QUANTUM KEY DISTRIBUTION SYSTEMS FOR FUTURE-PROOF INFORMATION SECURITY IN COMMUNICATION NETWORKS

Dr. Nino Walenta
Fraunhofer Heinrich Hertz Institute (HHI)
Photonic Networks and Systems
Einsteinufer 37, 10587 Berlin

Tel: +49 30 31002-514
Email: nino.walenta@hhi.fraunhofer.de
www.hhi.fraunhofer.de

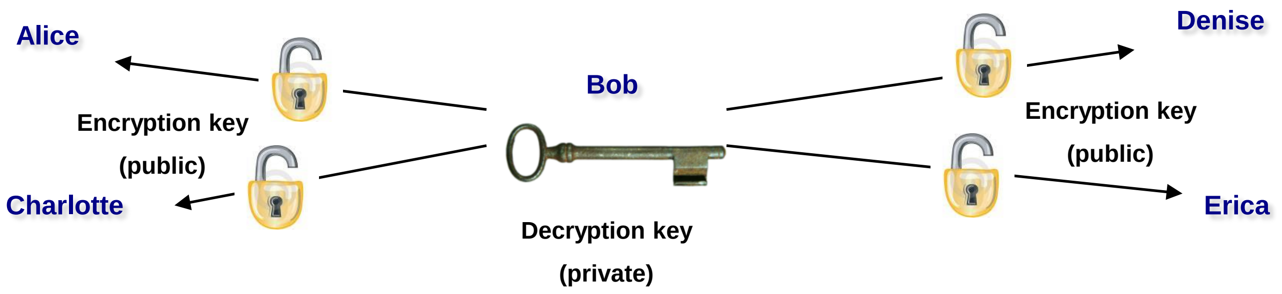
Why do we need secret keys?

- **Goal: Secure message transfer**
  - Authenticity: Message can't be altered by unauthorized party
  - Secrecy: Message can't be read by unauthorized party
- **Secret keys for authentication**
  - Comparison of authentication tags generated by **shared symmetric secret keys** to verify that message has not been altered during transfer.
- **Secret keys for encryption**
  - Encrypt confidential messages with **shared symmetric secret keys** to disclose information.
  - Symmetric encryption methods: OTP, AES, DES, 3DES, IDEA, ...

Problem: How to distribute the shared symmetric key?

