Quantum Key Distribution

Quantenbasiertes Schlüsselaustauschverfahren für abhörsichere Kommunikation

Die rasante Weiterentwicklung der Quantencomputer verändert die Grundlagen der Cybersicherheit nachhaltig. Während klassische Verschlüsselungsmethoden wie RSA in Zukunft leicht angreifbar werden, eröffnet die Quantenphysik neue Möglichkeiten, Datenverbindungen uneinnehmbar zu machen. Quantum Key Distribution (QKD) nutzt die Gesetze der Quantenmechanik – insbesondere verschränkte Lichtteilchen – um symmetrische Schlüssel so zu übertragen, dass jeder Abhörversuch sofort erkennbar wäre. Österreich verfügt dank jahrzehntelanger Forschung über eine international führende Kompetenz in diesem Feld. Das AIT Austrian Institute of Technology hat diese Expertise gebündelt und Europas bedeutendste Quantum-Kommunikationsinitiativen maßgeblich mitgestaltet.

Fakten

- Lösungsbereich: **Organisationen, Prozesse, Technologische Innovation**
- Verwaltungsebene: **Bundesland, Bund**
- Lösungsprozess: **Digitalisierung und Technologie, Öffentlicher Dienst, Sicherheit und Verteidigung, Wissenschaft und Forschung**
- Technologie: **Informationstechnologie, Netzwerke**

So funktioniert es

QKD ermöglicht die Generierung und Übertragung kryptografischer Schlüssel über optische Fasern oder künftig auch über Satelliten – geschützt durch fundamentale physikalische Prinzipien. Wird ein Photon während der Übertragung abgefangen oder manipuliert, verändert sich dessen Zustand unmittelbar. Dieser Effekt macht Angriffe messbar und verhindert unentdecktes Mitlesen. Die Schlüssel dienen anschließend zur symmetrischen Verschlüsselung von Daten, während die Übertragung der Schlüssel selbst vollkommen abhörsicher bleibt. Die Rolle des AIT ist hierbei zentral: Die Forschungseinrichtung war bereits an den frühen Experimenten des Nobelpreisträgers Anton Zeilinger beteiligt, dessen bahnbrechende Versuche 2004 erstmals eine QKD-Übertragung zwischen einer Bank und dem Wiener Rathaus demonstrierten. In der Folge bündelte das AIT seine wissenschaftliche Exzellenz und übernahm internationale Leitrollen in großen europäischen Projekten wie OpenQKD, UNIQORN, CiViQ oder QUARTZ. Während OpenQKD ein europaweites Testbed für Quantenkommunikation schuf, gelang in UNIQORN die Miniaturisierung eines voll funktionsfähigen QKD-Transmitters auf einen 2x4-mm-Photonik-Chip – ein entscheidender Schritt zur Massenmarkttauglichkeit. Künftig werden hardwarebasierte QKD-Protokolle parallel zu softwarebasierten Post-Quantum-Cryptography-Verfahren eingesetzt, bis europaweit eine vollständige Ende-zu-Ende-Quantenkommunikationsinfrastruktur (EuroQCI) etabliert ist. Österreich nimmt hier eine Vorreiterrolle ein: Durch nationale KIRAS Projekte wie QKD4GOV und QCI-CAT entsteht bereits ein erstes operationelles Quantennetzwerk für hochsichere Behörden- und Gesundheitskommunikation. Auch die Beteiligung des AIT an QUARTZ ermöglicht es, terrestrische QKD-Übertragungen durch satellitengestützte Quantenverbindungen zu ergänzen, um globale Reichweiten zu erzielen.

Das große Ganze

QKD markiert einen strategischen Paradigmenwechsel: Weg von rein mathematischer Kryptografie, hin zu physikalisch garantierter Sicherheit. Für Staaten, kritische Infrastrukturen, Netzbetreiber, Cloud-Provider, Forschungseinrichtungen und Unternehmen bedeutet dies ein völlig neues Sicherheitsniveau. Europa sichert sich damit digitale Souveränität in einer Zukunft, in der Quantencomputer etablierte Verschlüsselungen brechen können. Durch die enge Verflechtung von Forschung, Industrie und öffentlicher Verwaltung in den

Quantum Key Distribution

Quantenbasiertes Schlüsselaustauschverfahren für abhörsichere Kommunikation

europäischen Projekten konnten Know-how-Aufbau, Standardisierung, Interoperabilität und die Entwicklung neuer Produktionskapazitäten beschleunigt werden. Österreich und seine Partner sind heute in der Lage, sowohl hochsichere Regierungsnetze aufzubauen als auch kostengünstige, miniaturisierte QKD-Komponenten für künftige Massenanwendungen zu entwickeln. Von sicheren Gesundheitsdaten über vernetzte Behördenprozesse bis hin zu globalen Kommunikationseinrichtungen entstehen neue Ökosysteme, neue Qualifikationen und zukunftsorientierte Arbeitsplätze entlang der gesamten Wertschöpfungskette. QKD ist damit weit mehr als eine Sicherheitslösung: Es ist ein europäischer Technologietreiber, der wissenschaftliche Exzellenz, industrielle Innovation und staatliche Souveränität verbindet – und Europa im globalen Wettlauf um Quantenkommunikation sichtbar an die Spitze setzt.

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Wien, Österreich

+43 (1) 448 00 55 10
platform@bestpracticeaustria.at