AR-Versuch „Quantenschlüsselaustausch“ – Didaktischer Kommentar & Übersicht zu den Versuchsteilen

Der AR-Versuch „Quantenschlüsselaustausch“ wurde mit dem Ziel entwickelt, einen komplexen quantenoptischen Versuchsaufbau für Studierende zugänglich zu machen und über geeignete interaktive Visualisierungen das Verständnis der zugrundeliegenden physikalischen Konzepte zu fördern.

Auf den folgenden Seiten finden Sie eine Übersicht über die Inhalte und Tätigkeiten in den verschiedenen Versuchsteilen des Versuchs, sowie die damit verbundenen didaktischen Zielsetzungen

Allgemeines: Die Lernumgebung richtet sich an Studierende im fortgeschrittenen Bachelorpraktikum und umfasst verschiedene Experimente mit polarisationsverschränkten Einzelphotonenpaaren. Die Photonenpaare werden mittels spontaner parametrischer Fluoreszenz in einem BBO-Kristall erzeugt. Die Studierenden lernen dabei schrittweise den verwendeten Experimentalaufbau kennen und untersuchen zunächst verschiedene Eigenschaften des erzeugten Quantenzustandes, bevor sie diese Eigenschaften zur Generierung eines abhörsicheren Schlüssels mit dem Ekert-91-Verfahren anwenden. Der Fokus liegt dabei in der Unterstützung des Erwerbs grundlegender Fachkonzepte der Quantenoptik sowie von Kenntnissen, wie diese Konzepte im Experiment untersucht werden können. Konkret umfasst der Versuch die folgenden experimentellen Aktivitäten:

- Winkelabhängige Polarisationsmessung von Einzel- und Koinzidenzzählraten
- Bestimmung der Polarisationskorrelationen zwischen den Photonenpaaren
- Prüfung der CHSH-Ungleichung
- Quantenschlüsselaustausch mittels Ekert-91-Protokolls
- Vergleich der Ergebnisse mit denen eines Produktzustandes

Die oben beschriebenen Experimente sind typischerweise eher unanschaulich, da die optischen Aufbauten oft komplex sind und sich Lernenden der Bezug zwischen experimentellen Handlungen, resultierenden Messwerten und abstrakter Modellebene häufig nicht erschließt. Augmented-Reality (AR) Technologie ermöglicht während der Durchführung der Versuche die Einblendung von verschiedenen interaktiven Visualisierungen, die diese Bezüge hervorheben sollen. Die Visualisierungen basieren dabei stets auf den realen Messdaten, die die Studierenden selbst generieren und sind interaktiv mit den Komponenten des Aufbaus gekoppelt. Experimentelle Handlugen wie das Drehen eines Wellenplättchens wirken sich daher unmittelbar auf die dargestellten Visualisierungen aus.

Die AR- Darstellungen umfassen:

- Darstellung von Strahlengängen und Strukturen innerhalb des Aufbaus
- Kurzinformationen zu den optischen Komponenten
- Echtzeit-Darstellung der gewählten Messbasis
- Interaktive Datenplots zur Messung von Einzel- und Koinzidenzzählraten
- Raster-Darstellung einzelner gemessener Bits
- Darstellung von gemessenen Korrelationen zwischen Koinzidenzzählraten und einzelnen Bitfolgen
- Modell-Visualisierung des verschränkten Quantenzustandes in der gewählten Basis
- Interface für Quantenschlüsselaustausch nach dem Ekert-91-Protokoll und Übermittlung von eigenen Nachrichten

Zudem ist die Lernumgebung als Multi-User Umgebung ausgelegt, d. h. die Studierenden arbeiten zu zweit und schlüpfen jeweils in die Rolle von Alice und Bob, um die Messungen und den Schlüsselaustausch durchzuführen. Dabei können sie selbst entscheiden, wann und auf welche Weise sie Informationen über einen klassischen Kanal austauschen, um beispielsweise Korrelationen zwischen ihren Messergebnissen zu bestimmen oder sich die gewählten Messbasen mitzuteilen.

Strukturierung und Visualisierungen:

Die Lernumgebung ist in sieben aufeinander aufbauende Teile gegliedert, die auf verschiedene Konzepte fokussieren und jeweils einen Teil der oben genannten Visualisierungen bereitstellen:

1. Aufbau
2. Zufall
3. Korrelation
4. Verschränkung
5. Nichtlokalität
6. Kryptographie
7. Produktzustand

Diese Versuchsteile werden in der folgenden Übersicht einzeln vorgestellt.

Kapitel 1: Aufbau

Aufgabe: Verschaffe Dir einen Überblick über den Aufbau und die verwendeten Komponenten

Tätigkeiten & Zielsetzung:

- Aktivierung von Vorwissen aus der Vorbereitung zum Versuch
- Die verschiedenen Sektionen des Aufbaus (Einzelphotonenquelle, Walkoff-Kompensation, Messeinrichtung) als Funktionseinheiten kennen lernen
- Den aus der Einführung bekannten schematischen Versuchsaufbau mit dem Realaufbau verknüpfen
- Interaktion mit den AR-Elementen einüben