nino.walenta@hhi.fraunhofer.de

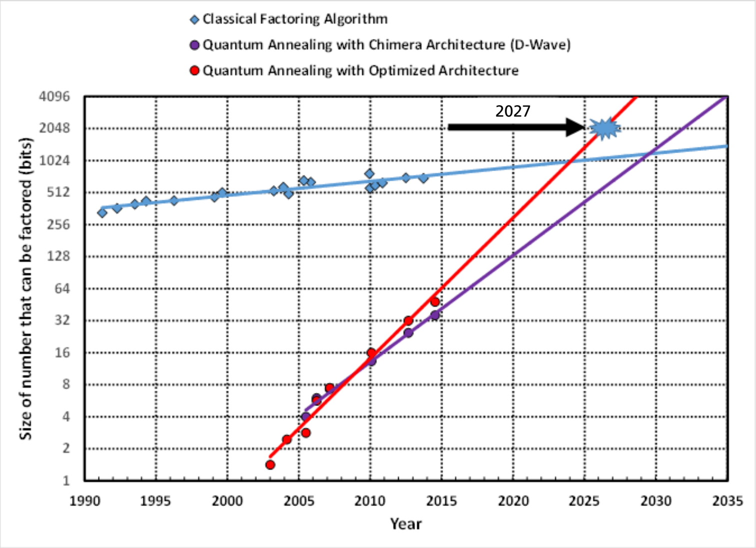
Public-Private-Key cryptography

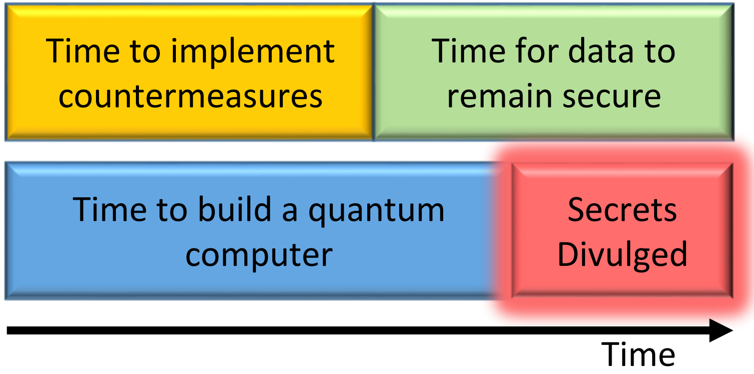


- Asymmetrical method that uses different keys for encryption (public) and for decryption (private)
- Security based on mathematical one-way-functions for factorization of large prime numbers
  - Easy to compute in one direction: 7’919 x 7’907 → 62’615’533
  - Difficult (but not impossible) in reverse: 62’615’533 → 7’919 x 7’907
- **Problem: Vulnerable to mathematical and technological progress**

nino.walenta@hhi.fraunhofer.de

When Quantum Computers Will Be Ready?



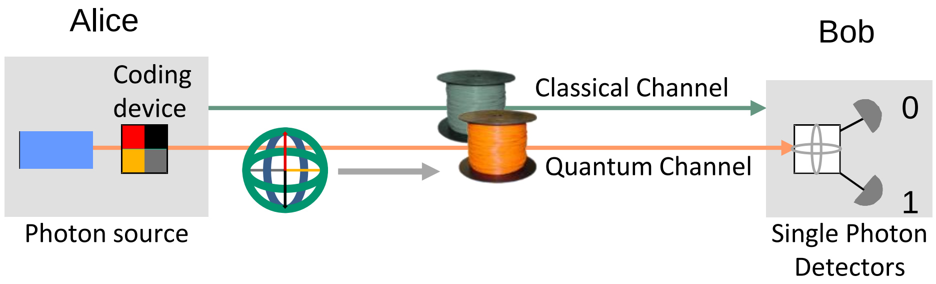


- M. Mosca (NIST April 2015, ISACA September 2015): *"There's a 1/7 chance that quantum computers are capable of breaking RSA-2048 by 2026, and 1/2 chance of breaking it by 2031"*.
- Working hypothesis of the BSI for the high-security sector: *"With a significant probability, there will be a cryptographically relevant quantum computer in the beginning of the 2030s"**

nino.walenta@hhi.fraunhofer.de
Fraunhofer HHI

BB84 Quantum key distribution

- Quantum key distribution (Bennett and Brassard, 1984)
  - Idea: - Encoding information in quantum states (Qubits)
  - Basis: - No-cloning theorem for quantum states
    - Unavoidable perturbation through a measurement on an unknown quantum system
  - Aim: - Distribution of shared secret keys with information-theoretically proven security



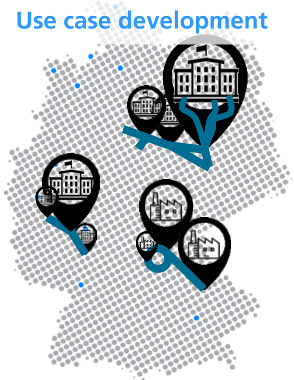
- Quantum key distribution allows
  - continuously expanding a **secret key shared** between Alice and Bob
  - while measuring the information an **arbitrary powerful eavesdropper** could gain.

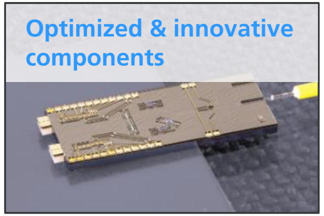
nino.walenta@hhi.fraunhofer.de

BMBF QuNET-initiative

Quantum technologies for secure federal agencies communication

- German initiative on **Quantum Key Distribution** (QKD) funded by **BMBF**
- Timeframe 2019 - 2026, ca. 165 Mio € budget
- **4 core institutes**: Fraunhofer HHI and IOF, German Aerospace Center (DLR-IKN), Max Planck Institute (MPL)
- **Preparation of certification** with BSI and industry by operation of a test-infrastructure
- **Interoperability** to other national and EU initiatives for quantum communication
- **Partner projects** with industry and academia, e.g. towards industrialization



