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 Theorie

Kryptografie befasst sich mit der Verschlüsselung von Daten, sodass nur Sender und Empfänger die Nachricht lesen können. Die Sicherheit basiert entweder auf komplexen Algorithmen oder praktischen Hindernissen wie der Faktorisierung großer Zahlen. Klassische Verfahren sind jedoch nie absolut sicher, da Schlüssel geknackt werden können. Mithilfe der Quantenphysik lässt sich dieses Problem lösen, indem ein zufälliger Schlüssel generiert wird, der nur Sender und Empfänger bekannt ist. Abhörversuche werden dabei grundsätzlich erkannt.

2.1 One-Time Pad

Das One-Time Pad ist ein Schlüsselverfahren mit einem zufällig generierten schlüssel aus bits, welcher auf die zu verschlüsselnde Nachricht addiert werden soll. Hierbei sind die gelten die Regeln

$$\begin{aligned} 0+0&=0\\ 1+0&=1\\ 0+1&=1\\ 1+1&=0\,. \end{aligned}$$

Falls ein Abhörversuch stattfindet, kann die Nachricht also nur entschlüsselt werden, wenn der zufällig gewählte Schlüssel bekannt ist. Die Voraussetzungen für die Sicherheit des Verfahrens sind

1. Die Länge des Schlüssels entspricht der Nachrichten Länge,
2. Einmalige Verwendung eines Schlüssels,
3. Komplett zufällige Wahl des Schlüssels,
4. Schlüssel darf nur dem Sender und Empfänger bekannt sein.

Punkt 3 und 4 sind im klassischen Sinn schwierig umzusetzen, da klassische Zufallszahlen bei genauer Betrachtung nur pseudozufällig als Ergebnis eines Algorithmus sind und die Übermittlung eines Schlüssels prinzipiell auch Abgefangen werden könnte. Diese Probleme können durch die Quantenmechanik gelöst werden.

2.2 Erstellung eines Schlüssels

Für die Erstellung eines Schlüssels ist es nötig vorab die Darstellung der Bits zu diskutieren. Hierzu wird der Sender, der im Folgenden Alice genannt wird genutzt. ALice möchte eine verschlüsselte Nachricht an den Empfänger Bob senden. Hierzu müssen die Bits übertragen werden. Grundsätzlich beinhaltet die Wahl des Bits nur ob das gesendete Photon horizontal ("0") oder vertikal polarisiert ("1") polarisiert ist. Die Polarisationsrichtung wird über die Verwendung einer $\lambda/2$-Platte realisiert. Eine $\lambda/2$-Platte ist ein optisches Element aus einem doppelbrechenden Material, das dazu dient, die Polarisationsrichtung von Licht gezielt zu drehen. Die Funktion basiert auf der Eigenschaft der Doppelbrechung, bei der Licht in zwei Komponenten, die schnelle Achse und die langsame Achse, aufgeteilt wird, die unterschiedlich schnell durch das Material laufen. Licht, das entlang der schnellen Achse polarisiert ist, bewegt sich schneller, während Licht, das entlang der langsamen Achse polarisiert ist, verlangsamt wird. Der Unterschied in der Geschwindigkeit führt zu einer Phasenverschiebung zwischen den beiden Lichtkomponenten. Für eine $\lambda/2$-Platte beträgt die Phasenverschiebung genau eine halbe Wellenlänge, also 180°. Wenn linear polarisiertes Licht in die $\lambda/2$-Platte eintritt, wird die Polarisationsebene um einen Winkel gedreht, der doppelt so groß ist wie der Drehwinkel der Platte relativ zur ursprünglichen Polarisationsrichtung.

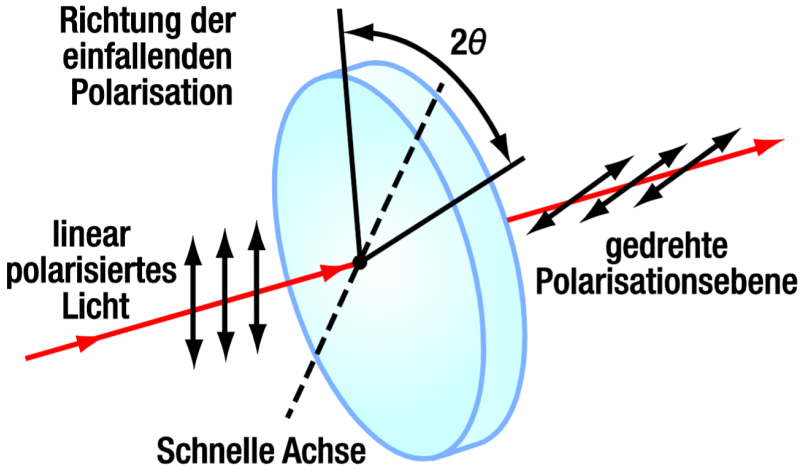

Abbildung 1: Schematische Darstellung der Funktionsweise eines $\lambda/2$-Plättchen. [1]