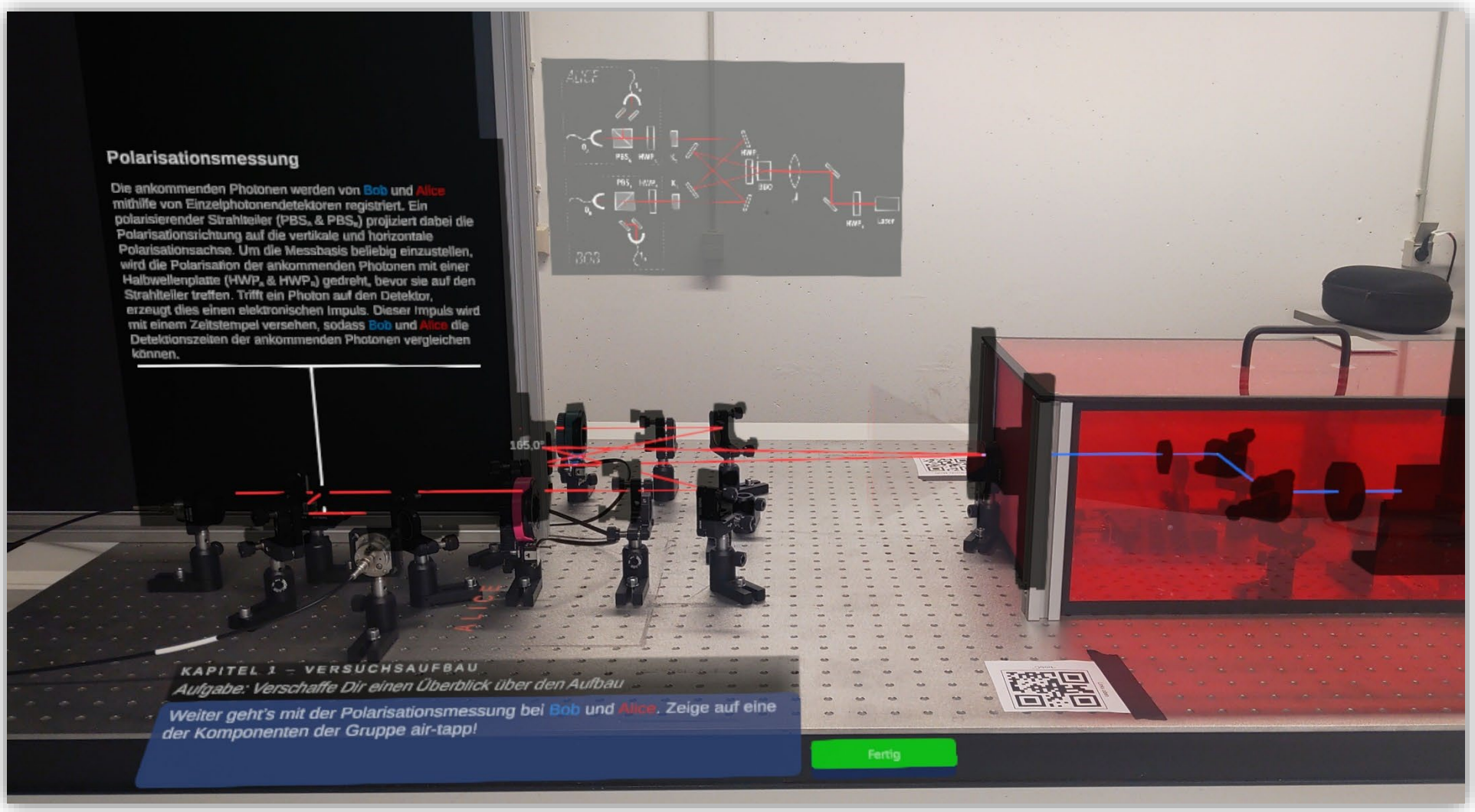
Visualisierungen:

- Schematische 2D-Skizze des Versuchsaufbaus
- Info-Texte zu den verschiedenen Funktionseinheiten
- Overlay des Strahlengangs im realen Setup

Beschreibung der Funktionalität:

Die Studierenden haben zuvor Einführungsmaterialien erhalten, in denen eine schematische Skizze des Versuchsaufbaus dargestellt ist. Das Übertragen der schematischen Darstellung auf den realen Aufbau ist jedoch eine Herausforderung, da die realen Komponenten sich alle sehr ähnlich sehen und der Verlauf des Strahlengangs nicht auf den ersten Blick erkennbar ist. Der eingeblendete Strahlengang soll daher die Struktur des Aufbaus besser erkennbar machen. Zudem wird parallel die den Studierenden bekannte schematische Skizze dargestellt, sodass diese mit dem Realaufbau verglichen und einzelne Komponenten identifiziert werden können. Die Skizze und der Strahlengang im Setup bauen sich dabei, beginnend beim Pumplaser, schrittweise auf. Die Studierenden werden in der AR-Umgebung dazu aufgefordert, bestimmte Schlüsselkomponenten im Setup (z. B. Pumplaser, BBO-Kristall, Messeinrichtung) anzuwählen. Haben sie die korrekte Komponente gewählt, wird ihnen ein kurzer Info-Text zur Funktion der jeweiligen Komponente oder einer Gruppe von Komponenten angezeigt, bevor sich die Skizze und der Strahlengang bis zur nächsten Schlüsselkomponente ausbreitet. Der Strahlengang bleibt während der folgenden Versuchsteile permanent sichtbar. Desweiteren lassen sich nach Abschluss der Aufgabe kurze Tooltipps zu jeder einzelnen Komponente durch Anwählen der Komponente anzeigen.

Screenshot zum Versuchsteil „Aufbau“:



Kapitel 2: Zufall

Aufgabe: Miss die Polarisationsabhängigkeit der ankommenden Einzelphotonen

Tätigkeiten & Zielsetzung:

- Sich mit dem Messinterface vertraut machen
- Aufnehmen von Einzelzählraten und einer Sequenz einzelner Bits (ohne Vergleich der Messwerte mit Alice/Bob)
- Aus den aufgenommenen Messdaten Schlussfolgerungen über den Polarisationszustand der Photonenquelle ableiten: Die Messergebnisse ergeben ein Zufallsmuster für einzelne Messereignisse, bzw. liefern gleichverteilte Zählraten für jede gewählte Messrichtung.

