEY DISTRIBUTION SYSTEM FOR FUTURE-PROOF SECURITY

Fraunhofer
Heinrich Hertz Institute

AT A GLANCE

Quantum Key Distribution (QKD) enables future-proof long-term protection of sensitive data transmission and communication applications – even against the imminent security threats of quantum computers. Fraunhofer HHI developed a high-speed QKD system that seamlessly integrates with commercial network encryptors.

Specifications

- Automated startup and operation
- Secure key rates:
  · 160 kbit/s over 140 km fiber distance
- Standardized interface to commercial encryptors
- Operation at DWDM-telecom wavelengths
- Quantum entropy source
- 19” rack compatible housing
- 625 MHz Decoy-BB84 QKD protocol

Background

Today’s information society relies heavily on the omnipresent availability of secure communication and information services. However, the security of the used protection algorithms is constantly threatened by improved eavesdropping methods, increasing computing power and, in particular, the rapid progress of quantum computers. To counter these threats, quantum key distribution (QKD) provides a highly secure solution. Instead of complex mathematical algorithms, the security of QKD relies on fundamental quantum-physical principles that ensure the long-term protection of the generated and distributed keys. These secure keys are provided at very high rates for their use in a wide range of cryptographic applications.

Applications

- Offsite data backup
- Backbone link protection
- High-security private networks
- Critical infrastructure SCADA protection
- Key server distribution links

Benefits

- Highly secure symmetric keys for cryptographic applications
- Transmission of sensitive data with future-proof long-term security
- Protection against store-now-decrypt-later attacks
- Protection against security threats of quantum computers
- Quantifiable security
- High key rates

Description

The QKD system comprises a sender unit and a receiver unit in 19" rack compatible housing. The QKD system is based on a time-phase encoding following a BB84 protocol with the single Decoy-state method. The time-bin frequency is 1.25 GHz, the qubit frequency is 625 MHz. A QRNG is used as primary entropy source. The quantum channel wavelength is 1546.92 nm. In addition, an optical synchronization signal is transmitted from sender to receiver, which has a wavelength of 1549.32 nm. The system performs its initial synchronization as well as continuous re-synchronization automatically. The receiver is compatible with a wide range of single-photon detectors that can be optimized for specific use cases. The systems is monitored and controlled via screens at the front panels as well as through an Ethernet connection. The QKD-Postprocessing and Key Management Software Suite comprises the complete post-processing stack for the Time-Phase BB84 Protocol with single Decoy-state method and includes sifting, error correction, error verification and privacy amplification. The Key management system (KMS) provides the key interface based on the ETSI QKD ISG 004 standard for the use of the generated keys by encryption devices or other applications.

Dr. Nino Walenta
Photonic Networks

Phone +49 30 31002-514
Nino.walenta@hhi.fraunhofer.de

Fraunhofer Heinrich Hertz Institute
Einsteinufer 37, 10587 Berlin
Germany

www.hhi.fraunhofer.de/pn