V00

Quantenkryptografie Analogieversuch

Fritz Ali Agildere
fritz.agildere@udo.edu

Jan Lucca Viola
janlucca.viola@udo.edu

Durchführung: 9. Dezember 2024
Abgabe: ??. Dezember 2024

TU Dortmund – Fakultät Physik

Inhaltsverzeichnis

1 Zielsetung

2 Einleitung

Quantenkryptographie ist ein faszinierender Bereich der Quantenphysik, der sichere Kommunikation durch die Gesetze der Quantenmechanik ermöglicht. Das Ziel dieses Kapitels ist es, die theoretischen Grundlagen des Analogieversuchs zur Quantenkryptographie zu erläutern, wie er in einem didaktischen Kontext verwendet wird, sowie einen Vergleich zur echten Quantenkryptographie darzustellen.

3 Grundlagen der Quantenkryptographie

3.1 Das BB84-Protokoll

Das BB84-Protokoll wurde 1984 von Charles Bennett und Gilles Brassard entwickelt und stellt das erste Quantenkryptographie-Protokoll dar. Es basiert auf der Übertragung von Qubits, den fundamentalen Informationsträgern in der Quantenmechanik, in zwei verschiedenen Basen: der rectilinearen Basis ($|0\rangle, |1\rangle$) und der diagonalen Basis ($|+\rangle, |-\rangle$). In der rectilinearen Basis entsprechen die Zustände horizontal ($0°$) und vertikal ($90°$) polarisierten Zuständen. Die diagonale Basis repräsentiert Zustände, die diagonal ($45°$) und anti-diagonal ($135°$) polarisiert sind.

Alice wählt zufällig eine dieser beiden Basen aus und sendet Qubits an Bob. Bob misst diese Qubits ebenfalls in einer zufällig gewählten Basis. Wenn die von Alice und Bob gewählten Basen übereinstimmen, können die Ergebnisse der Messungen zur Schlüsselerzeugung verwendet werden.

3.2 Sicherheitsprinzip

Die Sicherheit des BB84-Protokolls basiert auf zwei fundamentalen Prinzipien der Quantenmechanik: dem No-Cloning-Theorem, das besagt, dass ein unbekannter Quantenzustand nicht exakt kopiert werden kann, und der Tatsache, dass jede Messung den Zustand eines Qubits beeinflusst. Wenn ein Abhörer (Eve) versucht, die Informationen abzufangen, führt dies zwangsläufig zu Störungen in den Messwerten, die Alice und Bob erkennen können.

4 Der Analogieversuch

Der Analogieversuch simuliert die Prinzipien der Quantenkryptographie durch die Manipulation von polarisiertem Licht. Anstelle echter Qubits werden Lichtpulse verwendet, deren Polarisationszustände die Quantenbasen nachahmen.

4.1 Aufbau des Versuchs

Der Versuch umfasst drei Hauptkomponenten: den Sender (Alice), der Polarisationsgeneratoren zur Erzeugung von Lichtpulsen in verschiedenen Polarisationszuständen verwendet, den Empfänger (Bob), der die Pulse mit Polarisationsdetektoren in zwei möglichen Messbasen misst, und einen potenziellen Abhörer (Eve), der die Übertragung abhören und dadurch Störungen im System verursachen kann.

4.2 Experimentelle Schritte

Im Verlauf des Experiments sendet Alice Lichtpulse in zufällig gewählten Polarisationszuständen an Bob, der diese Pulse mit einer ebenfalls zufällig gewählten Basis misst. Nach Abschluss der Übertragung teilen Alice und Bob öffentlich die von ihnen verwendeten Basen, ohne die gemessenen Ergebnisse preiszugeben. Nur in den Fällen, in denen ihre Basen übereinstimmen, können die entsprechenden Bitwerte für die Schlüsselerzeugung genutzt werden.

Tabelle 1: Polarisationszustände und ihre Zuordnung

Polarisationswinkel	Basis	Bitwert
0°	Rectilinear	0
90°	Rectilinear	1
45°	Diagonal	0
135°	Diagonal	1

4.3 Erkennung eines Abhörversuchs

Ein Abhörversuch durch Eve verändert den Zustand der Lichtpulse und führt zu Fehlern in den von Bob gemessenen Bitwerten. Da Eve die von Alice verwendete Basis nicht kennt, misst sie die Polarisationszustände in 50 Prozent der Fälle in der falschen Basis. Diese falschen Messungen beeinflussen die ursprünglichen Zustände der Lichtpulse, bevor sie an Bob weitergeleitet werden. Die Konsequenz ist eine erhöhte Fehlerrate in den Messergebnissen von Bob.

