Hector Seminar

Quanteninformation

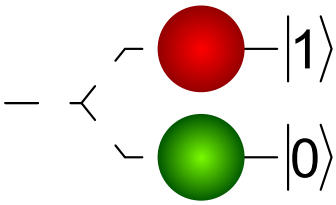
Quantencomputer und Quantenkryptographie

2025

Modulausschreibung

Zeitraum: AB

Die Quanteninformatik beschäftigt sich mit der Nutzung quantenmechanischer Prinzipien zur Verarbeitung und Übertragung von Informationen. Im Gegensatz zur klassischen Informatik, die auf Bits basiert, die entweder den Zustand 0 oder 1 annehmen, verwendet die Quanteninformatik sogenannte Qubits, die sich gleichzeitig in einer Überlagerung von Zuständen (*Superposition*) befinden können. Ein weiteres zentrales Prinzip der Quanteninformatik ist die *Verschränkung*, bei der zwei oder mehr Qubits so miteinander verbunden sind, dass der Zustand eines Qubits unmittelbar den Zustand der anderen beeinflusst, unabhängig von der Entfernung.

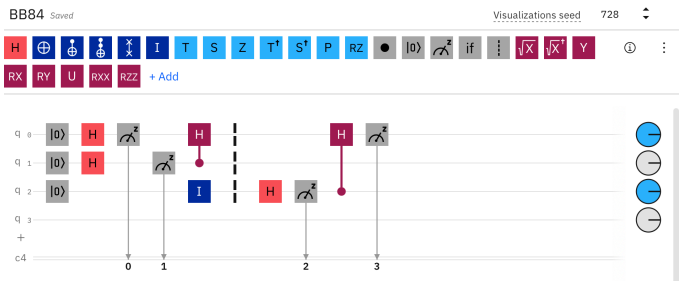


Qubit-Zustände
Von Clemens Adolphs, Lizenz

Die Quanteninformatik bietet sowohl auf algorithmischer Ebene als auch in der Kryptographie revolutionäre Möglichkeiten, die weit über das hinausgehen, was mit klassischer Informatik erreichbar ist.

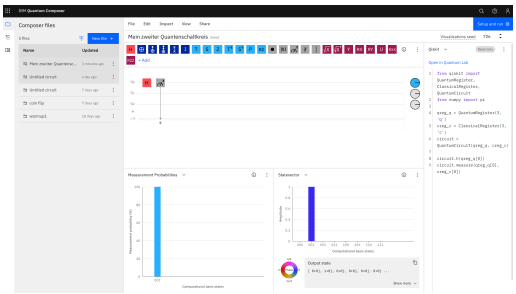
Quantenalgorithmen: die Phänomene der Superposition und der Verschränkung ermöglichen es Quantencomputern, mehrere klassische Berechnungen parallel durchzuführen und daher Rechenaufgaben effizienter zu lösen als klassische Rechner. Ein bekannter Quantenalgorithmus ist *Shor's Algorithmus*, der zur Faktorisierung großer Zahlen verwendet wird. Er hat weitreichende Konsequenzen für die Kryptographie, da er theoretisch in der Lage ist, klassische Verschlüsselungsverfahren wie RSA, die auf der Schwierigkeit der Primfaktorzerlegung beruhen, zu brechen. Im Gegensatz zu klassischen Algorithmen benötigt Shor's Algorithmus exponentiell weniger Rechenschritte.

Die **Quantenkryptographie** nutzt die Prinzipien der Quantenmechanik, um sichere Kommunikationsprotokolle zu entwickeln, die auch theoretisch nicht abhörbar sind. Das bekannteste Protokoll in diesem Bereich ist das *BB84-Protokoll*, benannt nach seinen Erfindern Bennett und Brassard (1984). Dieses Protokoll dient dem sicheren Austausch von kryptographischen Schlüsseln und basiert auf der Tatsache, dass der Zustand eines Qubits durch Messung verändert wird. Ein Abhörversuch würde also entdeckt, da die Messung der Qubits die Kommunikationspartner darauf hinweist, dass die Daten kompromittiert wurden.



