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.

2.1 Grundlagen der Quantenkryptographie

2.1.1 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 +-Basis ($|0\rangle, |1\rangle$) und der X-Basis ($|+\rangle, |-\rangle$). In der +-Basis entsprechen die Zustände horizontal (0°) und vertikal (90°) polarisierten Zuständen. Die diagonale Basis repräsentiert Zustände, die diagonal (-45°) und anti-diagonal (45°) 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.

2.1.2 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.

2.2 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.

2.2.1 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.

2.2.2 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°	+	0
90°	+	1
-45°	X	0
$+45^\circ$	X	1

2.2.3 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.

2.2.4 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.

2.3 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.

3 Durchführung

Im Folgenden werden die in [1] beschriebenen Schritte durchgeführt und dokumentiert. Die gestellten Komponenten liegen zunächst als Einzelteile vor und umfassen eine in [2] beschriebene modifizierte Version des Versuchs. Neben denselben Komponenten für rotes Licht sind darin zusätzlich zwei grüne Laser und vier weitere Sensormodule mit den zugehörigen Elektroniken enthalten. Außerdem umfasst es zwei Strahlteilerwürfel, vier für die kürzere Wellenlänge optimierte Halbwellenplatten sowie vier dichriotische Spiegel zur Parallelstellung der grünen und roten Laserstrahlen. Damit lassen sich nun doppelt so viele Polarisationszustände übertragen, statt binärer können ternäre oder quartäre Zustände gewählt werden, die in einem Puls mehr Informationen enthalten. Indem Täuschzustände definiert werden, die von den normalen Parteien nicht verwendet werden aber durch die notwendige Messung eines Lauschers unbeabsichtigt auftreten können, lässt sich ein Abhörversuch identifizieren, ohne Schlüsselbits zu opfern.

Auf diese Ergänzung wird hier verzichtet, es kommen also nur zwei rote Laser mit ihren Elektroniken, vier Detektoreinheiten von denen je zwei an eine Elektronik angeschlossen werden, vier Halbwellenplatten für rotes Licht, sowie zwei polarisierende Strahlteiler vor. Diese werden nach den Anweisungen aus [1] zur Montage auf den Steckbrettern in den entsprechenden Halterungen montiert und stets so verbaut, dass ausreichend Platz für eine zukünftige Erweiterung um den vollständigen Aufbau gegeben ist. Von Werk aus sind die Laser vermessen und alle Netzteile stabilisiert.

3.1 Justierung

Zunächst wird die ebene Ausrichtung der beiden Laser justiert. Dabei hilft eine Justierhilfe, die zur Anzeige des Strahls in geringer und großer Entfernung genutzt werden kann. Der Laserpunkt sollte die Skala abstandsunabhängig in der gleichen Höhe treffen. Ist dies erfolgt wird weiter die bevorzugte Polarisationsrichtung der Laser parallel zur Brettebene eingestellt. Dazu wird ein Strahlteiler mit korrekter Orientierung in den senkrecht zu ihm verlaufenden Strahlengang gebracht und der reflektierte Teil auf einen Schirm geworfen. Nun kann der Laser in seiner Halterung solange um die Strahlachse gedreht werden, bis die abgebildete senkrecht polarisierte Intensität minimal wird. In dieser Orientierung werden die Laser dann befestigt. Auf ähnliche Weise wird die Richtung der Halbwellenplatten überprüft. Es wird je eine Polarisatorplatte zwischen Laser und Strahlteilerwürfel positioniert, die Drehskala gelöst und solange rotiert, bis die reflektierte Intensität das Minimum erreicht. Diese Einstellung muss dann wieder fixiert werden, bevor die Winkelanzeige ausgeschraubt und auf die Nullstelle gestellt wieder eingebaut wird. Die Polarisatoren sind also in plattenparalleler Ausrichtung genullt, alle Komponenten sind somit einsatzbereit.