Um einen Abhörversuch zu erkennen, teilen Alice und Bob nach der Übertragung eine Teilmenge ihrer Ergebnisse und vergleichen die Übereinstimmung. Unter normalen Bedingungen, also ohne Abhörversuch, liegt die Fehlerquote durch zufällige Einflüsse typischerweise unter 11 Prozent. Wird dieser Wert überschritten, deutet dies auf einen Abhörversuch hin, da die zusätzlichen Fehler durch Eves Eingreifen verursacht werden.

5 Vergleich mit echter Quantenkryptographie

Im Gegensatz zum Analogieversuch basiert die echte Quantenkryptographie auf der Übertragung von echten Qubits, die häufig durch einzelne Photonen realisiert werden. Solche Photonen werden durch spezialisierte Geräte wie verschränkte Photonengeneratoren erzeugt und durch hochempfindliche Detektoren gemessen.

Die echte Quantenkryptographie bietet unbedingte Sicherheit, da kein Abhörversuch unentdeckt bleibt. Die Sicherheitsgarantie basiert dabei nicht auf mathematischen Annahmen, sondern auf den fundamentalen Naturgesetzen der Quantenmechanik. Allerdings gibt es auch praktische Herausforderungen, wie etwa die Schwierigkeit, einzelne Photonen über große Distanzen zu übertragen, oder die technologische Komplexität der notwendigen Geräte.

6 Zusammenfassung

Der Analogieversuch zur Quantenkryptographie ist eine wertvolle Methode, um die Prinzipien der Quantenkommunikation und die Funktionsweise des BB84-Protokolls anschaulich darzustellen. Durch die Verwendung von polarisiertem Licht können wesentliche Konzepte wie Schlüsselerzeugung und die Entdeckung von Abhörversuchen demonstriert werden. Gleichzeitig bleibt die echte Quantenkryptographie mit ihrer unbedingten Sicherheit und ihren technologischen Herausforderungen ein hochaktuelles und faszinierendes Forschungsfeld.

7 Justieren

8 Aufbau

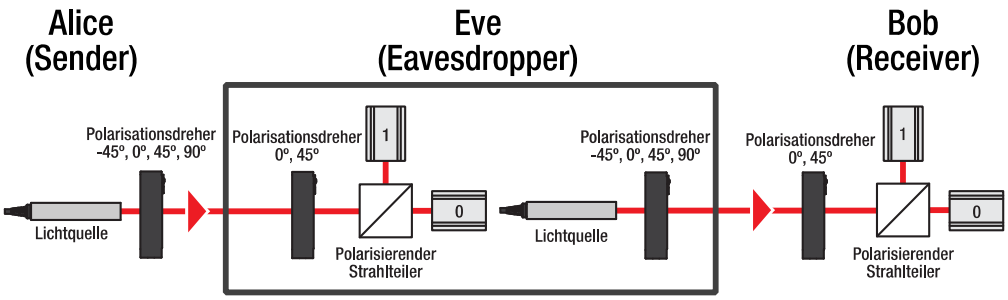

Abbildung 1: . [1]

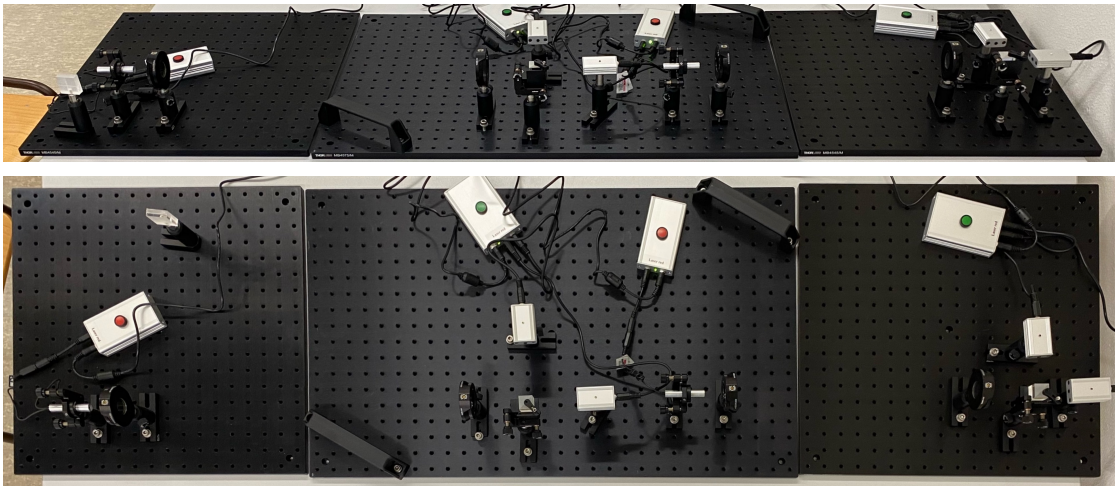

Abbildung 2: .

