Verschränkung und Quantenverschlüsselung

Das Feld der Quantentechnologie gilt als ein Forschungsbereich mit enormem Potential für revolutionäre technische Entwicklungen. So scheint beispielsweise der Bau von Quantencomputern bereits in greifbarer Nähe: Große Technologiefirmen wie Google oder IBM liefern sich schon jetzt einen Wettlauf in der Entwicklung entsprechender Technologien. Doch im gleichen Maße, in dem die neuen Möglichkeiten des Quantencomputings als reale Zukunftsszenarien betrachtet werden müssen, gewinnen auch andere Bereiche der Quantentechnologien an Relevanz, so etwa im Bereich der Kommunikationstechnik. Die Tatsache, dass Quantencomputer aktuell übliche Verschlüsselungsverfahren potentiell sehr einfach knacken können, macht es erforderlich, alternative Verschlüsselungsmethoden zu nutzen, die ebenfalls auf Prinzipien der Quantenphysik basieren. Die Verfahren zur sogenannten Quantenkryptographie sind zwar technisch aufwändig, aber grundsätzlich abhörsicher und auch bereits technisch umsetzbar.

1 Nachrichtenübertragung - Grundbegriffe

Auch ohne Einbezug von Aspekten der Quantenphysik basiert die Übermittlung von Informationen stets auf physikalischen Grundlagen. Beispielsweise kann dieselbe Information auf vielfältige Weise physikalisch codiert werden. Daher ist es sinnvoll, die Ebene der Physik von der Ebene der codierten Information auch begrifflich klar zu trennen.

1.1 Signale, Information & Bits

Als Signal bezeichnet man in der Nachrichtentechnik eine beliebige physikalische Größe, der durch Konvention von Sender und Empfänger eine Information zugeordnet wird. Prinzipiell können daher alle messbaren physikalischen Größen ein Signal sein, sofern sich ein Sender und ein Empfänger darauf einigen, dieser Größe auf zuvor verabredete Art und Weise Informationen aufzuprägen. Information kann dem Signal nur entnommen werden, wenn Sender und Empfänger sich zuvor auf konkrete Regeln über die Bedeutung bestimmter Signalmuster geeinigt haben.
Bei digitalen Signalen werden in der Regel diskrete Signalwerte genutzt, die im Binärsystem mit der Information ‚Null' und ‚Eins' assoziiert werden. Dies ermöglicht es, den Informationsgehalt einer Folge von Messwerten, die aus einem digitalen Signal gewonnen wurden, zu quantifizieren: Jeder Messwert repräsentiert entweder die Information ‚Null' oder ‚Eins' und stellt damit die

kleinstmögliche Einheit an zu übermittelnder Information dar - ein einzelnes Bit.

1.2 Codierung von Bits in Polarisation

Zur fehlerfreien Übertragung eines Bits ist es entscheidend, dass bei Messung der entsprechenden physikalischen Messgröße durch den Empfänger die Werte ‚Null' und ‚Eins' eindeutig voneinander unterschieden werden können. Bei elektrischen Signalen wird dies durch die Definition von entsprechenden Spannungs-Schwellwerten umgesetzt. Im Falle von Lichtsignalen kann die Polarisationsrichtung auf folgende Weise zur Festlegung der Bitwerte verwendet werden:
Linear polarisiertes Licht, das auf einen Polfilter mit parallel ausgerichteter Transmissionsachse trifft, wird von diesem Polfilter vollständig transmittiert. Ist der Polfilter dagegen um 90° zur Polarisationsrichtung des Lichtes verdreht, wird das Licht vollständig absorbiert. Die Transmissionsachse des Polfilters und die dazu senkrechte Achse definieren so zwei Polarisationsrichtungen, die eindeutig mit den Werten ‚Null' und ‚Eins' assoziiert werden können. Eine Senderin (die im Folgenden den Namen ‚Alice' erhält) kann also mit dem Empfänger (im Folgenden ‚Bob') zwei senkrecht zueinander liegende Raumrichtungen vereinbaren, die die beiden Werte eines Bits repräsentieren. Sendet Alice eine Reihe von Lichtpulsen, kann sie durch Drehung der Polarisationsrichtung für jeden Puls die Richtung bestimmen und so Binärwerte codieren. Bob misst die Polarisationsrichtung des ankommenden Pulses anhand der Intensität und kann so die Bitwerte rekonstruieren. Hierzu kann Bob entweder einen Polarisationsfilter nutzen, den er während der Messung eines Pulses um 90° dreht, oder er verwendet einen polarisierenden Strahlteiler in Kombination mit zwei Fotodioden und erhält so direkt die vollständige Information über das gesendete Bit.
Die Methode funktioniert jedoch nur dann, wenn Alice die Lichtpulse stets nur entlang der beiden abgesprochenen Achsen polarisiert. Andernfalls erhält Bob keine eindeutigen Messwerte und kann keinen eindeutigen Bitwert auslesen.

1.3 Kryptographie

Das Aufprägen von Information auf ein Signal basiert auf einer gemeinsamen Konvention über die Bedeutung bestimmter Messgrößen, z. B. der Zuordnung von Messwerten in einem bestimmten Bereich zu Bitwerten. Damit Kommunikation universell möglich ist, muss auch die zugrundeliegende Konvention universell bekannt sein. Das bedeutet aber auch, dass potentiell jeder aus einem öffentlich gesendeten oder angezapften Signal Informationen entnehmen kann.

Es stellt sich also die Frage, wie man Nachrichten vor dem Zugriff Dritter geschützt übertragen kann. Hierfür gibt es verschiedene denkbare Möglichkeiten. Der vielleicht naheliegendste Weg wäre die Errichtung einer physischen Direktverbindung zwischen den Kommunikationspartnern, sodass das Signal nur schwer abgefangen werden kann (bspw. ein direktes Telefonkabel). Diese Variante ist jedoch technisch extrem aufwändig und sehr unflexibel, was die einbezogenen Kommunikationspartner angeht. Zudem ist sie trotz des nötigen Aufwandes nicht intrinsisch abhörsicher. Schafft es ein Spion, die Leitung anzuzapfen, hat er immer noch unbegrenzten Zugriff auf die übermittelten Daten. Dasselbe gilt für den Ansatz, eine möglichst unkonventionelle Form der Datenübertragung zu wählen (etwa im 21. Jahrhundert mittels Brieftauben zu kommunizieren).
Will man daher einerseits die Vorteile standardisierter Massenkommunikationsmittel nutzen und andererseits private Informationen übermitteln, bleibt als einzige Möglichkeit, die Nachricht selbst zu verschlüsseln. Wird die verschlüsselte Nachricht durch einen Spion abgefangen, kann dieser zwar das physische Signal anhand der universellen Konvention in Bitwerte umsetzen, die so erhaltenen Bitwerte enthalten jedoch keine ihm ersichtliche Information mehr.
Ein solches Vorgehen bietet den Vorteil, dass technisch weiterhin dieselben Kanäle zur Übertragung von Nachrichten genutzt werden können wie bisher, basiert aber auf zwei Voraussetzungen:

- Das Verschlüsselungsverfahren an sich muss so beschaffen sein, dass die Nachricht nicht ohne Schlüssel wieder entschlüsselt werden kann. Im Falle von Binärzahlen existiert ein solches Verschlüsselungsverfahren: Als Schlüssel dient hierbei eine zufällige Bitfolge, die mindestens so lang ist, wie die Nachricht selbst. Auf jedes Bit der Nachricht wird einzeln ein Bit der Zufallsfolge binär addiert. Das Ergebnis ist eine reine Zufallszahl, die keinerlei Informationen enthält (Abb. 1). Durch erneute Addition des Schlüssels kann die ursprüngliche Bitfolge zurückgewonnen werden. Da die Entschlüsselung nur anhand der Zufalls-Bitfolge möglich ist, hängt die Sicherheit des Verfahrens an der Sicherheit des Schlüssels. Damit ergeben sich die folgenden Bedingungen:

- Die Bitfolge muss absolut zufällig sein. Andernfalls ergeben sich statistisch auswertbare Muster, die zur Rekonstruktion des Schlüssels führen können.