Eine schematische Darstellung der Funktionsweise einer $\lambda/2$-Platte ist in Abbildung 1 dargestellt. Bob kann die Polarisationsrichtung unterscheiden, indem vor den verwendeten Detektoren (siehe Unterabschnitt 3.2) einen polarisierenden Strahlteiler verwendet, welcher in Abbildung 2 gezeigt ist.

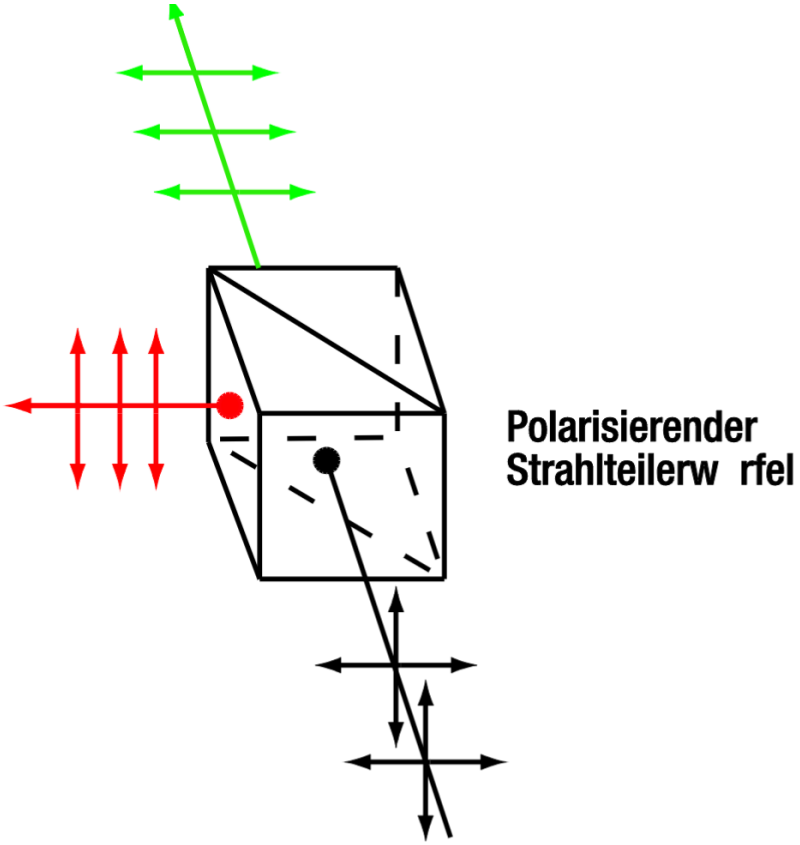

Abbildung 2: Darstellung eines polarisierenden Strahlteilers. [1]

Ein polarisierender Strahlteilerwürfel ist ein optisches Element, das Licht in zwei verschiedene Richtungen aufteilt, basierend auf dessen Polarisation. Er besteht aus zwei Glasprismen, die an ihrer gemeinsamen Grenzfläche durch eine spezielle, teildurchlässige Beschichtung verbunden sind. Diese Beschichtung ist so gestaltet, dass sie unterschiedlich auf die beiden Polarisationskomponenten des Lichts reagiert.

Die Trennung der Polarisationskomponenten entsteht durch die gezielte Interferenz an der dielektrischen Beschichtung. Diese Beschichtung weist für s-polarisiertes Licht (senkrecht zur Einfallsebene polarisiert) einen hohen Reflexionsgrad auf, wodurch der s-polarisierte Anteil an der Grenzfläche reflektiert wird. Im Gegensatz dazu wird p-polarisiertes Licht (parallel zur Einfallsebene polarisiert) nahezu vollständig durch die Beschichtung hindurchgelassen und setzt seinen Weg im Würfel fort.