Visualisierungen:

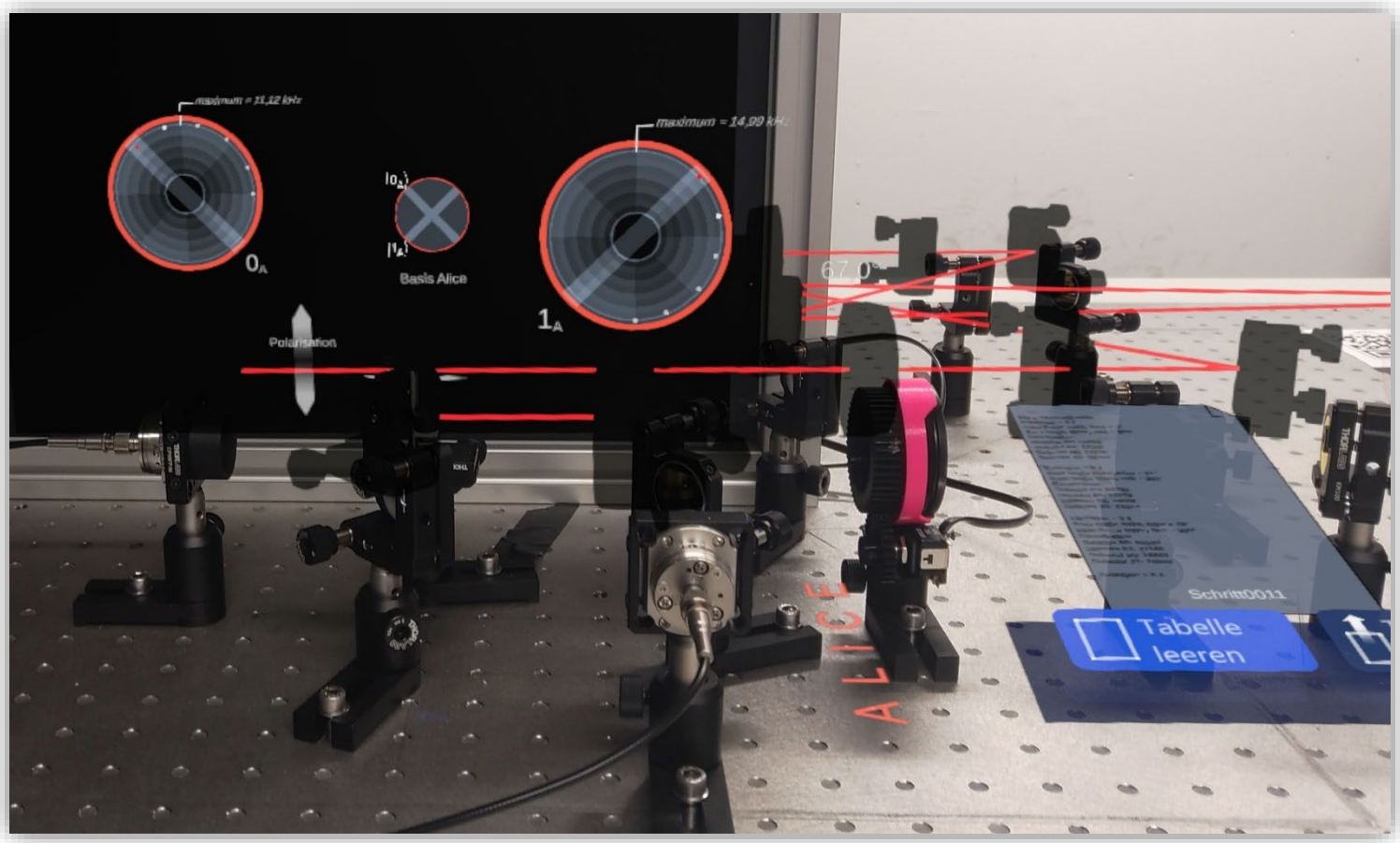
- Auf Zählratenebene:
    - Messdiagramm für die aufgenommenen Zählraten gegen gewählten Messwinkel (je ein Polarplot für jeden der beiden eigenen Detektoren)
- Auf Ebene einzelner Messereignisse:
    - Raster-Darstellung für 25 aufgenommene Messereignisse und die jeweils zugeordneten Bitwerte
- Für beide Darstellungsebenen:
    - Darstellung des aktuell eingestellten Messwinkels als Zahlenwert und als Koordinatensystem an den jeweiligen Messkanälen
    - Interface zur Aufnahme, Export & Löschen von Messdaten

Beschreibung der Funktionalität:

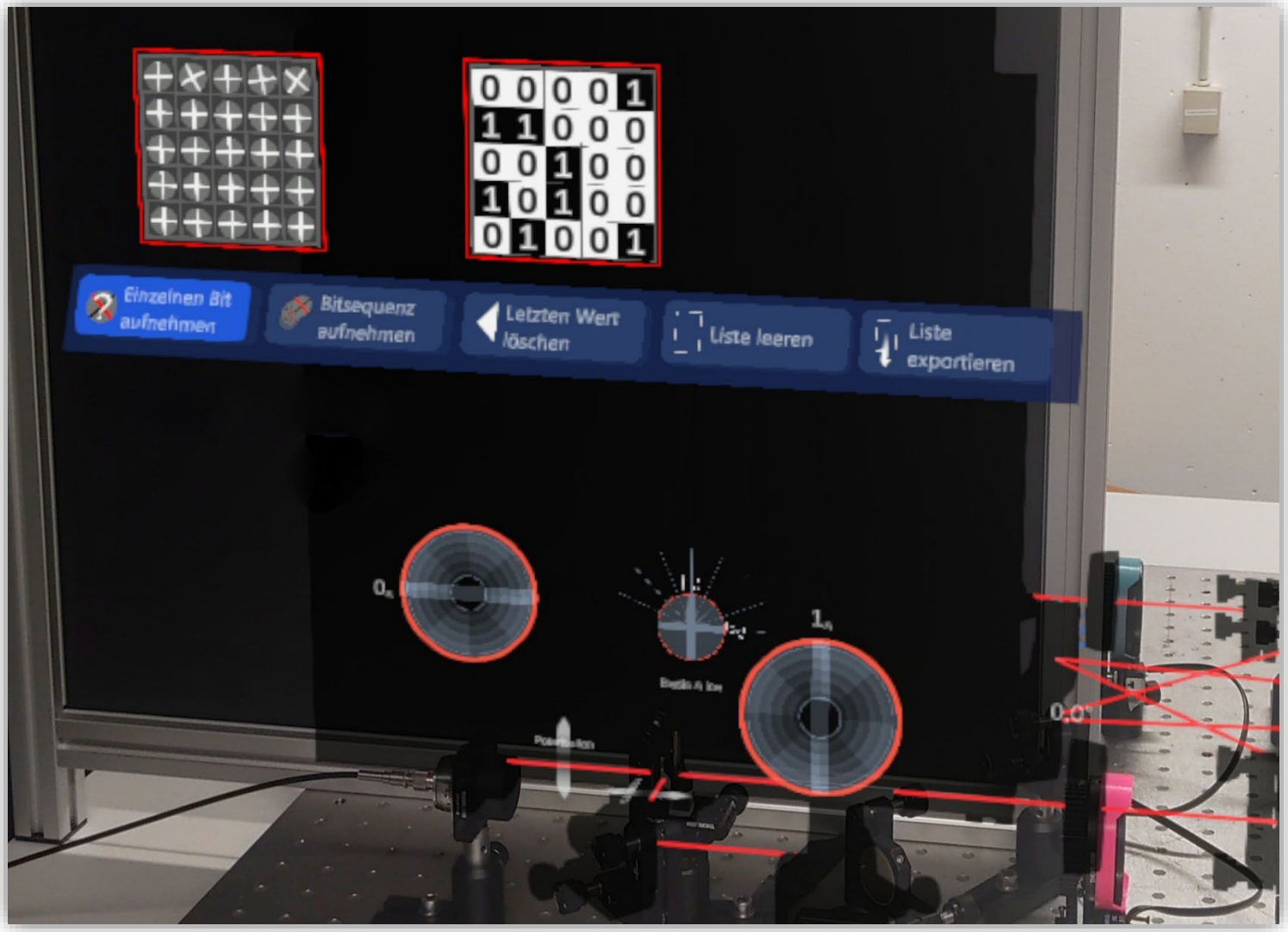
In diesem Versuchsteil werden zwei zentrale Ebenen der Visualisierung von Messdaten eingeführt. Es können sowohl Messungen an Ensembles als Zählraten in einem Polarplot dargestellt werden, als auch einzelne Messereignisse in Form eines Bitrasters. Die Studierenden arbeiten in diesem Versuchsteil zunächst unabhängig voneinander, da in diesem Versuchsteil kein Austausch von Informationen nötig ist. Zunächst messen sie in der Zählraten-Darstellung die Einzelzählrate in Abhängigkeit vom gewählten Basiswinkel. Dazu variieren sie über die Rotation eines Halbwellenplättchens die Messbasis und nehmen jeweils Messwerte für die Zählrate auf. Die erhaltenen Werte werden direkt unter dem gemessenen Winkel in der Polardarstellung angezeigt. Das Ergebnis ist eine nahezu konstante Zählrate unabhängig vom gewählten Basiswinkel.

In der Einzelbit-Darstellung messen die Studierenden jeweils für verschiedene Basiswinkel eine Bitsequenz aus 25 Einzelphotonen. Nachdem 25 Messwerte vorliegen, können die zu den Messwerten gehörigen Bitwerte bestimmt werden. Das Ergebnis ist eine Zufallsfolge.

Screenshot zum Versuchsteil „Zufall“: Polarplots der Zählraten-Darstellung



Screenshot zum Versuchsteil „Zufall“: Bitraster aus der Einzelbit-Darstellung



Kapitel 3: Korrelation

Aufgabe: Miss die Polarisationsabhängigkeit der ankommenden Photonenpaare

Tätigkeiten & Zielsetzung:

- Aufnehmen von Koinzidenzzählraten, sowie Vergleich von gemessenen Bitsequenzen zwischen Alice und Bob
- Unterscheidung zwischen Einzel- und Koinzidenzmessungen nachvollziehen
- Korrelationen qualitativ abschätzen
- Aus den aufgenommenen Messdaten Schlussfolgerungen über die Winkelabhängigkeit von Korrelationen ziehen

Visualisierungen:

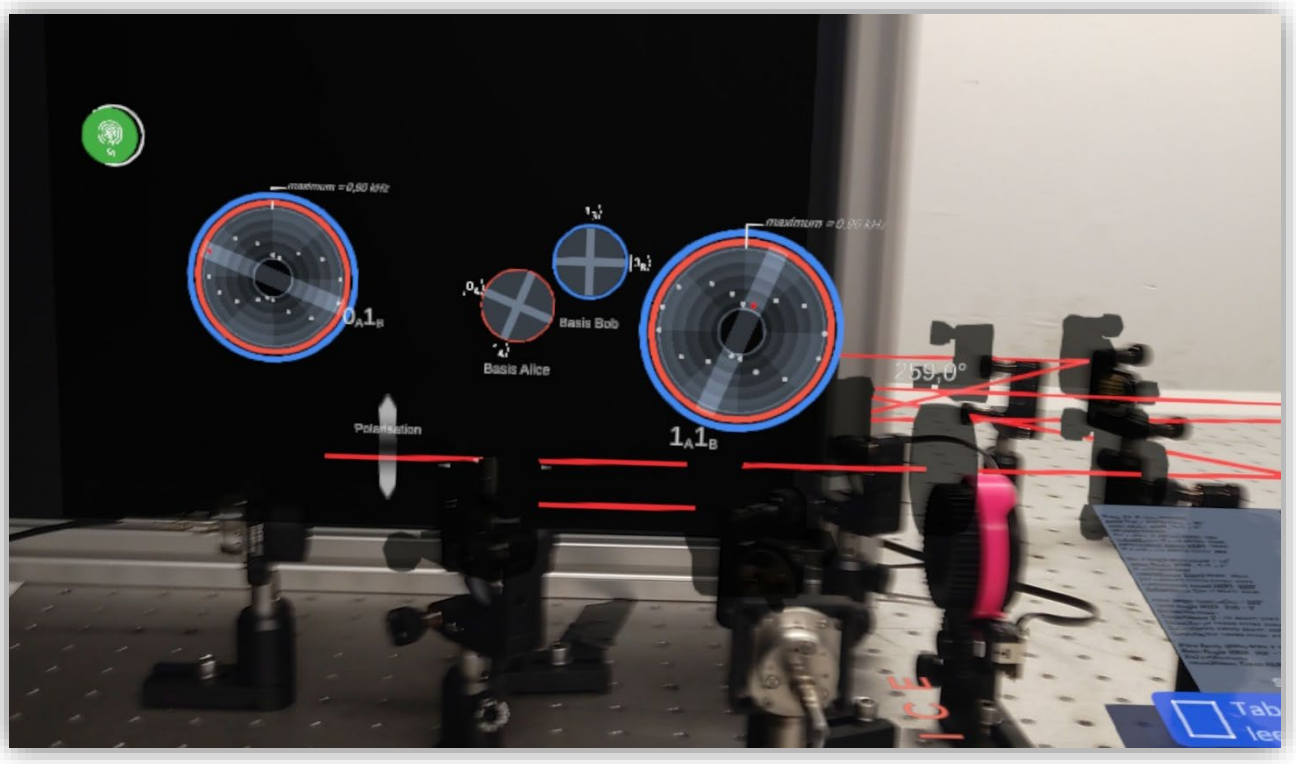
- Auf Zählratenebene:
    - Messdiagramm für die aufgenommenen Koinzidenzzählraten gegen gewählten Messwinkel (je ein Polarplot für jeden der beiden eigenen Detektoren)
- Auf Ebene einzelner Messereignisse:
    - Raster-Darstellung für 25 aufgenommene Messereignisse und die jeweils zugeordneten Bitwerte
    - Interface zum Vergleich der gewählten Basen von Alice und Bob und der zugehörigen Bitwerte durch Überlagerung
- Für beide Darstellungsebenen:
    - Darstellung des aktuell eingestellten Messwinkels als Zahlenwert und als Koordinatensystem an den jeweiligen Messkanälen
    - Falls öffentlicher Kommunikationskanal aktiviert: Echtzeit-Darstellung der Messbasis des zweiten Teilnehmers
    - Interface zur Aufnahme, Export & Löschen von Messdaten

Beschreibung der Funktionalität:

Die Tätigkeiten gleichen denen im vorherigen Versuchsteil, allerdings werden Alice und Bob hier aufgefordert, öffentlich Informationen über ihre Messungen miteinander zu teilen, um Koinzidenzereignisse ermitteln zu können. Über einen entsprechenden Button im Interface kann die Information über die aktuell eingestellte Basis für den Partner sichtbar gemacht werden und zwischen Einzel- und Koinzidenzmessung umgeschaltet werden. Alice und Bob müssen sich gemeinsam auf das Vorgehen zur Messung der Winkelabhängigkeit der Koinzidenzen einigen. Ein Teilnehmer sollte eine feste Messbasis einstellen. Die andere Teilnehmerin variiert die Messbasis durch Rotation ihres Halbwellenplättchens und nimmt für verschiedene Winkel die Koinzidenzzählrate auf. Anders als im vorherigen Versuchsteil ergibt sich nun eine klare

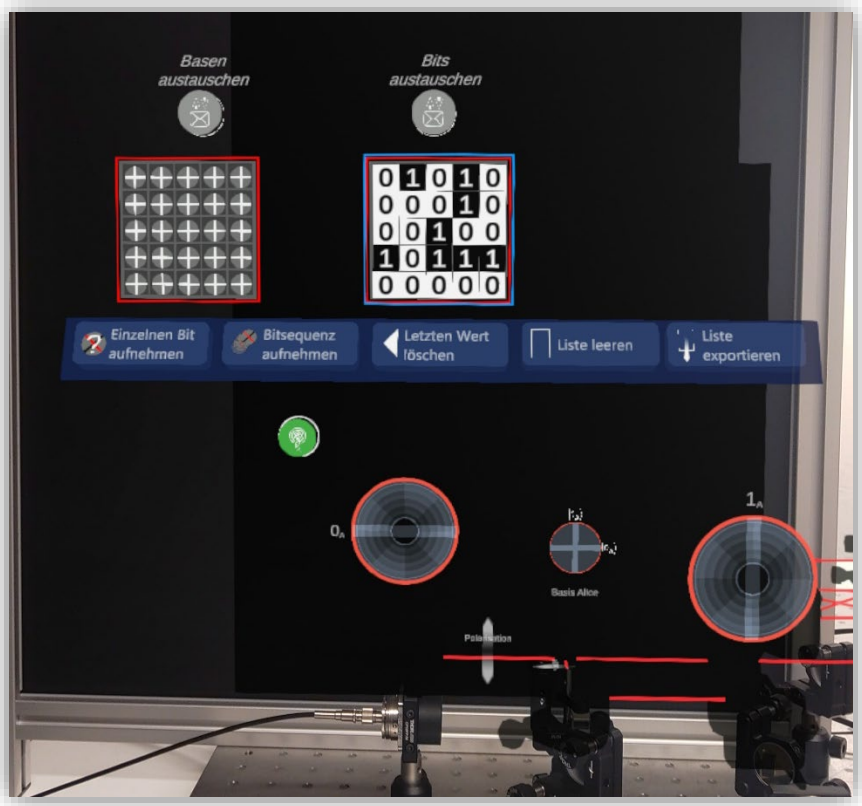
Winkelabhängigkeit der Zählrate. Die Wiederholung für verschiedene Messbasen zeigt, dass sich ein Maximum stets für senkrechte Polarisationsrichtungen bei Alice und Bob ergibt (Bell-Zustand $|\Psi^-\rangle$). In der Einzelbit-Darstellung messen die Studierenden wieder zunächst für sich eine Sequenz aus 25 Messereignissen, können aber vorab die Information über ihre Basis teilen. Nach Aufnahme von 25 Werten können sie auch ihre Bitwerte vergleichen, indem sie die erhaltenen Raster austauschen und grafisch überlagern. Auf diese Weise lässt sich abschätzen, wie stark die Messergebnisse von Alice und Bob miteinander korrelieren. Die Wiederholung der Messung für verschiedene Winkeldifferenzen zeigt, dass die Korrelationen nur dann auftreten, wenn Alice und Bob ihre Messbasis aufeinander abstimmen.