3.2 Aufbau

Nachdem die vorherigen Voraussetzungen erfüllt sind, kann der eigentliche Messaufbau eingerichtet werden. Das erfolgt nach dem in Abbildung 1 gezeigten Schema. Wie zuvor werden die Laser dafür zu Beginn in den Dauerbetrieb versetzt. Ohne verbaute Strahlteiler muss der transmittierte Anteil senkrecht auf den der Null entsprechenden Sensor fallen. Anschließend wird der Strahlteiler eingesetzt und an den Stellschrauben senkrecht zum Strahl gestellt, indem überprüft wird, ob der Laser weiterhin den Detektor trifft. Weiter wird der Sensor, welcher der Eins entspricht, so ausgerichtet, dass der reflektierte Strahl orthogonal auf dem Detektor steht. Um abschließend die korrekte Funktionsweise zu verifizieren, werden die Laser per Knopfdruck in den Pulsbetrieb und die Sensoren auf Justierbetrieb geschaltet. Nun gilt es alle in Tabelle 2 eingetragenen Möglichkeiten der Polarisationsdreher auf die richtige Leuchtkombination zu testen.

Tabelle 2: Unterschiedliche Fälle der Halbwellenplattenorientierung mit geforderten Leuchtanzeigen. Zum Vergleich sind auch die zugehörigen empfangenen Bits angegeben, die dann durch ein einzelnes Leuchten des jeweiligen Sensors im Normalbetrieb angezeigt werden.

Sender	Empfänger	Leuchten	Bit
−45°	0°	beide	Zufall
0°	0°	transmittiert	Null
45°	0°	beide	Zufall
90°	0°	reflektiert	Eins
−45°	45°	transmittiert	Null
0°	45°	beide	Zufall
45°	45°	reflektiert	Eins
90°	45°	beide	Zufall

Die darin beschriebene Übersetzung definiert für 0° die „+“ und für 45° die „×“ Basis. Eine übereinstimmende Basiswahl liefert dann ein eindeutiges „0“ oder „1“ Ergebnis, während abweichende Basen zufällige Bits ergeben. Im Fall einzelner Photonen wäre dies quantenmechanisch garantiert, für die hier verwendeten Laserpulse sorgt bei ähnlicher Intensität die Schaltung für eine Zufallswahl.

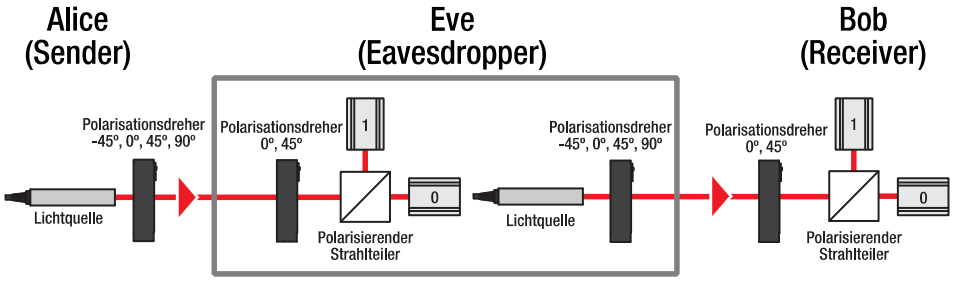

Abbildung 1: Schematischer Aufbau des Quantenkryptografie Analogieversuchs. [1]

Das beschriebene Vorgehen wird zunächst ohne „Eve“ nur für „Alice“ als Sender und „Bob“ als Empfänger ausgeführt. Nach Aufnahme der ersten Messreihe kann „Eve“ eingesetzt werden und wird dann sowohl für die Rolle des Senders als auch des Empfängers kalibriert. Dabei sollte eine veränderte Einstellung von „Alice“ und „Bob“ vermieden werden, um die Absicht eines zunächst unbemerkten Lauschers zu simulieren, der dann mittels der zweiten Messreihe enttarnt wird. Wie in Abbildung 2 zu sehen ist, kann die Steckplatte mit „Eve“ an zwei Griffen aus dem Aufbau gehoben werden, ohne „Alice“ und „Bob“ zu stören. An dieser Stelle sei noch angemerkt, dass ein unbemerkter Lauschangriff auf Lichtimpulse statt einzelne Photonen prinzipiell leicht zu realisieren ist, indem mithilfe eines passenden Strahlteilers nur ein geringer Anteil des Strahls abgezweigt würde. Die vorliegende Umsetzung dient als Analgie zum Abhören von Quanten, welche ohne Änderung kopiert werden müssten. Ein solches Klonen ist physikalisch unmöglich, da dabei der initiale Zustand geändert wird.