Dadurch werden die beiden Polarisationskomponenten räumlich voneinander getrennt. Der s-polarisierte Anteil verlässt den Würfel in einem Winkel, typischerweise 90◦ zur Einfallsrichtung, während der p-polarisierte Anteil geradlinig durch den Würfel austritt. Der Transmissionsfall wird von Bob als ”0”gezählt, während die Reflexion eine ”1”darstellt.

Im Umkehrschluss bedeutet das aber, dass es nicht möglich ist einen Schlüssel indirekt zu übertragen. Um das problem zu Lösen, wir der Begriff Basis eingeführt, der es effektiv ermöglicht eine weitere Darstellung der Bits zu verwenden. Das heißt, dass die Bits der Nachricht wie folgt gesendet werden können.

Tabelle 1: Zuordnung der Bitwerte zu den Basen und Einstellungen

Basis	**Bitwert**	**Einstellung**
+ (rectilinear)	0	0°
+ (rectilinear)	1	90°
x (diagonal)	0	−45°
x (diagonal)	1	45°

Neben der Wahl des Bits, muss Alice also noch die Basis festlegen, in der gesendet wird. Bob muss nur zwischen den beiden Basen Wählen. Wenn sowohl Alice als auch Bob die gleiche Basis gewählt haben, erhält Bob den richtigen Bit. Falls die falsche Basis gewählt wurde, wird die Hälfte des Lichtes transmittiert und die andere abgelenkt. Die Ablenkung der Hälfte entsteht dadurch, dass die Bits in den einzelnen Basen zu 45◦ verschoben sind. Welche Bits wann empfangen werden, ist in Abbildung 3 übersichtlich gezeigt.

Alice			Bob				Basen
Basis	Bit	=> Winkel	Basis	Winkel	Detektor „0“	Detektor „1“	gleich?
+	0	0°	+	0°	**100%**	0%	Ja
+	1	90°	+	0°	0%	**100%**	Ja
x	1	45°	+	0°	50%	50%	Nein
x	0	-45°	+	0°	50%	50%	Nein
+	0	0°	x	45°	50%	50%	Nein
+	1	90°	x	45°	50%	50%	Nein
x	1	45°	x	45°	0%	**100%**	Ja
x	0	-45°	x	45°	**100%**	0%	Ja

Abbildung 3: Darstellung des gemessenen Bits in Abhängigkeit der Basis und gesendeten Bits. [1]

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 4 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.

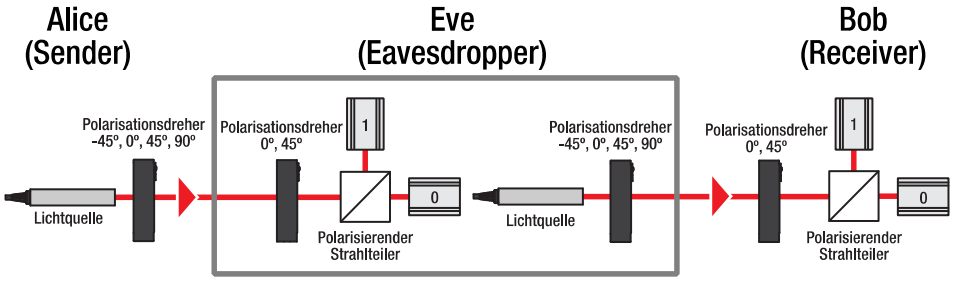

Abbildung 4: Schematischer Aufbau des Quantenkryptografie Analogieversuchs. [1]

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 5 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.