- Jeder Schlüssel darf nur einmal verwendet werden (das sogenannte ‚One-Time-Pad'-Verfahren). Andernfalls kann ebenfalls mit statistischen Methoden auf den schlüssel rückgeschlossen werden.

- Der Schlüssel selbst darf für Spione nicht zugänglich sein.

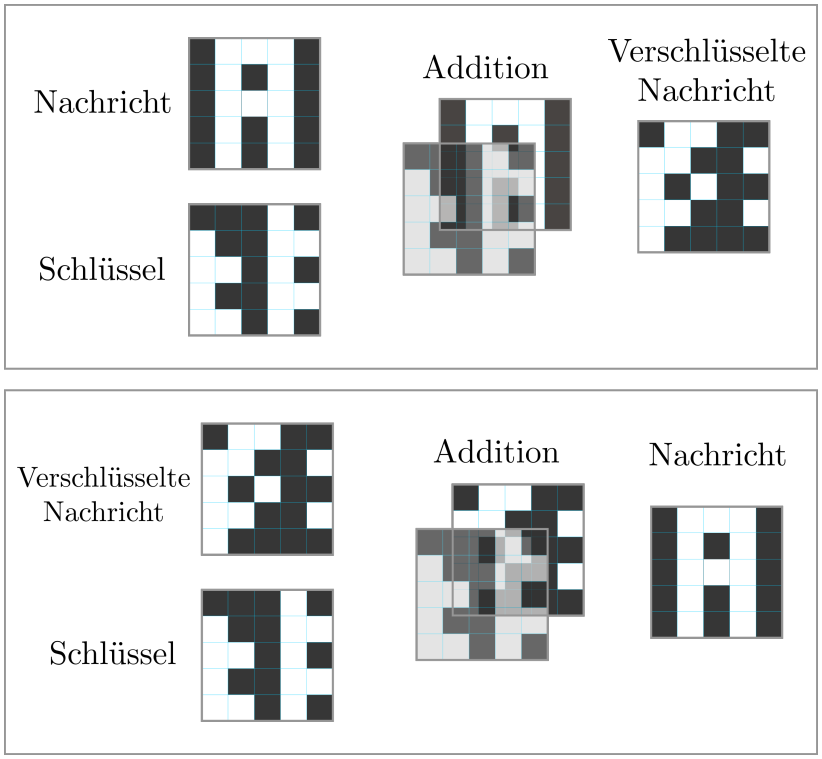

Abbildung 1: *Schematische Darstellung des Ver- und Entschlüsselungsprozesses. Bitwerte von 0 und 1 wurden als schwarze, bzw. weiße Kästchen codiert.*

Damit scheint sich aber das Eingangsproblem nur zu verlagern: Statt der Nachricht selbst muss nun ein Verfahren gefunden werden, wie man den Schlüssel sicher übertragen kann.
Eine Lösung in der klassischen Kryptographie besteht darin, dass Sender und Empfänger einen Teil des Schlüssels gar nicht austauschen, sondern für sich behalten. Gleichzeitig schicken sie sich gegenseitig einen öffentlich zugänglichen Schlüssel. Diesen haben beide nach einem festgelegten und ebenfalls öffentlich bekannten mathematischen Verfahren aus ihrem privaten Schlüssel erzeugt. Die Kombination des öffentlich gesendeten Schlüssels mit dem jeweils privaten Teil des Schlüssels erlaubt es dann, die Nachricht zu ver-, bzw. zu entschlüsseln.
Obwohl das mathematische Verfahren zur Erzeugung des öffentlichen Schlüssels aus dem privaten Schlüssel öffentlich bekannt ist und daher prinzipiell rechnerisch auf den privaten Schlüssel rückgeschlossen werden kann, basiert die Sicherheit des Verfahrens darauf, dass der zugehörige Rechenaufwand für klassische Computer unrealistisch hoch wäre. Konkrete Verfahren basieren beispielsweise auf der Schwierigkeit der Primfaktorzerlegung großer Primzahlen. Damit ist das Verfahren jedoch nicht intrinsisch sicher, sondern lediglich in der Praxis nicht mit realistischem Aufwand zu entschlüsseln.

Wie in Abschnitt 4.5 erläutert, bietet die Quantenphysik andere, intrinsisch sichere Lösungen für das Problem des Schlüsselaustausches.

2 Grundlagen der Quanteninformationstechnik

2.1 Einzelphotonen

Das Konzept der Quantelung lässt sich nicht nur auf die Energie eines Elektrons im Potential eines Atomkerns, sondern auch auf die Energie des von ihm ausgesendeten Lichtes übertragen: Beim Übergang von einem Schwingungszustand hoher Energie zu einem Zustand mit geringerer Energie wird die Energiedifferenz in Form einer diskreten Portion elektromagnetischer Energie abgegeben, die als *Photon* bezeichnet wird. Für die Energie eines Photons gilt Plancks bekannte Formel:

$$E = h \cdot \nu \tag{1}$$

h beschreibt in dieser Formel das Plank'sche Wirkungsquantum und ν die Frequenz der elektromagnetischen Schwingung.
Anhand dieser Formel wird deutlich: Das Wort ‚Photon'beschreibt die *kleinstmögliche Anregung des elektromagnetischen Feldes* bei einer vorgegebenen Frequenz. Es ist also zu erwarten, dass alle aus der klassischen Elektrodynamik bekannten Phänomene auch auf Basis eines quantenphysikalischen Photonenbegriffes als Grenzfall beschrieben werden können. Der Übergang besteht vereinfacht ausgedrückt in der Erhöhung der Anzahl der betrachteten Emissionsprozesse: Betrachtet man nicht nur ein einzelnes Atom, sondern alle Licht emittierenden Atome eines Festkörpers oder Gases zugleich, so entspricht dies einer statistischen Mittelung über alle emittierten Photonen, was zurück zum klassischen Konzept einer kontinuierlichen elektromagnetischen Welle führt.
Umgekehrt bedeutet dies, dass einige Eigenschaften kontinuierlicher Wellen in Bezug auf einzelne Photonen ihre Anschaulichkeit verlieren oder sogar gar nicht sinnvoll zugeschrieben werden können. Ähnlich wie bspw. die Temperatur als physikalische Größe nur Vielteilchensysteme sinnvoll beschreiben kann, kann einzelnen Photonen keine Intensität zugeschrieben werden. Da es sich um die kleinstmögliche Anregung des elektromagnetischen Feldes handelt, können Photonen nur erzeugt oder vernichtet, aber nicht in kleinere Energiequanten ‚aufgeteilt' werden. Dies hat Konsequenzen für die Betrachtung von Messergebnissen, etwa bei Polarisationsmessungen: Während eine kontinuierliche Lichtwelle an einem polarisierenden Strahlteiler zu verschiedenen Anteilen reflektiert und transmittiert werden kann, können für ein einzelnes Photon nur Wahrscheinlichkeiten für mögliche Messergebnisse angegeben werden. das Messergebnis selbst ist dabei immer eindeutig. Die Eigenschaft der Polarisation verliert damit ihre Anschaulichkeit: Statt wie

bisher als Schwingungsrichtung einer elektromagnetischen Welle kann sie nur noch abstrakt verstanden werden als Eigenschaft, die sich nur rückwirkend zuschreiben lässt: Wenn ein Photon hinter einem vertikal eingestellten Polfilter registriert wird, besitzt es die Eigenschaft ‚vertikale Polarisation '. Wird es an einem vertikal eingestellten Polfilter absorbiert, besitzt es dagegen die Eigenschaft ‚horizontale Polarisation '. Ähnliche Bedingungen lassen sich für die Polarisationsmessung mit einem polarisierenden Strahlteiler formulieren.