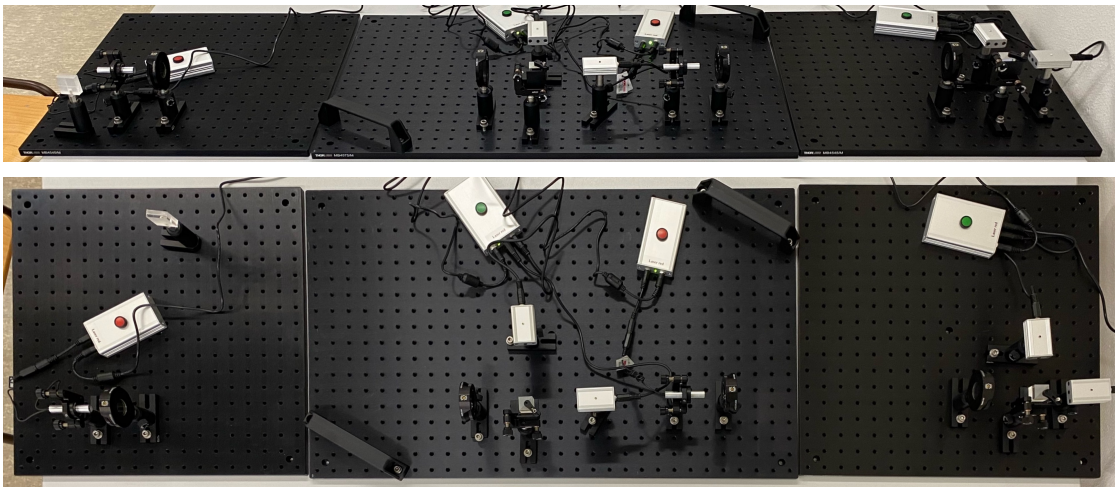

Abbildung 2: Vollständiger Aufbau des Quantenkryptografie Analogieversuchs.

3.3 Verfahren

Nach abgeschlossener Justierung und vollständigem Aufbau können nun die verschlüsselte Übertragung einer Nachricht sowie das Testen auf einen Abhörer implementiert werden.

3.3.1 Verschlüsselung einer Nachricht

Für „Alice“ und „Bob“ werden je 52 zufällige Basiseinstellungen sowie für „Alice“ weitere 52 willkürliche Bits generiert. Hier passiert dies über Pseudozufallszahlen, wogegen im Idealfall echter Zufall aus quantenmechanischen Prozessen wie Zerfall oder Transmission extrahiert würde. Die Anzahl der Messungen wird auf 52 festgelegt, um mit ausreichend hoher Sicherheit 20 Schlüsselbits zu erhalten und 4 Zeichen durch 5 Bits zu senden.

Unter den festgelegten Basen sendet „Alice“ nun die zufälligen Bits, „Bob“ empfängt die resultierenden Signale. Im Anschluss tauschen sich „Alice“ und „Bob“ öffentlich über ihre jeweilige Basiswahl aus, halten dabei aber die gesendeten oder empfangenen Bitwerte geheim. Bei übereinstimmenden Basen werden die ersten 20 dieser Bits in der gegebenen Reihenfolge als Schlüssel definiert. „Alice“ kodiert nun ihre Nachricht in Binärform und verschlüsselt diese durch binäre Addition der Schlüsselsequenz. Gleiche Ziffern ergeben „0“ und verschiedene „1“ als somit ebenfalls zufälliges Signal, das nun in einer gemeinsam bekannten Basis versendet wird. „Bob“ dechiffriert die Nachricht durch erneute Addition des von ihm unabhängig gefundenen Schlüssels und erhält so den Text zurück.