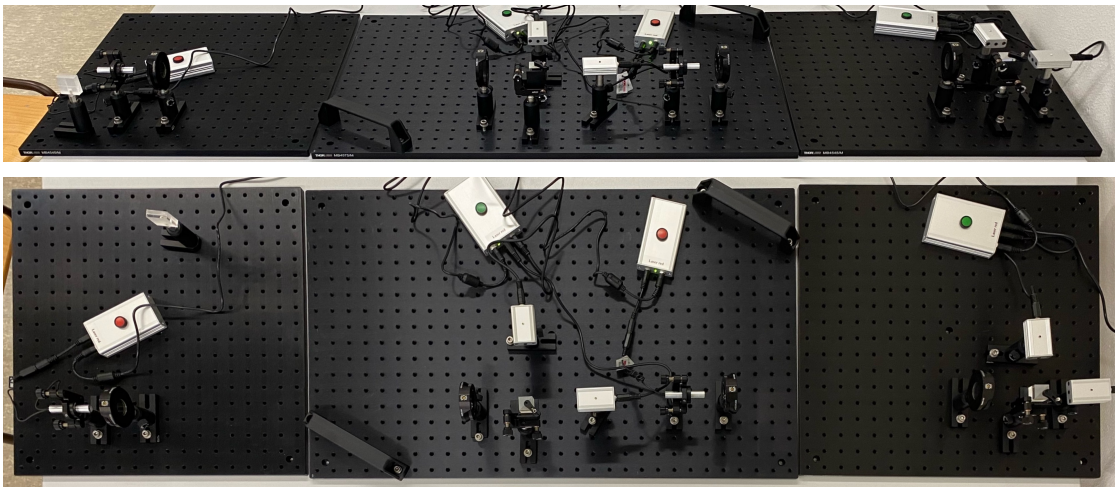

Abbildung 5: Vollständiger Aufbau des Quantenkryptografie Analogieversuchs.

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.

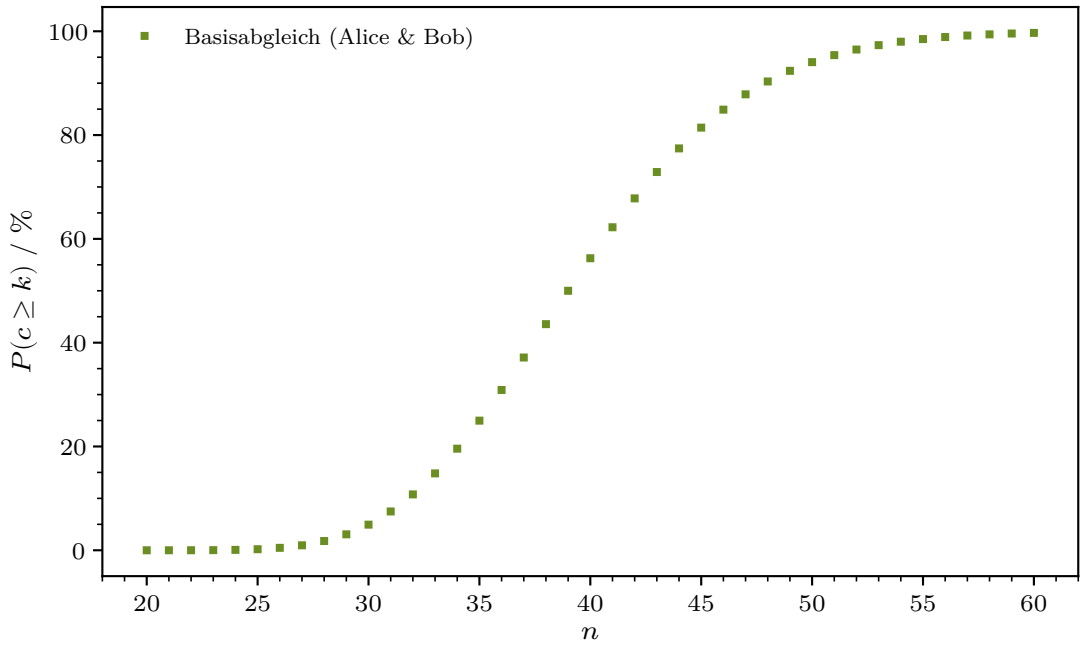

Abbildung 6: Kumulierte Verteilung für das Auftreten von mindestens $k = 20$ passenden Basispaaren mit $p = 50\,\%$ in n Messungen zur Schlüsselgeneration.

4 Auswertung

Als Serie gleichartiger und unabhängiger Events lassen sich die Wahrscheinlichkeiten für das Eintreten der verschiedenen Fälle in diesem Versuch mithilfe der Binomialverteilung

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

bestimmen. Daraus folgt auch die in Abbildung 6 aufgetragene kumulierte Verteilung

$$P(c \geq k) = F(k, n, p) = \sum_{m=k}^{n} f(m, n, p)$$

für das Auftreten von k oder mehr Ereignissen mit Einzelwahrscheinlichkeit p aus den insgesamt n diskreten Messungen. Das zufällige Eintreten gleicher Basen hat $p = 50\,\%$ und tritt bei den empfohlenen $n = 52$ Signalen in 96,48 % der Fälle ausreichend oft für die geforderte Schlüssellänge $k = 20$ auf.