2.2 Qubits als Zweiniveausysteme

Die POalrisationsmessung an einem einzelnen Photon hat stets nur zwei mögliche Ergebnisse: Im Falle eines Polfilters lauten die Möglichkeiten *Transmission* oder *Absorption*. Nutzt man einen polarisierenden Strahlteiler zur Polarisationsbestimmung, ergeben sich die beiden möglichen Ergebnisse *Transmission* oder *Reflektion*. Das Ergebnis der Messung ist in jedem Fall eindeutig. Mathematisch betrachtet handelt es sich bei der Polarisation von einzelnen Photonen daher um ein typisches Zweiniveausystem (wie auch bspw. der Spin eines einzelnen Elektrons bezgl. jeder Raumrichtung nur zwei mögliche Werte annehmen kann).
Die Observablen zur Beschreibung solcher Zweiniveausysteme können durch die Pauli-Matrizen mit den Eigenwerten ± 1 ausgedrückt werden:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2}$$

Jede der drei Pauli-Matrizen hat zwei Eigenvektoren, die jeweils eine vollständige Basis zur Beschreibung des Quantenzustandes bilden. In Bezug auf die Polarisation können diese Eigenvektoren mit den folgenden Polarisationsrichtungen identifiziert werden:

$$\begin{aligned} &\sigma_z \text{ :horizontal/vertikal} && |H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &\sigma_y \text{ :links/rechtszirkular} && |L\rangle = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |R\rangle = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ &\sigma_x \text{ :}+45^\circ/-45^\circ\text{diagonal} && |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned} \tag{3}$$

Mithilfe der Eigenvektoren der Pauli-Matrizen lässt sich der Polarisationszustand $|\psi\rangle$ eines einzelnen Photons beispielsweise darstellen als:

$$|\psi\rangle = a\,|H\rangle + b\,|V\rangle \quad ; \quad |a^2| + |b^2| = 1 \tag{4}$$

Analog kann jedes der anderen Paare von Basisvektoren zur Darstellung des Zustandes genutzt werden.

Da die Pauli-Matrizen untereinander nicht kommutieren, lässt sich die Polarisationsrichtung nicht gleichzeitig in verschiedenen Basen bestimmen. Auch dies wird an den Eigenvektoren ersichtlich: Befindet sich das Photon im Zustand $|+\rangle$ (lineare Polarisation in $+45°$), so bedeutet dies für eine Messung in der $|HV\rangle$-Basis eine Superposition ($|+\rangle = \frac{1}{\sqrt{2}}[|H\rangle + |V\rangle]$). Die Messung dieses Zustandes in der $|HV\rangle$-Basis liefert daher komplett zufällige Ergebnisse.
Aufgrund ihrer Eigenschaften sind Zweiniveausysteme naheliegende Kandidaten, um die Bitwerte ‚0 ‘und ‚1‘ zu codieren, wobei ein Bitwert mit einem möglichen Eigenwert der Messung assoziiert wird. Da es sich bei Zweiniveausystemen jedoch um Quantensysteme handelt, bei denen Interferenz- und Superpositionsphänomene eine Rolle spielen, spricht man in diesem Zusammenhang von einem ‚Quanten-Bit‘ oder ‚Qubit‘. Anders als klassische Bits kann einem Qubit erst durch Messung einen eindeutiger Bitwert zugeschrieben werden, da je nach Präparation des Zustandes zuvor beliebige Superpositionen aus den Basiszuständen denkbar sind. Zudem ist der Bitwert nur in Bezug auf eine bestimmte Basis eindeutig festgelegt. Diese charakteristischen Quanteneigenschaften werden sowohl für das Quantencomputing, als auch zur Schlüsselgenerierung in der Kryptographie genutzt. Außerdem spielt eine weitere Besonderheit der Quantenphysik eine wichtige Rolle für die Sicherheit von übertragenen Qubits.

2.3 No-Cloning-Theorem

Das No-Cloning-Theorem besagt, dass Quantenzustände nicht kopiert werden können. Während ein klassisches Bit beliebig oft ausgelesen und vervielfältigt werden kann, ist dies bei Quantenzuständen nicht möglich, weil beim Auslesen der Werte eines Qubits die Information über die komplexe Phase des Quantenzustandes verlorengeht. Das Ergebnis der Messung gibt nicht den kompletten Quantenzustand wieder, sondern projiziert diesen auf die gewählte Messbasis. Mathematisch folgt das No-Cloning-Theorem aus der Unitarität der Messoperatoren [6][8]. Eine Vorrichtung, die den Zustand eines beliebigen Qubits $|\Psi\rangle$ perfekt auf ein anderes Qubit $|0\rangle$ übertragen kann, müsste durch einen unitären Operator U repräsentiert werden können. Der Kopiervorgang kann dann folgendermaßen repräsentiert werden:

$$U|\psi 0\rangle = |\psi\psi\rangle \tag{5}$$

Der Kopierer soll aber nicht nur *ein spezifisches* beliebiges Qubit $|\psi\rangle$, kopieren können, sondern potentiell *alle möglichen* beliebigen Qubits. In erster Näherung soll nun neben $|\psi\rangle$ ein zweiter Zustand $|\phi\rangle$ kopiert werden:

$$U|\phi 0\rangle = |\phi\phi\rangle \tag{6}$$

Für das Skalarprodukt $\langle\phi|\,|\psi\rangle$ gilt dann:

$$\begin{aligned}\langle\phi|\psi\rangle = \langle\phi|\psi\rangle \cdot \langle 0|0\rangle = \langle\phi 0|\, U^\dagger U\,|\psi 0\rangle = \langle\phi\phi|\psi\psi\rangle = \langle\phi|\psi\rangle^2 \\ \Rightarrow \langle\phi|\psi\rangle = 0 \vee \langle\phi|\psi\rangle = 1\end{aligned} \tag{7}$$

Da die beiden zu kopierenden Vektoren entweder senkrecht oder orthogonal zueinander stehen müssen, folgt, dass ein Quantenkopierer stets nur Eigenzustände einer einzigen Basis zuverlässig kopieren kann. Versucht man dagegen, einen Superpositionszustand der Form $|\xi\rangle = a\,|\phi\rangle + b\,|\psi\rangle$ mit $|\phi\rangle \perp |\psi\rangle$zu kopieren, erwartet man:

$$\begin{aligned}U\,|\xi 0\rangle = |\xi\xi\rangle &= (a\,|\phi\rangle + b\,|\psi\rangle)\,(a\,|\phi\rangle + b\,|\psi\rangle) \\ &= a^2\,|\phi\phi\rangle + b^2\,|\psi\psi\rangle + ab\,|\phi\psi\rangle + ba\,|\psi\phi\rangle\end{aligned} \tag{8}$$

Es ergibt sich jedoch:

$$U\,(a\,|\phi 0\rangle + b\,|\psi 0\rangle) = a\,|\phi\phi\rangle + b\,|\psi\psi\rangle \tag{9}$$

Da 8 und 9 sich widersprechen, muss geschlussfolgert werden, dass kein unitärer Operator existiert, der den geforderten Eigenschaften entspricht. Das Kopieren beliebiger unbekannter Quantenzustände ist also nicht möglich.

3 Verschränkung als Prüfstein für die klassische Physik

3.1 lokaler Realismus und EPR-Paradox

Die klassische Physik geht für bei der Beschreibung von Wechselwirkungen zwischen Systemen von zwei Grundannahmen aus [5]:

- **Realismus:** Durch eine Messung bestimmbare Größen eines physikalischen Systems sind auf real existierende Eigenschaften dieses Systems zurückzuführen. Beispiel: Da die Polarisation eine prinzipiell jederzeit messbare Eigenschaft eines Photons ist, kann davon ausgegangen werden, dass jedes Photon auch ohne Messung jederzeit eine bestimmte eindeutig festgelegte Polarisation besitzt.
- **Lokalität:** Eine Wechselwirkung mit einem physikalischen System A am Ort 1 mit der Umwelt kann nicht unmittelbar gleichzeitig ein anderes physikalisches System B an Ort 2 beeinflussen.