3.3.2 Identifikation eines Abhörversuchs

Um einen Lauscher zu erkennen werden zunächst analog generierte Signale zwischen „Alice“ und „Bob“ ausgetauscht. Allerdings ist dazwischen „Eve“ geschaltet, die ebenfalls 52 zufällige Basen einstellt und ihre Messung in eben dieser weitergibt. Ist dies erfolgt, informieren sich „Alice“ und „Bob“ wieder über die gemeinsamen Basen, übermitteln für diese aber ebenfalls die gesendeten und gemessenen Bitwerte öffentlich. Hatte nun „Eve“ eine abweichende Basis, kann durch Zufall ein falscher Wert bei „Bob“ ankommen, obwohl er dieselbe Basis wie „Alice“ einstellt. Daran lässt sich unter Annahme statistischer Signifikanz ein Abhörversuch klar identifizieren. In realen Anwendungen würden die Schritte des Abhörtests und der verschlüsselten Übertragung in umgekehrter Reihenfolge durchgeführt werden.

4 Auswertung

$$f(k, n, p) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

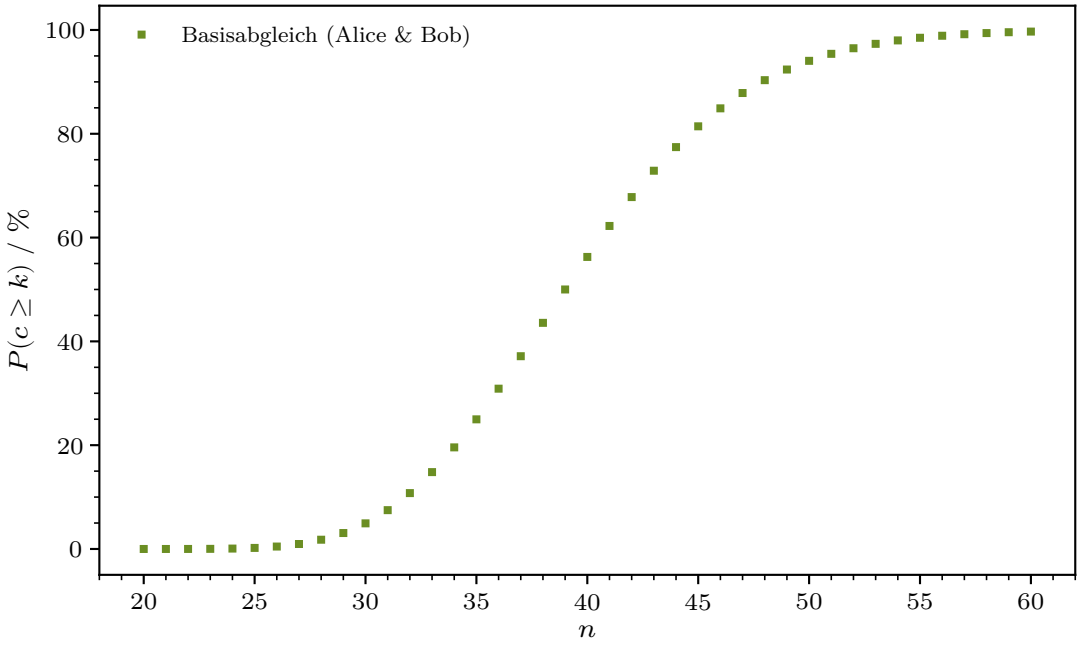

Abbildung 3: .

96,48 %

4.1 Verschlüsselung einer Nachricht

Tabelle 3: .

	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

7,84 %

Tabelle 4: .

Buchstabe:	T	E	S	T
Kodierung:	1 0 0 1 1	0 0 1 0 0	1 0 0 1 0	1 0 0 1 1
Schlüssel:	0 1 0 1 1	1 0 0 1 0	1 0 0 1 1	1 0 0 0 1
Nachricht:	1 1 0 0 0	1 0 1 1 0	0 0 0 0 1	0 0 0 1 0

Tabelle 5: .

Nachricht:	1 1 0 0 0	1 0 1 1 0	0 0 0 0 1	0 0 0 1 0
Schlüssel:	0 1 0 1 1	1 0 0 1 0	1 0 0 1 1	1 0 0 0 1
Kodierung:	1 0 0 1 1	0 0 1 0 0	1 0 0 1 0	1 0 0 1 1
Buchstabe:	T	E	S	T

4.2 Identifikation eines Abhörversuchs

Tabelle 6: .