Screenshot zum Versuchsteil „Korrelation“: Polarplots der Zählraten-Darstellung

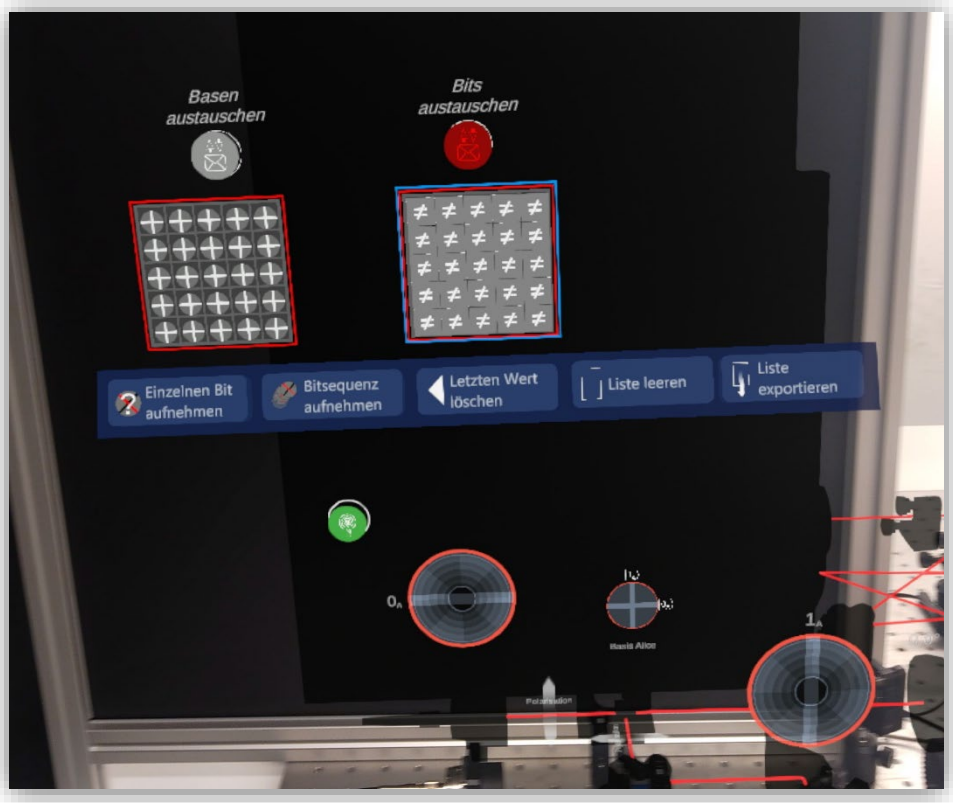


Screenshot zum Versuchsteil „Korrelation“: Bitraster aus der Einzelbit-Darstellung

Links: Vor dem Vergleichen der Messergebnisse von Alice & Bob



Rechts: Nach dem Vergleich der Messergebnisse von Alice & Bob



Kapitel 4: Verschränkung

Aufgabe: Zeige, dass die Polarisationskorrelationen der Photonenpaare die Bell'sche Ungleichung verletzen

Tätigkeiten & Zielsetzung:

- Argumentation der Bell'schen Ungleichung nachvollziehen
- Quantitative Messung von Korrelationsfunktionen durchführen
- CHSH-Ungleichung prüfen