Die Existenz von Verschränkung bei Quantenobjekten zeigt nun, dass diese beiden Annahmen in der Quantenphysik nicht uneingeschränkt aufrecht erhalten werden können. Experimentell lässt sich die Unvereinbarkeit von

Lokalität und Realismus mit der Quantenphysik anhand von Einzelphotonenpaaren messen, die in ihrer Polarisation verschränkt sind. Diese Paare einzelner Photonen sind aufgrund der physikalischen Randbedingungen bei ihrer Entstehung in ihrer Polarisationsrichtung wechselseitig voneinander abhängig, das heißt die Polarisationsrichtungen der beiden Photonen weisen eine starke Korrelation auf, wenn man – wie im Versuch – mehrere Messungen an identisch präparierten Paaren durchführt. Mathematisch lässt sich der Zustand, in dem sich die zwei Photonen befinden, als einer der vier sogenannten Bell-Zustände ausdrücken:

$$\begin{aligned} |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}} \left[|H_A V_B\rangle \pm |V_A H_B\rangle \right] \\ |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}} \left[|H_A H_B\rangle \pm |V_A V_B\rangle \right] \end{aligned} \tag{10}$$

Die Indizes A und B stehen dabei für das Photon bei Alice, bzw. bei Bob. Die Korrelation zwischen den beiden Photonen liegt mathematisch darin begründet, dass sich der Gesamtzustand nicht als Produkt aus den Einzelzuständen von Alice und Bobs Photonen umschreiben lässt:

$$\cancel{|\Psi_{AB}\rangle \Rightarrow |\phi_A\rangle \cdot |\phi_B\rangle} \tag{11}$$

Die Interpretation dieses Zustandes führt im lokal-realistischen Weltbild zu widersprüchlichen Schlussfolgerungen: Die Annahme des Realismus besagt, dass die Photonen bei ihrer Entstehung festgelegte Polarisationsrichtungen besitzen müssen. Die Korrelation zwischen den Messergebnissen lässt sich dann aber nur dadurch erklären, dass die Polarisationsmessung bei Alice das Photon bei Bob *beeinflusst*, also instantan Information zwischen den beiden Photonen ausgetauscht wird. Wenn Alice und Bob sich aber weit voneinander entfernt befinden, widerspricht diese Folgerung der Annahme der Lokalität von Ursache und Wirkung. Es scheint also, dass in der Quantenphysik einige fundamentale Annahmen über die Struktur der Welt nicht aufrechterhalten werden können.
Dieser Widerspruch ist als Einstein-Podolsky-Rosen-Paradoxon [3] bekannt geworden und von Einstein als Argument gegen die Vollständigkeit der Quantenphysik verwendet worden. Zur Auflösung des Widerspruchs und zur Rettung des lokal-realistischen Weltbildes ist die Existenz sogenannter verborgener Parameter angenommen worden. Laut dieser Ad-hoc-Hypothese sollen experimentell nicht direkt zugängliche, weitere Eigenschaften existieren, durch die insgeheim doch alle messbaren Eigenschaften der Quantenobjekte festgelegt sind. Da die verborgenen Parameter nicht selbst gemessen werden könnten, sehe es so aus, als würden sich die Einzelmessungen von Alice und Bob gegenseitig beeinflussen - in Wirklichkeit aber würden doch nur bereits festgelegte Eigenschaften der beiden Photonen aufgedeckt.
Die Quantenphysik hingegen verwirft die Annahme des lokalen Realismus,

statt mit verborgenen Parametern zu argumentieren. Eine quantenphysikalische Interpretation kommt daher zu den folgenden Schlussfolgerungen:

- Die Polarisationsrichtung der Photonen von Alice und Bob existiert nicht unabhängig von der Messung und wird erst bei der Messung festgelegt.
- Durch Messung der Polarisationsrichtung des Photons von Alice ist direkt die Polarisationsrichtung von Bobs Photon festgelegt. Dabei wird jedoch keine Information ausgetauscht.

Es scheint, als sei die Existenz solcher verborgener Parameter eine experimentell nicht überprüfbare Hypothese und daher eher eine philosophische Interpretationsfrage. Dem Physiker John Stewart Bell ist es jedoch gelungen ein mathematisches Prüfkriterium für die Richtigkeit lokal-realistischer Modelle zu formulieren.

3.2 Korrelationsmessung und CHSH-Ungleichung

Bells Argument ist von Clauser, Horne, Shimonyi und Holt (CHSH, [1][2]) in die im Folgenden wiedergegebene Form gebracht worden.
Die Forderung des Lokalen Realismus besagt, dass sich die Messungen von Alice und Bob nicht gegenseitig beeinflussen, das heißt, dass die Wahrscheinlichkeit für ein bestimmtes Messergebnis einer gemeinsamen Betrachtung von Alice und Bob als Produkt der Wahrscheinlichkeiten zweier Einzelmessungen geschrieben werden kann. Alice messe die Polarisation in Richtung des Vektors $\vec{a}$ und Bob in Richtung des Vektors $\vec{b}$. Dann gilt für die Erwartungswerte E der kombinierten und Einzelmessungen [7]:

$$E(\vec{a}, \vec{b}) = E(\vec{a}) \cdot E(\vec{b}) \tag{12}$$

Betrachten wir nun eine spezielle Kombination S von kombinierten Messungen unter den Winkeln $\vec{a}$ und $\vec{a}'$ bei Alice und $\vec{b}$, bzw. $\vec{b}'$ bei Bob:

$$S = E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}') + E(\vec{a}', \vec{b}) + E(\vec{a}', \vec{b}') \tag{13}$$

Diese Gleichung lässt sich unter Berücksichtigung des Separabilitätskriteriums 12 umschreiben als:

$$\begin{aligned} & E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}') + E(\vec{a}', \vec{b}) + E(\vec{a}', \vec{b}') \\ = {} & E(\vec{a}) \cdot E(\vec{b}) - E(\vec{a}) \cdot E(\vec{b}') + E(\vec{a}') \cdot E(\vec{b}) + E(\vec{a}') \cdot E(\vec{b}') \\ = {} & E(\vec{a}) \cdot \Big[E(\vec{b}) - E(\vec{b}')\Big] + E(\vec{a}') \cdot \Big[E(\vec{b}') + E(\vec{b})\Big] \end{aligned} \tag{14}$$

Da es sich um Messungen an einem Zweiniveausystem handelt, gibt es für Alice und Bob jeweils zwei mögliche Messergebnisse, repräsentiert durch die Eigenwerte $E(i) = \pm 1$. Betrachtet man die möglichen Kombinationen von

Eigenwerten für die Einzelmessungen ergibt sich eine Obergrenze für den Wert von S:

$$|S| \leq 2 \tag{15}$$

Dies ist die Bell'sche Ungleichung in der Formulierung nach CHSH.

In der Quantenphysik wird das Separabilitätskriterium (Gleichung 12) nicht vorausgesetzt. Das Ergebnis einer Einzelmessung entspricht der Messung des Erwartungswertes einer Observable, die für Zweiniveausysteme gegeben sind durch die Pauli-Matrizen (Gleichung 2).

für die Messrichtungen $\vec{a}$ und $\vec{a'}$, bzw. $\vec{b}$ und $\vec{b'}$ergeben sich die Observablen

$$O_a = \sum \sigma_i a_i \qquad O_{a'} = \sum \sigma_i a'_i \qquad O_b = \sum \sigma_i b_i \qquad = \sum \sigma_i b'_i \tag{16}$$

Bei gemeinsamer Betrachtung der beiden Messungen wird der Erwartungswert des Produkts der Observablen betrachtet, nicht das Produkt einzelner Erwartungswerte. Damit ergibt sich:

$$E(\vec{a}, \vec{b}) = \left\langle \Psi \left| \left(\sum \sigma_i a_i \right) \cdot \left(\sum \sigma_i b_i \right) \right| \Psi \right\rangle = -\vec{a} \cdot \vec{b} = -\cos\left(\theta_{ab}\right) \tag{17}$$

Damit hängt das Ergebnis der Messung nur vom Winkel θ_{ab} zwischen den jeweils gewählten Messrichtungen ab. Für passend gewählte Messrichtungen ergibt sich damit gemäß Gleichung 17 eine andere Obergrenze für S als unter klassischen Annahmen (Gleichung 14). Den Maximalwert für S erhält man für die Kombination:

$$\begin{aligned} \theta_{ab} = -\frac{1}{3}\theta_{ab'} = \theta_{a'b} = \theta_{a'b'} = \frac{\pi}{4} \\ \Rightarrow |S| \leq 3 \cdot \cos\left(\frac{\pi}{4}\right) - \cos\left(\frac{\pi}{4}\right) = 2\sqrt{2} \end{aligned} \tag{18}$$

Die Bell'sche Ungleichung ermöglicht also die Überprüfung der beiden verschiedenen Ansätze anhand der Messung von Polarisationskorrelationen unter verschiedenen Messwinkeln. Ergibt sich ein Ergebnis über der klassisch vorhergesagten Schwelle von $|S| \leq 2$ kann keine lokal realistische Theorie zur Erklärung herangezogen werden - auch keine, die verborgene Parameter beinhaltet.

