Quantenkommunikation

Einleitung: Was ist Quantenkommunikation?

Kurze, verständliche Einführung

- Quantenkommunikation = Informationsübertragung mit Prinzipien der Quantenmechanik.
- Nutzt **Verschränkung** und **Superposition** zur sicheren Schlüsselverteilung.
- Abhörversuch → Manipulation durch Abweichungen in der statistischen Verteilung sofort erkennbar
- Wichtige Anwendung: **Quantenschlüsselverteilung (QKD)** → Schlüssel ist abhörsicher.
- Erste praktische Anwendungen: Pilotprojekte wie **QuNet** in Berlin, Forschung an **Quantenrepeatern** und **Satelliten** für größere Entfernungen.
- https://www.youtube.com/watch?v=b4tHIckW8aY
- [1]
- **Beispiel Alice/Bob:**

- Grundsätzlich läuft das so: Zwei Kommunikationspartner, in der Quantenliteratur für gewöhnlich "Alice" und "Bob" genannt, wollen sich eine Botschaft schicken. Alice verschlüsselt die Information in Frankfurt und schickt sie als Zahlenreihe aus Nullen und Einsen, also im Binärcode zu Bob nach Kehl. Den verwendeten Schlüssel, eine ebenso lange Zahlenreihe aus Nullen und Einsen, schickt Alice anschließend mittels Quantenteilchen, zum Beispiel Photonen, durch die Glasfaserleitung zu Bob. Die beiden machen sich messbare Zustände dieser Lichtquanten zunutze, üblicherweise deren Polarisation – die Schwingungsrichtung des Lichts. Nach einem Abgleich kann Bob die ursprüngliche Botschaft entschlüsseln. Versucht nun eine dritte Person, üblicherweise "Eve" genannt, den Schlüssel in der Mitte der Leitung abzugreifen, können Alice und Bob das mit hoher Wahrscheinlichkeit feststellen. Die Regeln der Quantenphysik wollen es so: Bei jedem Versuch, die Polarisation der abgefangenen Photonen unbemerkt zu messen, läuft Eve Gefahr, diese zu verändern und sich so zu verraten. [2]

Grundlegende Prinzipien (Quantenmechanik) → näheres im zweiten Kapitel

- **Quantenunschärfe**: Messergebnisse sind nicht exakt vorhersehbar, sondern echt zufällig.
- **Verschränkung**: Zwei Teilchen oder Lichtstrahlen sind miteinander gekoppelt → Messungen an A und B zeigen zufällige, aber korrelierte Ergebnisse.
    - → Die Quantenkommunikation nutzt Eigenschaften der Quantenunschärfe, um abhörsichere Kommunikationsnetzwerke aufzubauen. Eine wichtige Rolle spielen dabei verschränkte Zustände des Lichts. Sind zwei Lichtstrahlen mit einander verschränkt, so macht sich dieses durch Korrelationen in ihren Unschärfen bemerkbar. Teilen sich „A“ und „B“ ein verschränktes System, so ergeben Messungen an den Teilsystemen zum einen echt zufällige Messergebnisse, zum anderen zeigen sich gemeinsame Muster in den Zufallsergebnissen. Die Abbildung rechts illustriert diesen Sachverhalt an zwei fiktiven Würfeln, die ungezinkt sein sollen und somit zufällig fallen, aber trotzdem immer identische Augenzahlen zeigen. (Bem.: Ein Wurf entspricht hier einer Messung. Vor jeder Messung müssen die Würfel wieder erneut verschränkt werden.)

- **Abhörerkennung**: Manipulation zerstört die Verschränkung und wird statistisch sichtbar.
    - ➔ Verschränkte Zustände des Lichts sind ideal, um einen Quantenschlüssel für die Quantenkryptographie zu verteilen. Die Eigenschaft der Verschränkung liefert für Messungen bei „A“ und bei „B“ echte Zufälligkeit, gleichzeitig aber auch die Übereinstimmung der Schlüsselketten, und drittens die Möglichkeit potenzielle Abhörversuche zu erkennen. Letzteres wird dadurch möglich, dass Abhörversuche (zu einem Teil) die Verschränkung stören und dadurch Spuren hinterlassen.
- **Dekohärenz**: Hauptproblem → Verlust der Verschränkung bei Übertragung.
- https://www.ingenieur.de/technik/fachbereiche/rekorde/quantenmechanik-verstehen-grundlagen-begriffe-und-phaenomene-einfach-erklaert/

Warum ist Quantenkommunikation wichtig?

- **Maximale Sicherheit**: Mathematisch beweisbar gegen heutige und zukünftige Angriffe.