4.1 Verschlüsselung einer Nachricht

Wie zuvor beschrieben wird nun das Vorgehen zur Erzeugung eines zufälligen Schlüssels in Tabelle 3 implementiert. Zur Veranschaulichung sind gleiche Basiseinstellungen farblich hervorgehoben und die Polarisationsdrehplattenpositionen von „Alice“ angegeben.

Tabelle 3: Dokumentation des Signalaustauschs zur Erzeugung einer Verschlüsselung. Übereinstimmende Basen sind blau hinterlegt. Zum besseren Verständnis sind zudem Winkeleinstellungen für die unterschiedlichen Kombinationen von Basis und Bit eingetragen.

	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

Bei dieser Messreihe stimmen die Basen in 23 Fällen überein. Dieser Anzahl kann eine Wahrscheinlichkeit von 7,84 % zugeordnet werden, was nach Vergleich mit Abbildung 7 relativ nah am Maximum der Verteilung und somit dem Erwartungswert liegt. Es folgt

$$0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1$$

als unabhängig von „Alice“ und „Bob“ bekannte Sequenz, deren erste 20 Stellen nun für den Schlüssel festgelegt werden.

Tabelle 4: Vorgehen von „Alice“ zum Senden der Nachricht `TEST`.

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: Vorgehen von „Bob“ zum Empfangen der Nachricht `TEST`.

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

Das Vorgehen zur Verschlüsselung durch Addition, zum Versenden der sicheren Nachricht, und dem abschließenden Entschlüsseln sind in Tabelle 4 für „Alice“ und Tabelle 5 für „Bob“ so nachgehalten, wie die einzelnen Schritte an der Apparatur ausgeführt werden. Dies ist offensichtlich erfolgreich, der gewählte Text `TEST` wird ohne Fehler übertragen.

4.2 Identifikation eines Abhörversuchs

Weiter wird „Eve“ verbaut, um das vorher eingeführte Verfahren zum Prüfen auf einen Lauscher zu erproben. Die einzelnen Messungen werden wie zuvor in Tabelle 6 protokolliert, wobei die Basis von „Eve“ zum Vergleich mitegeführt wird. Im realen Fall wäre diese „Alice“ und „Bob“ natürlich nicht bekannt. Es werden dann alle übereinstimmenden Einstellungen von „Alice“ und „Bob“ auf gesondert markierte Bitfehler untersucht, wobei auch die Basis von „Eve“ im Falle einer Abweichung von „Alice“ und „Bob“ hervorgehoben ist. Aus der gesamten Messreihe hat das Ereignis

$$\mathrm{Basis}_{\mathrm{Alice}} = \mathrm{Basis}_{\mathrm{Bob}} \neq \mathrm{Basis}_{\mathrm{Eve}}$$

eine Wahrscheinlichkeit von $p = 25\,\%$ und es gilt demnach $p = 12{,}5\,\%$ für ein in diesem Fall fehlerhaft übertragenes Bit.

Tabelle 6: Dokumentation des Signalaustauschs zur Untersuchung auf einen Lauscher. Übereinstimmende Basen von „Alice“ und „Bob“ sind blau hinterlegt. In diesem Fall korrekt übertragene Bits sind grün und falsche rot markiert. Zur Untersuchung der Fehlerrate ist es zusätzlich sinnvoll, Abweichungen von „Eve“ zu gleicher Basiswahl von „Alice“ und „Bob“ gelb hervorzuheben.

	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

Es werden hier 22 gleiche Basen von „Alice“ und „Bob“ eingestellt. In 11 Fällen weicht „Eve“ davon ab, wodurch insgesamt 4 Bitfehler zwischen „Alice“ und „Bob“ entstehen.