Obwohl es sich bei Verschränkung im Sinne der Quantenphysik um eine nichtlokale Wechselwirkung handelt, steht dies nicht im Widerspruch zur speziellen Relativitätstheorie. Durch die lokale Messung der Polarisationsrichtung bei Alice wird zwar die Polarisationsrichtung von Bobs Photon festgelegt, jedoch ist damit keine Informationsübertragung verbunden, denn ohne sich mit Alice auszutauschen hat Bob keinerlei Anhaltspunkte über die zu wählende Messbasis. Er erhält daher ein zufälliges Messergebnis. Erst wenn Alice und Bob über einen klassischen Kommunikationskanal (mit maximal Lichtgeschwindigkeit) ihre Messbasen abgleichen, können Korrelationen betrachtet werden.

4 Technische Umsetzungen

4.1 Erzeugung verschränkter Photonenpaare

Die Emission von Photonen verschiedener Lichtquellen erfolgt nicht mit einer konstanten Rate, sondern gehorcht einer statistischen Verteilung. Bei thermischen Lichtquellen beobachtet man den Effekt, dass häufiger mehrere Photonen gleichzeitig emittiert werden als einzeln - die Photonen sind also untereinander zeitlich korreliert (sog. ‚Bunching'). Die Emissionsverteilung eines perfekten Lasers ist hingegen statistisch unkorreliert, und folgt einer Poissonverteilung. Auch hier tritt jedoch eine gehäufte Emission von Photonen noch auf. Bei einer zuverlässigen Einzelphotonenquelle ohne Bunching muss die zeitliche Korrelation zwischen der Emission der Photonen hingegen negativ sein, d. h. dass häufiger nur ein Photon emittiert wird als mehrere gleichzeitig (sog. ‚Anti-Bunching'). Eine Möglichkeit, dies zu realisieren stellt die Ausnutzung von nichtlinearen Effekten in doppelbrechenden Materialien dar.
Durch Bestrahlung von doppelbrechenden Kristallen mit Laserlicht kann man leicht Feldstärken erzeugen, die groß genug sind um nichtlineare Effekte hervorzurufen. Ein solcher Effekt ist die *Spontane parametrische Fluoreszenz*, die im Experiment genutzt wird (Abb. 2).

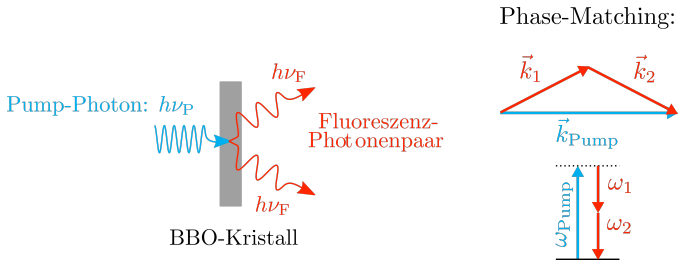

Abbildung 2: *Links: Schematische Darstellung des Prozesses der Spontanen Parametrischen Fluoreszenz. Rechts: Darstellung der Energie-und Impulsbeziehungen des Prozesses.*

Bei diesem Prozess wird ein doppelbrechender Kristall (z. B. Beta-Bariumborat oder kurz BBO) mit einem Laserstrahl hoher Intensität, dem sogenannten *Pumpstrahl* beleuchtet. Mit einer sehr geringen Wahrscheinlichkeit kann es aufgrund des nichtlinearen Effektes passieren, dass im Kristall ein ankommendes Photon mit Frequenz ν_P in zwei Photonen mit halber Frequenz ν_F umgewandelt wird. Die zeitliche Verteilung der emittierten Photonenpaare zeigt dabei das gewünschte Anti-Bunching. Zudem ist die Wahrscheinlichkeit für das Auftreten des Prozesses sehr gering: Nur eins von etwa 10^{11} ankommenden Photonen wird in ein Fluoreszenzpaar umgewandelt. Daher kann in guter Näherung von einzelnen Photonenpaaren gesprochen werden.

4.2 Erzeugung verschränkter Zustände

Damit der Fluoreszenzprozess im BBO-Kristall angeregt werden kann, müssen bestimmte Randbedingungen erfüllt sein [7]. Zunächst gilt für den betrachteten Prozess natürlich Energieerhaltung,

$$\omega_{\text{Pump}} = \omega_1 + \omega_2 \tag{19}$$

Im konkreten Fall gilt speziell $\omega_1 = \omega_2 = \frac{1}{2}\omega_{\text{Pump}}$.
Ein weiterer Erhaltungssatz betrifft die Wellenvektoren der beteiligten Photonen und kann als eine Art Impulserhaltungssatz aufgefasst werden:

$$\vec{k}_{\text{Pump}} = \vec{k}_1 + \vec{k}_2 \tag{20}$$

Gleichung 20 wird auch als ‚Phasematching-Bedingung' bezeichnet. Die Bedingungen 19 und 20 können im für den Versuch verwendeten doppelbrechenden Material gleichzeitig erfüllt werden. In linearen optischen Medien ergibt sich im Normalfall aufgrund der Dispersion eine Differenz zwischen den $\vec{k}$-Vektoren von Pump- und Fluoreszenzphotonen. Da in doppelbrechenden Medien der Brechungsindex polarisationsabhängig ist, kann diese Differenz bei passender geometrischer Ausrichtung des BBO-Kristalls jedoch ausgeglichen werden, sodass beide Gleichungen erfüllt werden. Damit ergibt sich jedoch auch eine zusätzliche Randbedingung, die Polarisation von Pump- und Fluoreszenzphotonen betrifft. Bezgl. der Polarisationsabhängigkeit werden zwei Arten des Phase-Matching unterschieden:

- Beim *Typ-I-Phasematching* ist der Pumpstrahl außerordentlich polarisiert. Die Fluoreszenzphotonen sind beide ordentlich polarisiert. Die Fluoreszenzphotonen weisen also parallele Polarisationsrichtungen auf.
- Beim *Typ-II-Phasematching* ist der Pumpstrahl außerordentlich polarisiert. Ein Fluoreszenzphoton ist ordentlich polarisiert, das andere außerordentlich. Die Fluoreszenzphotonen weisen also orthogonale Polarisationsrichtungen auf.

Mit Typ-II-Phasematching können auf einfache Weise polarisationsverschränkte Photonen erzeugt werden. Die beiden Photonen eines Paares verlassen den Kristall in unterschiedlichen Richtungen. Es ergeben sich zwei Emissionskegel, von denen einer vollständig vertikal, der andere vollständig horizontal polarisiert ist. Photonen eines Paares finden sich jeweils an den gegenüberliegenden Flanken des Doppelkegels.