    - ➔ Beispiel: Wir hatten 2015 die derzeit fortschrittlichste Quantenschlüsselverteilung basierend auf Amplituden- und Phasenmodulationen des Lichts demonstriert. Unsere Implementierung basiert auf stark Einstein-Podolsky-Rosen-verschränktes Licht [1] und ist absolut sicher gegen Abhörversuche, auch gegen solche, die möglicherweise erst zukünftig erfunden werden. Dieser Sicherheit liefert ein mathematischer Beweis auf Grundlage der Quantentheorie. Aus den Messdaten bei „A“ und „B“ wurde ein echt zufälliger und abhörsicherer Schlüssel mit einer Länge von über 108 Nullen und Einsen erzeugt. Das Besondere an unserer Implementierung war die Sicherheit gegen jegliche Angriffe auf den Kommunikationskanal (einschließlich Angriffe zukünftiger Technologien) sowie die Sicherheit gegen alle Angriffe auf die Geräte am Empfängerstandort [2]. → diese Quellen siehe Artikel

- **Abhörschutz**: Jeder Abhörversuch hinterlässt Spuren in den Messdaten.
- **Zukunftstechnologie**: Grundlage für sichere Kommunikationsnetze (z. B. Banken, Militär, Regierung).
- **Fortschrittliche Forschung**: z. B. Quantenrepeater, Photonenmessungen, Verschränkungs-Destillation

    - ➔ Zurzeit wird umfangreiche Forschung im Rahmen der Quantenkommunikation betrieben. Ein wesentliches Problem ist die Dekohärenz, die bei der Übertragung die Verschränkung reduziert und Quantenkommunikation schließlich unmöglich macht. 2008 konnten wir erstmalig eine Zwei-Kopien-Destillation von Verschränkung zeigen [3]. Auch die Grundlagenforschung an der Natur von verschränkten Systemen zeigt nach wie vor überraschende Ergebnisse. In unserer Arbeit [4] konnten wir zeigen, dass es verschränkte Systeme gibt, die Schrödingers „Steering“-Effekt nur in einer Richtung erlauben. Ob dieses Ergebnis zu einer Anwendung in der Quantenkommunikation führen wird, ist derzeit noch Gegenstand der Forschung. In [5] haben wir erstmalig die Quasiwahrscheinlichkeitsdichteverteilung der elektrischen Feldstärke eines

Ein-Photonen-Fockzustands bei der Telekommunikationswellenlänge von 1550 nm gemessen. Wie von der Quantentheorie vorhergesagt, ergeben sich negative(!) Werte (Abb.). In [6] haben wir aus einer großen Zahl nur wenig-gequetschter Zustände, eine geringe Zahl stärker gequetschter Zustände „destilliert“. Zum Einsatz kam eine hocheffiziente Photonenzählanlage.

- [3]

Grundlegende Konzepte der Quantenmechanik

- **Superposition:** Zustand, in dem sich ein Quantenteilchen in mehreren Zuständen gleichzeitig befindet (z. B. ein Qubit kann gleichzeitig 0 und 1 sein).
- **Verschränkung (Entanglement):** Zwei oder mehr Teilchen sind so miteinander verbunden, dass die Messung des Zustands eines Teilchens den Zustand der anderen sofort beeinflusst, unabhängig von der Entfernung.
- **No-Cloning-Theorem:** Ein unbekannter Quantenzustand kann nicht perfekt kopiert werden.
- Berühmte Experimente der Quantenmechanik

Anwendungen und Protokolle der Quantenkommunikation

- **Quantenschlüsselverteilung (QKD):** * Erklärung des Prinzips: Nutzung von Quantenmechanik, um einen sicheren kryptografischen Schlüssel zwischen zwei Parteien zu erzeugen.
    - Beispielprotokoll: **BB84** (Bennett-Brassard 1984).
- **Quanten-Teleportation:** * Erklärung des Prinzips: Übertragung eines Quantenzustands von einem Ort zu einem anderen ohne den physischen Transport des Teilchens selbst.
- **Quantennetzwerke:** Visionen und Herausforderungen für zukünftige, vernetzte Quantensysteme.

Herausforderungen und Zukunftsaussichten

- **Technologische Hürden:** Wie man Quantenteilchen stabil hält, um lange Distanzen zu überbrücken (Quantenrepeater).
- **Kosten und Infrastruktur:** Hohe Kosten für die Entwicklung und den Aufbau der Technologie.
- **Zukunftsaussichten:** Welchen Einfluss wird die Quantenkommunikation auf unsere Sicherheit und Technologie haben?

Fazit und Diskussionsrunde

- Zusammenfassung der wichtigsten Punkte.
- Ausblick auf die Relevanz für Kryptografie und Informationstechnologie.

References

- [1] Fraunhofer Gesellschaft, *Quantenkommunikation.* [Online]. Available: https://www.fraunhofer.de/de/forschung/artikel-2025/quantenforschung/quantenkommunikation.html
- [2] Leon Lindenberger, "Wie Quantenkommunikation den Datentransport künftig sicherer machen könnte," *Geo*, 2025. [Online]. Available: https://www.geo.de/wissen/forschung-und-technik/abhoersicher--wie-quantenkommunikation-alltag-werden-koennte-35665814.html
- [3] Prof. Dr. Roman Schnabel, *Quantenkommunikation und Verschränkung.* [Online]. Available: https://www.physik.uni-hamburg.de/iqp/ag-schnabel/forschung/quantenkommunikation.html