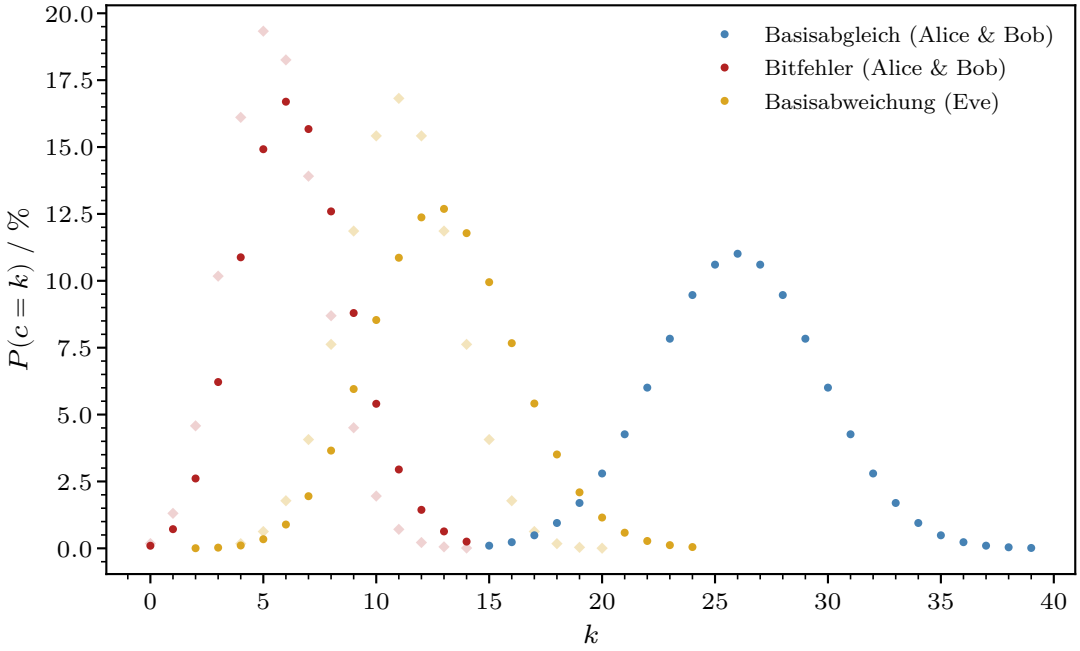

Abbildung 7: Verteilungen für den Basisabgleich mit $p = 50\,\%$ sowie dabei auftretende Abweichungen der Abhörbasis mit $p = 25\,\%$ und des übertragenen Bits mit $p = 12{,}5\,\%$ aus $n = 52$ Signalen. Dazu zeigen transparente Punkte die Verteilungen mit der gemessenen Anzahl der gleichen Basen als Vorwissen.

In Abbildung 7 sind die Wahrscheinlichkeitsverteilungen der untersuchten Ereignisse visualisiert. Es ergibt sich 6,01 % für die gemessenen 22 gleichen Basisstellungen. Aus 52 Signalen entsprechen 11 mit 10,86 % einem Fehler von „Eve“ bei übereinstimmenden Basen von „Alice“ und „Bob“. Für 4 Bitfehler gilt 10,88 % als Wahrscheinlichkeit. Wird für die abweichende Lauscherbasis und das inkorrekte Bit stattdessen $n = 22$ aus der Anzahl gleicher Basen von „Alice“ und „Bob“ angesetzt, gelten $p = 50\,\%$ für ersteren und $p = 25\,\%$ für letzteren Fall. Dann folgt 16,82 % für 11 Basisfehler und 16,11 % für 4 Bitfehler. Alle Anzahlen liegen im jeweiligen Bereich der maximalen Wahrscheinlichkeit und sind somit plausible Werte für eine fehlerfreie Durchführung der Messreihen.

5 Diskussion

Zusammenfassend lässt sich das Analogieexperiment als erfolgreich bewerten. Die dazu vorgenommene Justierung der Bauteile läuft ohne große Schwierigkeiten ab, auch die Feineinstellung und Funktionsweise der Apparatur scheint keine besonderen Ansprüche an Genauigkeit zu haben. Dagegen ist zu erwarten, dass eine Implementierung tatsächlicher Quantenkryptographie mit einzelnen photonischen Zuständen deutlich sensibler gegenüber solchen Störeinflüssen wäre.

Bei der Durchführung der Messung selbst tritt ebenfalls nichts Unerwartetes auf. Nach sorgfältigem Testen werden alle Signale den Erwartungen entsprechend übertragen, sodass Nachrichten problemlos versendet werden können. Ein Punkt, der leicht übersehen werden könnte, ist die korrekte Ausrichtung der Halbwellenplatten, deren Skalen immer in Richtung des jeweiligen Lasers oder Detektors zeigen sollten. Ansonsten können gekippte Bits auftreten, obwohl die Basen übereinstimmen.

Anhand der Analyse der Wahrscheinlichkeitsverteilungen wird auch für den Abhörtest klar, dass mit hoher Sicherheit ein Lauscher zwischen den kommunizierenden Parteien verbaut ist. Die dazu aufgenommene Fehlerrate liegt im Bereich der Erwartungswerte und ist dadurch wahrscheinlich nicht auf inkorrekte Anwendung der Apparatur zurückzuführen.

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.