Während jeder Kegel für sich genommen also eindeutig polarisiert ist, ergibt sich an den Schnittpunkten eine Überlagerung aus horizontaler und vertikaler Polarisation (Abb 3). In diesen Punkten emittierten Photonen lässt sich aufgrund der Überlagerung keine eindeutige Polarisation mehr

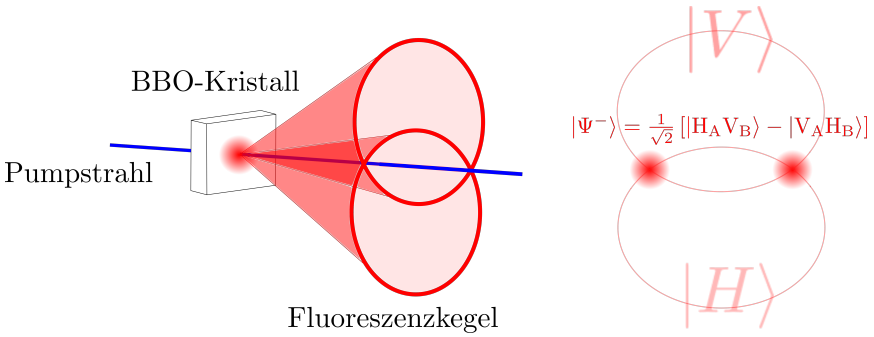

Abbildung 3: *Darstellung der Emissionsgeometrie des Fluoreszenzprozesses (links) und Detailbetrachtung der Polarisationen auf den Doppelkegeln (rechts). An den Schnittpunkten der Kegel ergibt sich der verschränkte Zustand.*

zuschreiben, es ist nur bekannt, dass beide Photonen zusammen betrachtet orthogonal zueinander polarisiert sein müssen. Diese Beschreibung entspricht der Definition eines verschränkten Zustands der Form $|\Psi^-\rangle$(Gleichung 10).

4.3 Detektion und Polarisationsmessung

Der Nachweis der Photonenpaare erfolgt über Einzelphotonendetektoren. Jedes Detektionsereignis wird von einem Rechner registriert und mit einem genauen Zeitstempel versehen. Die Detektionsereignisse können für Alice und Bob jeweils getrennt betrachtet werden, oder Alice und Bob tauschen sich über ihre Ergebnisse aus und vergleichen die Zeitstempel ihrer Detektionsereignisse. Bei gleichzeitigen Ereignissen können sie annehmen, dass es sich um die zusammengehörenden Photonen eines Paares handelt (Koinzidenzmethode). In der technischen Umsetzung erfolgt dieser Vergleich durch eine Zeiterfassungselektronik mit einigen Pikosekunden Auflösung.

Zur Polarisationsmessung werden polarisierende Strahlteiler verwendet. Anhand des Kanals, in dem ein Photon detektiert wird, kann dann auf die gemessene Polarisation rückgeschlossen werden. In Kombination mit Halbwellenplättchen, die die Eingangspolarisation um beliebige Werte drehen können, lässt sich die Polarisation der ankommenden Photonen in beliebigen Messbasen bestimmen (Abb. 4).
In Abb. 5 ist der gesamte Experimentieraufbau skizziert.
Bei den gemessenen Detektionsereignissen handelt es sich um (näherungsweise) poissonverteilte Zufallsereignisse. Die statistische Unsicherheit auf einer Messung mit N Zählereignissen kann daher über den Zusammenhang $\sigma = \sqrt{N}$ modelliert werden. Mit längeren Messzeiten nimmt daher die relative statistische Unsicherheit ab, was bei der Wahl der Integrationszeiten zu berücksichtigen ist.

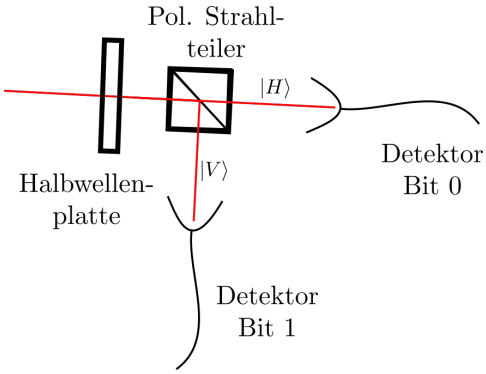

Abbildung 4: *Schema der Messaufbauten von Alice und Bob. Der polarisierende Strahlteiler projiziert die einfallende Polarisationsrichtung auf die HV-Basis. Mit dem Halbwellenplättchen kann die einfallende Polarisation zuvor beliebig gedreht werden, sodass prinzipiell in jeder linearen Polarisationsbasis gemessen werden kann.*

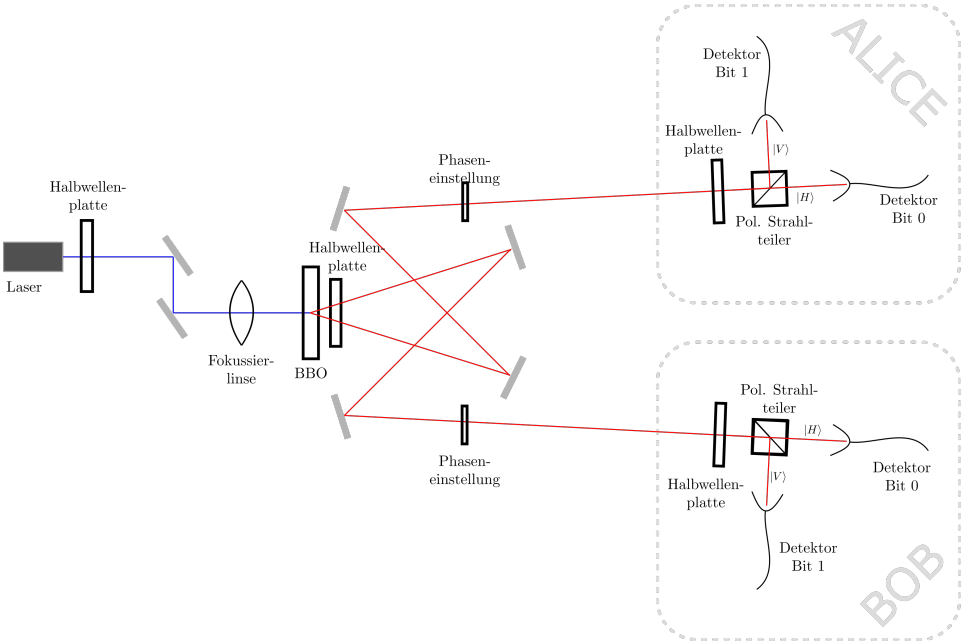

Abbildung 5: *Skizze des Versuchsaufbaus.*

4.4 Messung der CHSH-Ungleichung

In der theoretischen Herleitung der Bell'schen Ungleichung (Gl. 13) spielt der Erwartungswert $E(\vec{a}, \vec{b})$ einer kombinierten Polarisationsmessung an zwei Photonen eine entscheidende Rolle. In der Praxis muss dieser Wert durch mehrere Einzelmessungen statistisch angenähert werden. In der Praxis wird daher statt des Erwartungswertes $E(\vec{a}, \vec{b})$ einer Einzelmessung wird daher die Korrelationsfunktion $C(\vec{\alpha}, \vec{\beta})$ für viele aufeinanderfolgende Messereignisse

bestimmt. α und β entsprechen dabei den gewählten Polarisationswinkeln. Zur Messung der Korrelationsfunktion nehmen Alice und Bob unter den Winkeln α und β jeweils eine längere Sequenz von Detektionsereignissen auf, wobei anhand der Zeitstempel die Ereignisse aussortiert werden, wo nur einer der beiden ein Photon registriert hat. Als Ergebnis erhalten Alice und Bob je eine Bitfolge aus Einsen und Nullen. Anschließend vergleichen Alice und Bob ihre Listen auf Gemeinsamkeiten und Unterschiede, um den Grad der Korrelation zu ermitteln. Gleiche Messergebnisse werden positiv gewertet (positive Korrelation), abweichende Messergebnisse negativ [9]:

$$C_{A,B} = \frac{N_{\alpha,\beta} + N_{\alpha^\perp,\beta^\perp} - N_{\alpha^\perp,\beta} - N_{\alpha,\beta^\perp}}{N_{\alpha,\beta} + N_{\alpha^\perp,\beta^\perp} + N_{\alpha^\perp,\beta} + N_{\alpha,\beta^\perp}} \tag{21}$$

