CVSTAR

Continuous-Variable Multi-User Quantum Key Distribution for 5G and distributed storage applications

Programm / Ausschreibung	Quantenforschung (QFTE), Quantenforschung und -technologie (QFTE), QFTE 2021 transnational	**Status**	laufend
Projektstart	01.06.2022	**Projektende**	31.05.2025
Zeitraum	2022 - 2025	**Projektlaufzeit**	36 Monate
Keywords	quantum communication; quantum key distribution; continuous variables; multipartite; telecom networks		

Projektbeschreibung

Quantenschlüsselverteilung ist eine Quantentechnologie, die kryptographische Schlüssel zur Verfügung stellt, die quantum-safe sind, d.h. auch von Quantencomputern nicht berechnet werden können. Als Zwei-Parteien-Protokoll wird die Quantenschlüsselverteilung üblicherweise mit direkten Punkt-zu-Punkt-Verbindungen über Glasfasern genutzt. Die typische Telekom-Infrastruktur besteht aber auch aus passiven optischen Netzwerken, die Beam-Splitter verwenden, um kosteneffizient mehrere Benutzer mit einem zentralen Zugangsknoten zu verbinden.

Im vorgeschlagenen Projekt beabsichtigen wir, Protokolle zur Quantenschlüsselverteilung für mehrere Benutzer zu entwickeln, Prototypen zu implementieren und zwei typische Anwendungsfälle in bestehender Telekom-Infrastruktur zu demonstrieren: Die Verschlüsselung von Fronthaul-Verkehr in mobilen 5G-Netzen und informationstheoretisch sichere, redundante, verteilte Datenspeicherung. Unsere Lösungen für Quantenschlüsselverteilung basieren auf der Technology der kontinuierlichen Variablen, die die Amplituden- und Phasen-Quadratur von Licht und die kohärente Detektion, ähnlich wie in der optischen Telekommunikation nutzt. Im Szenario mit mehreren Anwendern betrachten wir unterschiedliche Vertrauensbeziehungen (Anwender vertrauen einander nicht bzw. Anwender arbeiten zusammen), was es Service Providern ermöglichen wird, ihre Infrastruktur optimal auf die Anwendungsfälle abzustimmen. Während unsere Felddemonstrationen ausschließlich auf kohärenten Zuständen basieren wird, werden die Labordemonstrationen auch gequetschte Zustände verwenden, die die Erzeugung von kryptographischen Schlüsseln zwischen weiter entfernten Empfängern ermöglicht.
Wir erwarten, dass die Methoden, die in diesem Projekt entwickelt werden, erste Schritte hin zu einer zukünftigen Anwendung von Quantenschlüsselverteilung in Zugangsnetzen setzen wird. Mögliche Anwendungen werden die quantensichere Verschlüsselung von 5G Fronthaul Verkehr, verteilte Datenspeicherung, verteilte Berechnungen und andere Multi-Anwender-Szenarios sein. Schließlich wird es die quantensichere Verschlüsselung für Endanwender ermöglichen, die Fiber-to-the-home benutzen.

Abstract

Quantum key distribution is a quantum technology providing cryptographic keys with future proof and therefore quantum-safe security. As a two-party protocol, quantum key distribution is usually used with

direct point-to-point fiber connections. However, typical telecom infrastructures consist also of point-to-multipoint passive optical networks which use a beam splitter to cost-efficiently connect multiple users to a central access node.
In the proposed project, we aim to develop multi-user quantum key distribution protocols, to implement prototypes and to demonstrate two typical use-cases in existing telecom infrastructure: encrypting fronthaul traffic of 5G mobile networks and information theoretical secure and redundant distributed data storage.
Our quantum key distribution solutions are based on continuous-variable quantum technology making use of amplitude and phase quadratures of light and coherent detection similar to optical telecommunication. In the multi-user scenario, we consider different levels of trust, with users either not trusting each other or collaborating with each other, which will allow service providers to optimally map infrastructure and use-cases. While our field demonstrations will be based on coherent states exclusively, lab demonstrations will also employ squeezed light which enables generation of cryptographic keys between remote receivers.
We expect that the methods developed in this project will constitute first steps towards a future deployment of quantum key distribution in access networks. More specifically, potential applications will be quantum-safe encryption of 5G fronthaul traffic, distributed data storage, distributed computing and other multi-user scenarios. Finally, it may enable quantum-safe cryptography for end-users using fiber-to-the-home.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- fragmentiX Storage Solutions GmbH