9 Verfahren

9.1 Verschlüsselung einer Nachricht

9.2 Identifikation eines Abhörversuchs

10 Auswertung

10.1 Verschlüsselung einer Nachricht

Tabelle 2: .

	Alice			Bob	
Messung	Basis	Gesendet	Einstellung	Basis	Empfangen
1	×	0	−45°	+	0
2	×	0	−45°	+	0
3	×	0	−45°	×	0
4	+	1	90°	+	1
5	+	0	0°	×	0
6	×	0	−45°	×	0
7	+	1	90°	+	1
8	+	0	0°	×	0
9	+	1	90°	+	1
10	+	1	90°	+	1
11	×	0	−45°	+	0
12	+	0	0°	+	0
13	×	0	−45°	×	0
14	+	1	90°	×	0
15	×	1	45°	+	0
16	+	1	90°	×	1
17	×	1	45°	×	1
18	×	0	−45°	+	1
19	×	1	45°	+	0
20	+	1	90°	×	0
21	×	0	−45°	×	0
22	+	0	0°	×	1
23	+	1	90°	×	0
24	×	1	45°	×	1
25	×	1	45°	+	0
26	×	0	−45°	+	1
27	×	1	45°	+	1
28	×	0	−45°	×	0
29	×	0	−45°	×	0
30	×	1	45°	×	1
31	×	1	45°	×	1
32	×	0	−45°	+	1
33	+	1	90°	+	1
34	×	1	45°	+	1
35	×	1	45°	+	1
36	+	1	90°	×	1
37	×	0	−45°	×	0
38	+	1	90°	×	0
39	×	0	−45°	×	0

40	×	0	−45°	+	1
41	+	1	90°	×	1
42	+	0	0°	+	0
43	+	1	90°	+	1
44	×	0	−45°	+	0
45	+	0	0°	+	0
46	×	0	−45°	+	0
47	+	1	90°	×	1
48	×	0	−45°	+	1
49	×	1	45°	×	1
50	+	1	90°	+	1
51	+	0	0°	×	0
52	×	1	45°	+	0

10.2 Identifikation eines Abhörversuchs

Tabelle 3: .

	Alice			Eve	Bob	
Messung	Basis	Gesendet	Einstellung	Basis	Basis	Empfangen
1	×	0	−45°		+	0
2	×	0	−45°		+	0
3	×	0	−45°		×	0
4	+	1	90°		+	1
5	+	0	0°		×	0
6	×	0	−45°		×	0
7	+	1	90°		+	1
8	+	0	0°		×	0
9	+	1	90°		+	1
10	+	1	90°		+	1
11	×	0	−45°		+	0
12	+	0	0°		+	0
13	×	0	−45°		×	0
14	+	1	90°		×	0
15	×	1	45°		+	0
16	+	1	90°		×	1
17	×	1	45°		×	1
18	×	0	−45°		+	1
19	×	1	45°		+	0
20	+	1	90°		×	0
21	×	0	−45°		×	0
22	+	0	0°		×	1

23	+	1	90°	×	0
24	×	1	45°	×	1
25	×	1	45°	+	0
26	×	0	−45°	+	1
27	×	1	45°	+	1
28	×	0	−45°	×	0
29	×	0	−45°	×	0
30	×	1	45°	×	1
31	×	1	45°	×	1
32	×	0	−45°	+	1
33	+	1	90°	+	1
34	×	1	45°	+	1
35	×	1	45°	+	1
36	+	1	90°	×	1
37	×	0	−45°	×	0
38	+	1	90°	×	0
39	×	0	−45°	×	0
40	×	0	−45°	+	1
41	+	1	90°	×	1
42	+	0	0°	+	0
43	+	1	90°	+	1
44	×	0	−45°	+	0
45	+	0	0°	+	0
46	×	0	−45°	+	0
47	+	1	90°	×	1
48	×	0	−45°	+	1
49	×	1	45°	×	1
50	+	1	90°	+	1
51	+	0	0°	×	0
52	×	1	45°	+	0

11 Diskussion

Literatur

[1] *EDU-QCRY1/M Quantenkryptografie - Analogieversuch. Handbuch.* Thorlabs GmbH. 2020. URL: `https://www.thorlabs.com/thorproduct.cfm?partnumber=EDU-QCRY1/M`.