α,$\alpha^\perp$ und β, $\beta^\perp$ bezeichnen dabei jeweils die gewählte Basis von Alice und Bob, N die Anzahl der Detektionsereignisse.
Anhand des Wertes der Korrelationsfunktion lassen sich auf Basis einer Messung bei Alice in der Basis α, $\alpha_\perp$ Aussagen über das wahrscheinliche Ergebnis einer Messung bei Bob in der Basis β, $\beta_\perp$ ableiten. Sie kann Werte von $C = -1$ (perfekte Antikorrelation: Alice und Bob finden ihre Photonen immer im entgegengesetzten Kanal) bis $C = +1$ (perfekte Korrelation: Alice findet ihre Photonen immer im gleichen Kanal wie Bob) annehmen. Ein Wert von $C = 0$ bedeutet dabei, dass keine Korrelation vorliegt. Es lassen sich dann auf Basis einer Polarisationsmessung an Photon A keine Aussagen über die wahrscheinliche Polarisation von Photon B treffen und umgekehrt. Das Ergebnis einer Korrelationsmessung nach Gleichung 21 lässt sich auch grafisch darstellen, wie in Abb. 6 gezeigt.

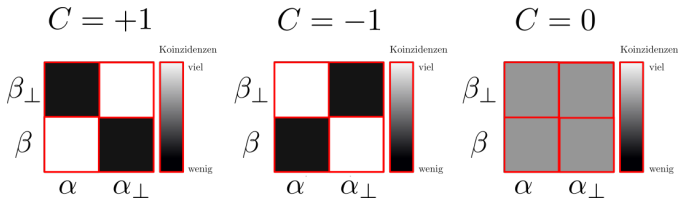

Abbildung 6: *Grafische Darstellung von Korrelationsfunktionen. Je mehr Detektionsereignisse gezählt wurden, desto heller ist das entsprechende Feld in der 2x2-Tafel.*

Da die verschränkten Photonen im Zustand $|\Psi^-\rangle$ stets senkrecht zueinander polarisiert sind, ergeben sich folgende, mit dem Gesetz von Malus vergleichbare Winkelabhängigkeiten für Koinzidenzmessungen:

$$N_{\alpha,\beta} \propto \sin^2(|\alpha - \beta|) \tag{22}$$

Daraus folgt für die Korrelationsfunktion $C_{A,B}$:

$$C_{A,b} = \frac{2\left[\sin^2(|\alpha - \beta|) - \cos^2(|\alpha - \beta|)\right]}{2\left[\sin^2(|\alpha - \beta|) + \cos^2(|\alpha - \beta|)\right]} = -\cos(2|\alpha - \beta|) \tag{23}$$

Tabelle 1: *Winkelstellungen für die maximale Verletzung der Bell'schen Ungleichung.*

Bob: \ Alice:		α (0°)	$\alpha_\perp$ (90°)	α' (45°)	$\alpha'_\perp$ (135°)
					
β (22.5°)		$C_{\alpha\beta}$		$C_{\alpha'\beta}$	
$\beta_\perp$ (112.5°)					
β' (67.5°)		$C_{\alpha\beta'}$		$C_{\alpha'\beta'}$	
$\beta'_\perp$ (157.5°)					

Zur experimentellen Überprüfung der Ungleichungen 15 bzw. 18 müssen dann nur noch die passenden Winkelkombinationen gefunden werden, für die der S-Parameter (Gleichung 13) maximal wird. Dies ist der Fall für:

$$|\alpha - \beta| = |\alpha' - \beta| = |\alpha' - \beta'| = \frac{1}{3}|\alpha - \beta'| = \frac{\pi}{8} \tag{24}$$

Durch Einsetzen in Gleichung 13 erhält man dann:

$$S = -3\cos\left(2 \cdot \frac{\pi}{8}\right) + \cos\left(6 \cdot \frac{\pi}{8}\right) = -2\sqrt{2} \tag{25}$$

Auf diese Weise kann man durch Messung von Koinzidenzzählraten auf einfache Weise die Vorhersagen von klassischer Physik und Quantenphysik überprüfen. Der tatsächlich experimentell ermittelte Wert liegt in der Regel leicht unter dem Maximalwert von $S = 2\sqrt{2}$, da im Experiment der Verschränkungszustand nicht perfekt präpariert werden kann. Die konkreten Winkeleinstellungen für die Messung sind in Tabelle 1 aufgelistet.

4.5 Quantenkryptographie im One-Time-Pad Verfahren

Eine Möglichkeit, mithilfe von verschränkten Photonenpaaren und einem öffentlichen einen sicheren Schlüssel für öffentlich versendete Nachrichten zu erzeugen, ist das Ekert91-Protokoll [4].

4.5.1 Das Ekert91-Protokoll

Die Grundidee des Ekert91-Protokolls besteht darin, dass Alice und Bob sich nicht den eigentlichen Schlüssel gegenseitig zusenden müssen, sondern sich diesen anhand der Polarisationskorrelationen erschließen. Die konkrete Bitfolge des Schlüssels kann damit nur den beiden bekannt sein. Das Verfahren funktioniert wie folgt:

- Alice und Bob einigen sich auf eine gewisse Anzahl an Messbasen, die zur Vermessung einer Sequenz von Photonen aus der verschränkten Quelle verwendet werden sollen. Zweckmäßigerweise wählen sie die vier Basen aus, die zur Überprüfung der Bell'schen Ungleichung verwendet werden können.

- Die beiden vermessen die ankommenden Photonen in einer der vier möglichen Basen. Dabei variieren sie die gewählte Messbasis zufällig. Idealerweise nutzen sie dazu echte Zufallszahlen, die ebenfalls mithilfe der Quantenphysik erzeugt werden können.

- Alice und Bob tauschen sich öffentlich über die verwendeten Messbasen aus, unter denen sie Koinzidenzen registriert haben, sie beschränken sich dabei also auf Detektionsereignisse, bei denen Alice und Bob gleichzeitig ein Photon registrieren konnten. Dabei nennen sie **auf keinen Fall die konkreten ermittelten Bitwerte**. Stattdessen teilen sie einander nur mit, in welcher Basis sie das jeweilige Qubit vermessen haben. Nur die Bits, die in der gleichen Basis gemessen wurden, werden weiter für den Schlüssel genutzt. Die Messungen, in denen unterschiedliche Basen verwendet wurden, erfüllen einen andere Funktion (siehe Kapitel 4.5.2).

- Alice und Bob besitzen nun eine jeweils nur ihnen bekannte Liste mit den von ihnen gemessenen Bitwerten, sowie eine öffentliche Liste mit den verwendeten Basen. Da die Bitwerte nicht übertragen wurden, können sie nun als Schlüssel zur Ver- und Entschlüsselung einer Nachricht dienen. Da Alice und Bob nur Bits mit der gleichen Basis verwenden, können sie aus ihrem eigenen Ergebnis anhand der bekannten Korrelation auf das Ergebnis des jeweils anderen schließen. Da sie den genutzten verschränkten Zustand genau kennen, können sie aus ihren Ergebnissen auf die Ergebnisse des jeweils anderen rückschließen und besitzen so einen gemeinsamen Schlüssel.

- Alice addiert den generierten Schlüssel auf eine Nachricht und sendet diese öffentlich an Bob. Für außenstehende enthält die Botschaft keine Information.

- Bob erhält die Nachricht und kann diese anhand seiner eigenen Bitfolge entschlüsseln. Danach muss muss er die so erhaltene Bitfolge aufgrund der Antikorrelation des verwendeten $|\Psi^-\rangle$-Zustandes noch invertieren, um die Originalnachricht zu erhalten.

