



Quantum Communication Infrastructure

- Quantum Key Distribution
- Post Quantum Cryptography

Quantensichere Kommunikation nutzt Prinzipien der Quantenmechanik, um die Sicherheit moderner Kommunikationssysteme langfristig zu gewährleisten.

CANCOM

Verschlüsseln Sie noch oder beamen Sie schon?

CANCOM bietet Lösungen für quantensichere Datenübertragung.

Herkömmliche Verschlüsselungsverfahren könnten in den nächsten 5 bis 10 Jahren durch Quantencomputer kompromittiert werden. Quantensichere Kommunikation wird entwickelt, um diesen zukünftigen Bedrohungen mit neuen, robusten Verschlüsselungsmethoden entgegenzuwirken.

| Quantensichere Kommunikation – wie funktioniert das?

Ein zentrales Element ist **Quantum Key Distribution (QKD)**. QKD basiert auf physikalische Prinzipien und ermöglicht die Erzeugung von kryptographischen Schlüsseln, in dem einzelne Lichtteilchen (Photonen) verwendet werden.

Ein weiteres wichtiges Konzept ist die **Post-Quantum Cryptography (PQC)**, welches auf neuen mathematischen Prinzipien basiert.

Diese kryptographische Verfahren sind so konzipiert, dass sie auch gegen Angriffe von Quantencomputern resistent sind. PQC und QKD können kombiniert werden, um eine hybride Verschlüsselung zu schaffen.

Stark vereinfacht beschrieben „beamt“ ein QKD-System kryptographische Schlüssel, welche für symmetrische Verschlüsselung unterschiedlichen Anwendungen (z.B. VPN) genutzt werden können.

| Die Use-Cases.



Abhörsichere Kommunikation. Für verschiedenste Branchen.

Durch das physikalische „No-Cloning-Theorem“ ist es unmöglich, unbekannte Quantenzustände zu kopieren – ein Abhören von Schlüsselaustausch ohne Entdeckung wird somit verhindert.



Hochsichere Übertragungswege. Sicherheit an erster Stelle.

Quantenresistente Verbindungen eröffnen neue Möglichkeiten zur hochsicheren Übertragung von Daten, speziell für die kritische Infrastruktur und öffentliche Bereiche.



Innovative Zukunftssicherung. Mit cutting-edge Technologie.

Mit Quantentechnologie wird der Grundstein für zukunftssichere Verschlüsselung gelegt, die auch gegen Entschlüsselungsversuche von Quantencomputern gesichert ist.

Die CANCOM Lösung.

- ✓ **Eigenentwicklungen** – das in-house Tool „Arnika“ ermöglicht quantenresistente VPN-Verbindungen.
- ✓ **Forschung/Entwicklung** – Beteiligung an Forschungsprojekten und Kongressen.
- ✓ **Partnerschaften** – mit Herstellern
- ✓ **Beratung** – Beratungsleistungen und Aufklärung

Adressierbare Verticals.

Branchen mit Anforderung an hohe Datenübertragungssicherheit.

- ✓ Netzbetreiber/Energiesektor
- ✓ Healthcare
- ✓ Finance
- ✓ Public
- ✓ Transport (Luft- und Raumfahrt)
- ✓ Militär

Holen Sie mit unseren Lösungen das Beste aus Ihrem Business heraus!
Fragen Sie ganz unverbindlich bei unseren Expert:innen an: quantum@cancom.com