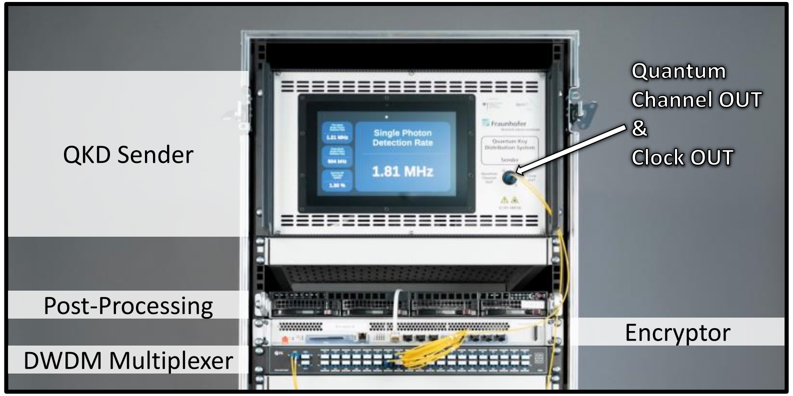


nino.walenta@hhi.fraunhofer.de

System Integration for Quantum Communication

HHI BB84 Quantum Key Distribution System

- 625 MHz Time-Bin encoded BB84 QKD system
  - Automatic startup and continuous operation under varying conditions
  - Interoperability with central key management system, industrial encryptors, and commercial Telco systems
  - Operation over telecom fiber and FSO-links
  - Single-decoy-state method for increased secret key rate



nino.walenta@hhi.fraunhofer.de

QKD-secured video-conferencing

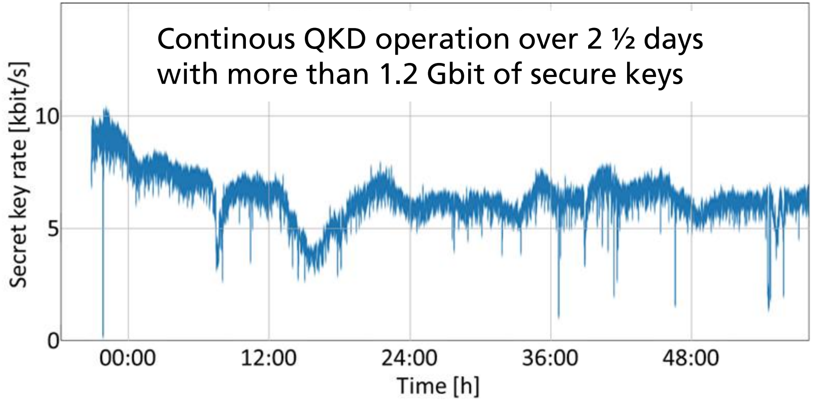
- **First QKD link between two German federal government offices** for quantum-secured video-conferencing
- Multiple QKD systems over fiber and free-space links in a heterogeneous architecture
- Compatibility with commercial encryption and video-conference solutions

https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/2021/08/100821-Quantenkommunikation.html

nino.walenta@hhi.fraunhofer.de

All-optical ad-hoc free-space QKD-link

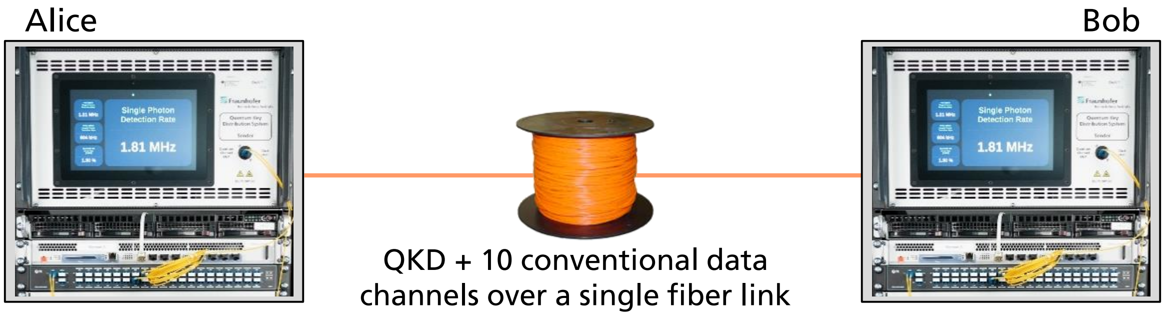
- Ad-hoc free-space QKD link connecting two HHI sites for QKD-secured optical communication
  - All optical installation
  - Day and night operation