BB84-Protokoll in der IBM Quantum Plattform

In unserem Modul wird ein Einblick in die Grundprinzipien der Quanteninformatik gegeben. Wir werden uns dabei einerseits mit Quantenalgorithmen beschäftigen und diese auch selbst auf der *IBM Quantum Plattform* programmieren (mit der Software Qiskit). Weiterhin werden wir uns auch mit Quantenkryptographie beschäftigen, insbesondere dem BB84-Protokoll. An dem *Labortag am Mi., 21.05.2025* an der Universität Stuttgart werden wir ein eigenes Experiment zum Erstellen und Austausch eines Quantenschlüssels mit dem BB84-Protokoll aufbauen und durchführen.



Hector Seminar

Quanteninformation

Quantencomputer und Quantenkryptographie

2025

Modulausschreibung

Zeitraum: AB

Voraussetzungen:

Eine regelmäßige Teilnahme an allen angegebenen Terminen ist notwendig.

Es wird eine besonders hohe Bereitschaft erwartet, sich mit den Themen selbstständig auseinander zu setzen. Zwischen den Treffen müssen die besprochenen Inhalte intensiv nachbereitet werden.

Ein gutes Hörverständnis der englischen Sprache ist notwendig, da wir z.T. englischsprachige Lernvideos verwenden werden.

Für die Teilnahme und Registrierung beim IBM Q Portal ist **das *Mindestalter von 14 Jahren*** (spätestens erreicht im Februar 2025) und die schriftliche Einwilligung der Erziehungsberechtigten erforderlich (siehe https://quantum.ibm.com/terms).

Die gemeinsame Abschlusspräsentation durch Vorträge und Poster findet am Samstag, 12. Juli 2025 am International Department in Karlsruhe statt.

Teilnehmerzahl: 20

Ort: Bunsengymnasium,
Humboldtstr. 23, Heidelberg

Kursleiter: Dr. Oliver Rudolph, Kursleiter Heidelberg
Brigitte Haller, Kursleiterin Heidelberg

Email: rudolph@hector-seminar.de
haller@hector-seminar.de

Termine:

- **Mi., 29.01.2025, 15^{00}-18^{00} Uhr**
- **Do., 30.01.2025, 15^{00}-18^{00} Uhr**
- **Mi., 19.02.2025, 15^{00}-18^{00} Uhr**
- **Do., 27.02.2025, 15^{00}-18^{00} Uhr**
- **Mi., 12.03.2025, 15^{00}-18^{00} Uhr**
- **Do., 13.03.2025, 15^{00}-18^{00} Uhr**
- **Mi., 02.04.2025, 15^{00}-18^{00} Uhr**
- **Do., 03.04.2025, 15^{00}-18^{00} Uhr**
- **Mi., 07.05.2025, 15^{00}-18^{00} Uhr**
- **Do, 08.05.2025, 15^{00}-18^{00} Uhr**
- **Mi., 14.05.2025, 15^{00}-18^{00} Uhr**
- **Do, 15.05.2025, 15^{00}-18^{00} Uhr**
- **Mi., 21.05.2025, ganztägig (Labortag, Uni Stuttgart)**
- **Do, 26.06.2025, 15^{00}-18^{00} Uhr**
- **Mi., 02.07.2025, 15^{00}-18^{00} Uhr**
- **Do., 03.07.2025, 15^{00}-18^{00} Uhr**
- **Mi., 09.07.2025, 15^{00}-18^{00} Uhr**
- **Do, 10.07.2025, 15^{00}-18^{00} Uhr**
- **Sa, 12.07.2025, Modulfest International Department KIT**
- **Do, 17.07.2025, 15^{00}-17^{00} Uhr Nachbesprechung**