4.5.2 Einfluss eines Spions im Aufbau

Die Methode ist intrinsisch sicher, da der Schlüssel selbst nicht übertragen wird und es einem Spion aufgrund des No-Cloning-Theorems nicht möglich

ist, den vorherigen Quantenzustand exakt zu kopieren. Da der verschränkte Zustand sich in Bezug auf einzelne, lokale Polarisationsmessungen für *jede* denkbare Basis in Superposition befindet, wird der Zustand beim Kopieren notwendigerweise zerstört und kann nicht kopiert werden.
Technisch gesehen muss ein Spion in der Lage sein, die Qubits sowohl im Kanal von Alice, als auch im Kanal von Bob auszulesen und danach ein anderes Paar Qubits an Alice und Bob weiterzusenden.

Egal wie er das anstellt, ist er gezwungen, den weitergesendeten Photonen vorab eine definierte Polarisation aufzuprägen. Damit wird der von ihm erzeugte Zustand immer ein klassischer Zustand sein und daher deutlich geringere Korrelationen aufweisen, als ein ‚echter' verschränkter Zustand. In diesem Fall brauchen Alice und Bob nur eine Messung der Bell'schen Ungleichung durchzuführen. um den Spion zu enttarnen. Praktischerweise können sie hierfür direkt die Messergebnisse nutzen, die sie nicht zur Schlüsselgenerierung verwendet haben. Ist das Ergebnis der Prüfung des S-Parameters im klassischen Bereich ($S \leq 2$), werden sie den Schlüssel verwerfen, da sie sich sicher sein können, abgehört zu werden. Im Experiment wird der Spion, der den Produktzustand erzeugt, durch Einbau zusätzlicher Polfilter realisiert. Die Polfilter dienen zur Festlegung der Polarisation der Photonen. Stellt der Spion einen Polfilter auf horizontale und einen auf vertikale Polarisation, ergibt sich der Produktzustand:

$$|\Lambda\rangle = |V_\mathrm{A} H_\mathrm{B}\rangle \tag{26}$$

Vergleichen Alice und Bob ihre Messwerte und bestimmen Korrelationen, werden sie nur in der $|HV\rangle$-Basis eine starke Antikorrelation feststellen. In der $|+-\rangle$-Basis wird dagegen - anders als beim verschränkten Zustand keine Korrelation auftreten, weshalb sich durch Messung der CHSH-Ungleichung der Produktzustand vom verschränkten Zustand unterscheiden lässt.

Literatur

[1] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[2] J. F. Clauser and A. Shimony. Bell's theorem. experimental tests and implications. *Reports on Progress in Physics*, 41(12):1881–1927, 1978.

[3] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[4] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[5] C. Friebe, M. Kuhlmann, H. Lyre, P. M. Näger, O. Passon, and M. Stöckler. *Philosophie der Quantenphysik: Zentrale Begriffe, Probleme, Positionen*. Lehrbuch. Springer Spektrum, Berlin and Heidelberg, 2. auflage edition, 2018.

[6] M. Le Bellac. *A short introduction to quantum information and quantum computation*. Cambridge University Press, Cambridge, 2006.

[7] M. Oberparleitner. *Effiziente Erzeugung verschränkter Photonenpaare*. Dissertation, Ludwig-Maximilians-Universität, München, 2002.

[8] W. Scherer. *Mathematics of Quantum Computing: An Introduction*. Springer eBook Collection. Springer, Cham, 2019.

[9] C. Schuck. *Experimental Implementation of a Quantum Game*. Diplomarbeit, Ludwig-Maximilians-Universität, München, 2003.

5 Aufgaben zur Durchführung und Auswertung

Die folgenden Aufgaben sind für die Bearbeitung zu zweit und für die Nutzung der interaktiven AR-Anwendung ausgelegt. Ein Teilnehmer kann dabei die Rolle von Alice übernehmen, ein anderer die Rolle von Bob, um die Situation der Nachrichtenübertragung zu simulieren. Reale Kommunikation und Absprachen während der Messung sind natürlich ausdrücklich erforderlich und erwünscht!
Während der Durchführung führt Sie die AR-Anwendung anhand verschiedener Aufgaben durch die Versuche. Die folgenden Aufgaben sind daher primär als Leitfaden zur Vorbereitung auf die Sie erwartenden Aufgaben und für die Auswertung der im Versuch aufgenommenen Daten zu verstehen:

- Nehmen Sie sich zunächst Zeit, um sich einen Überblick über den Aufbau und die verwendeten Komponenten zu verschaffen. Besprechen Sie Unklarheiten mit Ihrem Betreuer.

- Betrachten Sie zunächst die **Einzelzählraten** der ankommenden Fluoreszenphotonen bei Alice und Bob, ohne auf Koinzidenzen zu filtern. Nehmen Sie eine Messreihe auf, in der Sie den Polarisationswinkel gegen die gemessene Einzelzählrate auftragen.

- Beurteilen Sie in der Auswertung den Polarisationsgrad der ankommenden Einzelphotonen, indem Sie für jeden der vier Detektoren den Kontrast zwischen Maximum und Minimum bestimmen. Dieser berechnet sich gemäß der Formel:

$$V = \frac{N_{\max} - N_{\min}}{N_{\max} + N_{\min}}$$

- wiederholen sie die Betrachtung der Polarisationsabhängigkeit für die **Koinzidenzzählraten**. Hierfür wird in einem Messarm eine feste Polarisationsrichtung als Basis gewählt, und im anderen Arm systematisch die Polarisationsrichtung variiert. Nehmen sie jeweils eine Messreihe für die $0°/90°$-Basis und für die $+45°/-45°$-Basis auf.

- Berechnen Sie auch hier für die erhaltenen Messreihen den Kontrast V und vergleichen Sie die Ergebnisse mit denen der Einzelzählraten.

- Messen Sie in vier zur Prüfung der CHSH-Ungleichung geeigneten Basen die Koinzidenzzählraten. Bestimmen Sie aus den Daten jeweils die Korrelationsfunktion C und bestimmen Sie den Wert des S-Parameters. Ist die Bell'sche Ungleichung verletzt?

- Diskutieren Sie im Protokoll, inwiefern die Messung der CHSH-Ungleichung mit den zuvor durchgeführten Messungen des Kontrasts in verschiedenen Basen zusammenhängt.

- Führen Sie den vollständigen Prozess des Schlüsselaustauschs gemäß dem Ekert-91 Protokoll durch. der erzeugte Schlüssel sollte mindestens 25 Bits lang sein. Außerdem sollten Sie das Vorhandensein eines Lauschers anhand Ihrer aufgenommenen Daten effektiv ausschließen können.

- Geben Sie im Protokoll eine vollständige Liste der genutzten Basen und der erhaltenen Bitwerte von Alice und Bob an. Machen Sie kenntlich, welche Basen verworfen wurden und welche zur Schlüsselgenerierung weiterverwendet wurden.

- Erstellen Sie in der AR-App aus einer Bitfolge eine kleine Grafik, die Sie mit ihrem Schlüssel versenden können. Nutzen Sie den generierten Schlüssel, um diese Nachricht zu verschlüsseln.

- Entschlüsseln Sie die Nachricht durch erneutes Addieren des Schlüssels. Was können Sie beobachten? Wie lässt sich diese Beobachtung durch den verwendeten Bell-Zustand erklären? Diskutieren Sie Ihre Beobachtungen und Ursachen für mögliche Abweichungen vom Idealzustand im Protokoll.

- Erzeugen Sie einen Produktzustand, indem Sie zusätzliche Polfilter in den Aufbau einfügen. Justieren Sie **nur durch Anpassung der Polfilterhöhen- und Winkel** den Aufbau bestmöglich nach, um geeignete Zählraten zu erhalten.

- Messen Sie erneut den S-Parameter und vergleichen Sie ihr Ergebnis mit dem des verschränkten Zustandes. Diskutieren Sie im Protokoll die Auswirkungen auf die Schlüsselerzeugung mit einem Produktzustand.