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

19	+	0	0°	×	×	1
20	+	1	90°	×	×	1
21	×	0	−45°	×	+	0
22	+	0	0°	+	×	0
23	×	1	45°	+	+	1
24	+	1	90°	+	×	0
25	×	1	45°	×	×	1
26	×	0	−45°	+	+	1
27	×	0	−45°	+	×	0
28	+	1	90°	+	×	0
29	×	0	−45°	+	+	1
30	+	0	0°	+	×	0
31	+	0	0°	+	+	0
32	+	1	90°	+	+	1
33	+	1	90°	+	×	0
34	+	1	90°	×	+	0
35	×	1	45°	+	+	1
36	×	0	−45°	×	×	0
37	×	1	45°	×	+	1
38	+	1	90°	×	+	1
39	×	1	45°	×	×	1
40	×	0	−45°	+	+	1
41	+	0	0°	+	+	0
42	×	1	45°	×	×	1
43	+	1	90°	×	×	0
44	+	0	0°	×	×	1
45	×	0	−45°	×	×	0
46	+	0	0°	×	+	0
47	+	1	90°	×	×	1
48	×	0	−45°	+	×	1
49	×	1	45°	+	×	1
50	+	1	90°	×	×	0
51	+	0	0°	+	×	1
52	+	1	90°	×	×	1

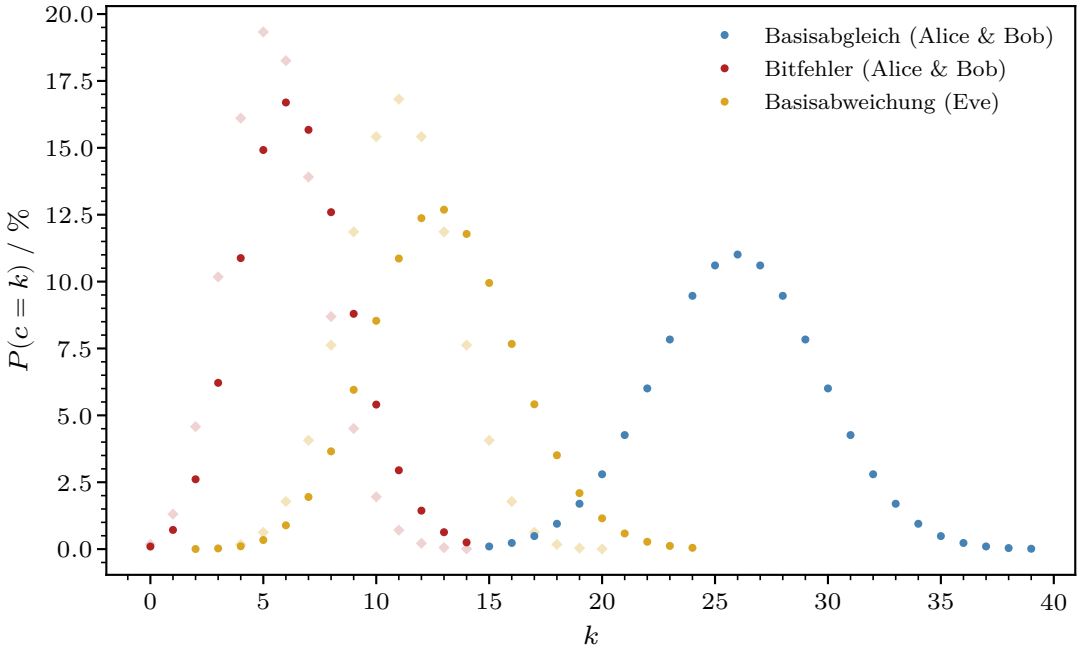

Abbildung 4: .

6,01 %

10,86 %

10,88 %

16,82 %

16,11 %

5 Diskussion

Literatur

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

[2] Brit Riggs u. a. „Multi-Wavelength Quantum Key Distribution Emulation with Physical Unclonable Function“. In: *Cryptography* 6.3 (2022). ISSN: 2410-387X. DOI: 10.3390/cryptography6030036. URL: https://www.mdpi.com/2410-387X/6/3/36.