

## QD-E-QKD

Quantum Dots for Entanglement-based Quantum Key Distribution

<b>Programm / Ausschreibung</b>	Quantenforschung (QFTE), Quantenforschung und -technologie (QFTE), QFTE 2021 transnational	<b>Status</b>	abgeschlossen
<b>Projektstart</b>	01.06.2022	<b>Projektende</b>	31.05.2025
<b>Zeitraum</b>	2022 - 2025	<b>Projektlaufzeit</b>	36 Monate
<b>Keywords</b>	Entanglement; Quantum Communication; Quantum Dots; Quantum Key Distribution;		

### Projektbeschreibung

Die Verschränkung ist ein grundlegender Bestandteil für die Ausweitung der Quantenschlüsselverteilung von der Kommunikation zwischen zwei Parteien auf Netzwerke ohne vertrauenswürdige Knoten. Die kommerzielle Anwendung dieses Konzepts wird derzeit jedoch durch die Natur des Photonenerzeugungsprozesses behindert, der den verwendeten Verschränkungsressourcen zugrunde liegt.

QD-E-QKD wird eine neuartige Technologie entwickeln, die auf Halbleiterquantenpunkten basiert, und diese in realistischen städtischen Kommunikationsszenarien testen, um die Grenzen der aktuellen Ansätze zur verschränkungsbasierten Quantenschlüsselverteilung zu überschreiten.

Unsere photonische Quelle wird aktuelle Forschungsentwicklungen in der Mikrofabrikation in einem einzigen Gerät kombinieren. Sein strukturelles Design wird hochwertige epitaktische Quantenpunkte einbetten und eine p-i-n -Diode zur Steuerung des Ladungsrauschens, einen kreisförmigen Bragg-Gitter-Resonator zur Helligkeitsverbesserung und ein piezoelektrisches Substrat für eine optimale Verschränkung umfassen. Wir gehen davon aus, dass unser Bauelement mit einem Verschränkungsgrad von nahezu eins mit Raten betrieben wird, die mehr als eine Größenordnung höher sind als diejenigen, die hochmoderne parametrische Down-converters erreichen können. Gleichzeitig garantiert die Multi-Paar-Emissionswahrscheinlichkeit nahe Null eine bessere Robustheit gegenüber Kanaldämpfungsverlusten bei der Implementierung des Kommunikationsprotokolls.

Wir werden dieses Bauelement verwenden, um die Quantenschlüsselverteilung unter Verwendung von zwei Quantenkanalansätzen, einer Singlemode-Faser und Freiraum, zu implementieren. Um einen stabilen Betrieb zu gewährleisten, werden wir ein eigenständiges Gerät entwickeln, das die Zeit-zu-Digital-Umwandlung mit der optischen Taktwiederherstellung für die Fernsynchronisation kombiniert, und einen Empfänger für die optische Kommunikation im freien Raum mit integrierter adaptiver Optik auf Basis deformierbarer Linsen.

Schließlich werden wir quantitatives Benchmarking bereitstellen, das durch theoretische Modellierung und Tests unterstützt

wird, um den Fortschritt gegenüber bestehenden verschränkungsbasierten Quantenschlüsselverteilungssystemen zu bestätigen. Dies wird eine brauchbare Technologie für die Realisierung komplexerer Quantenschlüsselverteilungsnetze bieten.

## **Abstract**

Entanglement is a fundamental ingredient for extending quantum key distribution from two-party communication to networks without trusted nodes. Yet, the commercial application of this concept is currently hindered by the probabilistic nature of the photon-generation process underlying the used entanglement resources.

QD-E-QKD will develop a novel technology based on semiconductor quantum dots and test it in realistic urban communication scenarios to surpass the limits of current approaches to entanglement-based quantum key distribution.

Our photonic source will combine recent research developments in microfabrication in a single device. Its structural design will embed high-quality epitaxial quantum dots and include a p i n diode for the control of charge noise, a circular Bragg grating cavity for brightness enhancement, and a piezoelectric substrate for optimal entanglement. We predict that our device will operate—at near-unity degree of entanglement—at rates that are more than one order of magnitude higher than those accessible by state-of-the-art parametric down converters. At the same time, the near-zero multi-pair emission probability guarantees better robustness against channel attenuation losses in the communication protocol implementation.

We will use this device to implement quantum key distribution using two quantum-channel approaches, a single-mode fiber and free space. To guarantee stable operation we will develop a stand-alone device that combines time-to-digital conversion with optical clock recovery for remote synchronization and a free space-optical-communication receiver with integrated adaptive optics based on deformable lenses.

Finally, we will provide quantitative benchmarking, backed by theoretical modelling and testing, to certify the advancement over existing entanglement-based quantum key distribution systems. This will offer a viable technology for the realization of more complex quantum key distribution networks.

## **Projektkoordinator**

- Universität Linz

## **Projektpartner**

- Quantum Technology Laboratories GmbH