nino.walenta@hhi.fraunhofer.de

Single-fiber operation of QKD + conventional channels

Goal: Reduced fiber costs and seamless integration



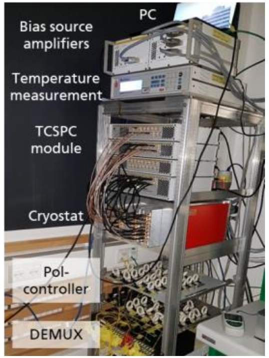
- Quantum channel at 1310 nm, and
- 10 conventional communication channels in C-band (~1550 nm)
- More than 8 mW total launch power
- DWDM-QKD over more than 70 km fiber

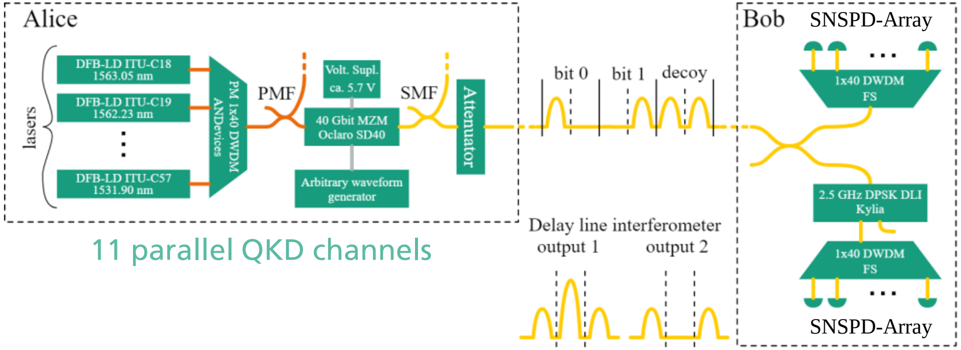
nino.walenta@hhi.fraunhofer.de
QuNET
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung
Fraunhofer

Multiple parallel quantum channels over 1 fiber

Goal: Massively increased secret key rate

- Massively parallelized Time-bin QKD with FPGA-processing and superconducting detector arrays
- Optimized QKD-Receiver with only one common delay-line interferometer for all QKD-channels
- Operation of 11 QKD channels with over 14 Mbit/s secret key rate over a single fiber
  - Sifted key rate per channel: 1.8 to 6.2 Mbit/s
  - QBER: 0.5 to 1.7 %
  - Visibility all above 95 %
  - Secret key rate per channel: 0.7 to 2.5 Mbit/s
- Total sifted key rate: 40 Mbit/s
- Total secret key rate: 14 Mbit/s



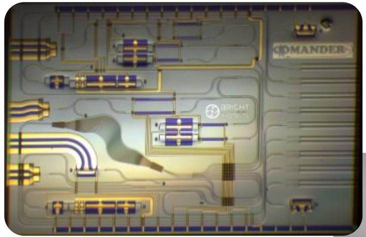


11 parallel QKD channels

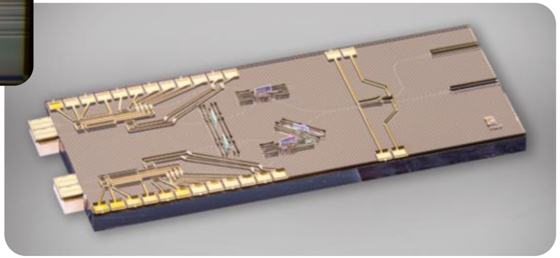
nino.walenta@hhi.fraunhofer.de

Photonic Integration for Quantum Communications

Towards integrated components and circuits



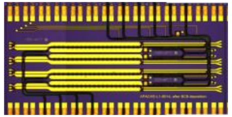
Monolithic PICs – InP



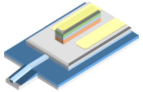
Tunable BB84 transmitter based on Polyboard Hybrid PICs

Lasers

Detectors



Modulators



SPADs

Components – InP

nino.walenta@hhi.fraunhofer.de

QuNET
Gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer

Fraunhofer Institute for Telecommunications, Heinrich Hertz Institute, HHI

WE PUT SCIENCE INTO ACTION.

Contact:

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

Einsteinufer 37
10587 Berlin

nino.walenta@hhi.fraunhofer.de