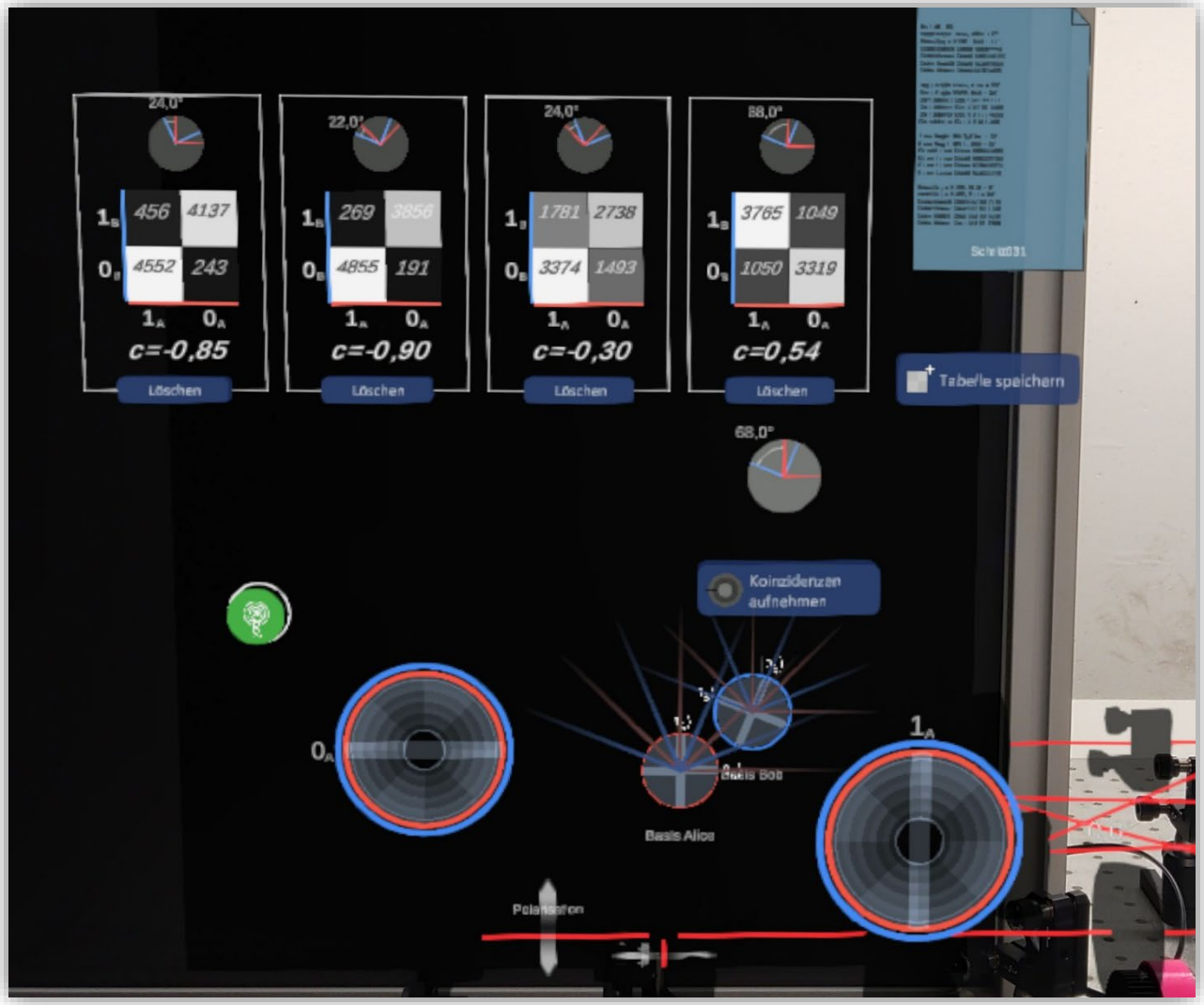
Visualisierungen:

- Auf Zählratenebene:
    - Messdiagramm für die von Alice und Bob gemessene Korrelationsfunktion zu einer bestimmten Winkelkombination (2x2-Matrix)
- Darstellung des aktuell eingestellten Messwinkels als Zahlenwert und als Koordinatensystem an den jeweiligen Messkanälen
- Visuelle Marker zur Einstellung der Basiswinkel mit maximaler Verletzung der CHSH-Ungleichung
- Falls öffentlicher Kommunikationskanal aktiviert: Echtzeit-Darstellung der Messbasis des zweiten Teilnehmers
- Interface zur Aufnahme, Export & Löschen von Messdaten

Beschreibung der Funktionalität:

In den vorangegangenen Versuchsteilen konnte anhand der Messdaten bereits auf das Vorliegen von Polarisationskorrelationen geschlossen werden. Auch konnten die Studierenden beobachten, dass die Korrelationen ausschließlich von der relativen Winkeldifferenz zwischen den Basen von Alice und Bob abhängen. Diese Beobachtungen werden hier nun weiter formalisiert. Die Studierenden können für von ihnen ausgewählte Winkelkombinationen den Wert der Korrelationsfunktion ermitteln lassen. Dieser Wert wird als Zahl und als grafische 2x2-Matrix dargestellt. Es können nacheinander bis zu vier Korrelationsfunktionen gemessen und gleichzeitig angezeigt werden. Ziel ist es, die Winkelkombinationen so zu wählen, dass die CHSH-Ungleichung verletzt wird.

Screenshot zum Versuchsteil „Verschränkung“: Messung der Korrelationsfunktionen zur CHSH-Ungleichung



Kapitel 5: Nichtlokalität

Aufgabe: Untersuchen Sie anhand der Visualisierungen, wie der Quantenzustand modelliert werden kann.

Tätigkeiten & Zielsetzung:

- Darstellung des Quantenzustandes in verschiedenen Basen untersuchen
- Bedeutung von Nichtlokalität anhand der Darstellungen diskutieren

Visualisierungen:

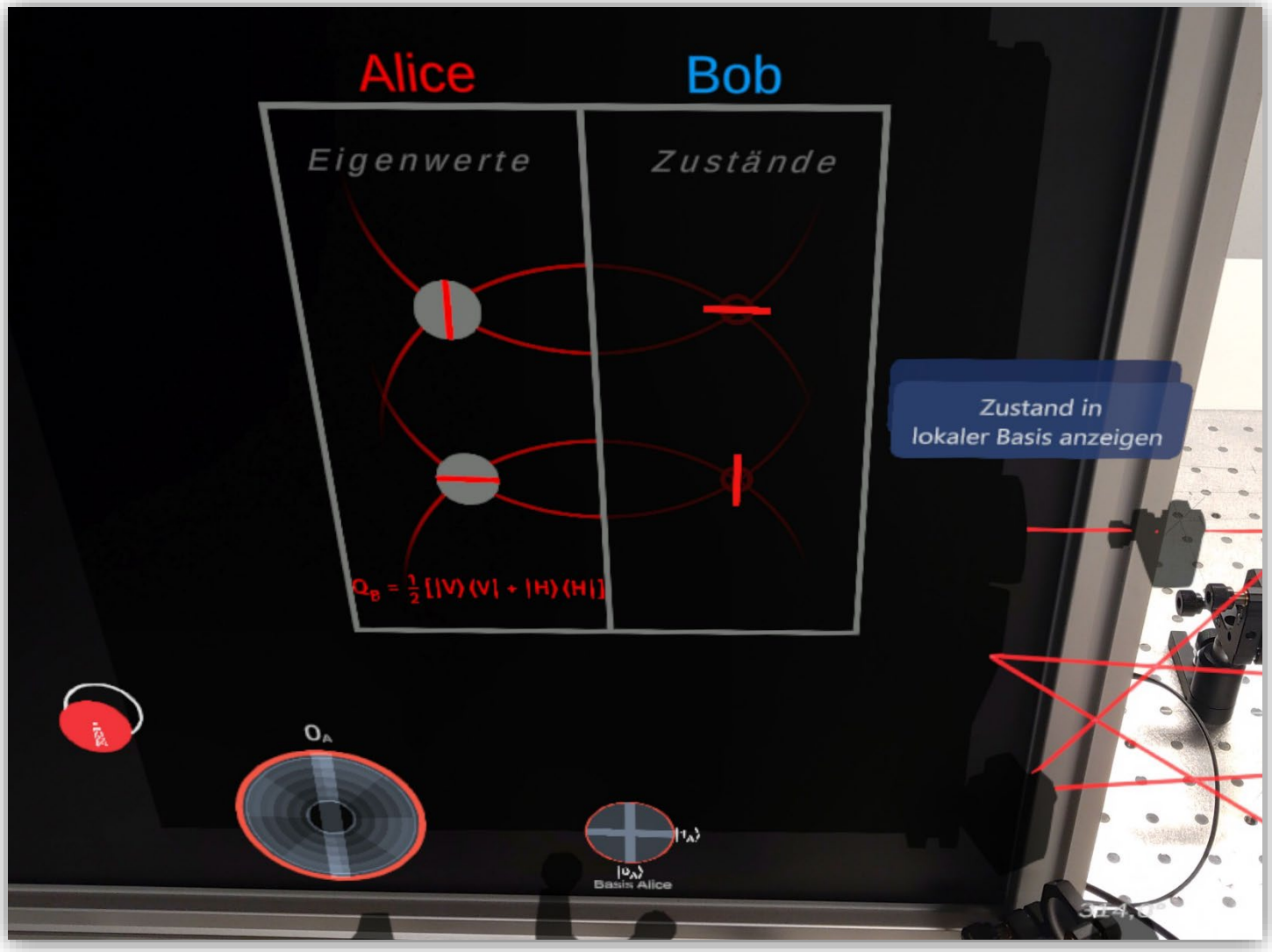
- Darstellung des verschränkten Quantenzustandes $|\Psi^-\rangle$ im Bra/Ket-Formalismus
- Visuelle Darstellung des Zustandes in der aktuell gewählten lokalen Messbasis
- Falls öffentlicher Kommunikationskanal aktiviert: Echtzeit-Darstellung der Messbasis des zweiten Teilnehmers

Beschreibung der Funktionalität:

Während die vorherigen Versuchsteile das Phänomen der Verschränkung primär durch Visualisierung von Messdaten darstellen, geht es in diesem Versuchsteil um die interaktive Modellierung des Zweiphotonenzustandes als Superpositionszustand. Die Darstellung des Zustandes im Bra-Ket-Formalismus wird hierzu auch grafisch umgesetzt Da der verwendete Bell-Zustand $|\Psi^-\rangle$ invariant unter Basistransformation ist, lässt er sich in jeder Basis als Superposition von zueinander senkrecht polarisierten Photonenpaaren darstellen. Die Darstellung des Zustandes ist dabei an die aktuell gewählte lokale Messbasis angepasst. Die Darstellungen sind dabei vor allem als Anregung gedacht, über die Interpretation von Messdaten hinaus theoretische Aspekte der Verschränkung zu thematisieren. So lässt sich beispielsweise erkennen, dass Alice zwar durch Wahl ihrer lokalen Messbasis den Zustand von Bob „festlegen“ kann und es sich insofern um einen nichtlokalen Zustand handelt. Durch Einblenden der lokalen Messbasis von Bob wird jedoch auch deutlich, dass hierdurch keine Informationsübertragung stattfindet, da Bob seinerseits keine Informationen über die zu wählende Basis besitzt. Außerdem würde aus Bobs Sicht dieselbe Argumentation anwendbar sein, wodurch deutlich wird, dass eine rein lokale Argumentation nicht ausreicht, um den Quantenzustand eindeutig zu beschreiben.

Die in der AR eingeblendeten Aufgaben und Fragen zielen darauf ab, dass Alice und Bob über diese Aspekte miteinander und der Versuchsbetreuung ins Gespräch kommen und auf potentielle Widersprüche in ihrem bisherigen Verständnis des Phänomens Verschränkung aufmerksam werden.

Screenshot zum Versuchsteil „Nichtlokalität“: Darstellung des Superpositionszustandes



Kapitel 6: Kryptographie

Aufgabe: Nutze den verschränkten Zustand, um abhörsicher einen Schlüssel für die Nachrichtenübertragung zu generieren

Tätigkeiten & Zielsetzung:

- Erworbene Kenntnisse aus den vorherigen Teilen anwenden
- Ekert-91 Protokoll zur Schlüsselverteilung abhörsicher umsetzen
- Entscheiden und reflektieren, welche Informationen öffentlich geteilt werden können

Visualisierungen:

- Auf Ebene einzelner Messereignisse:
    - Raster-Darstellung für 25 aufgenommene Messereignisse und die jeweils zugeordneten Bitwerte
- Interface zum Vergleich der gewählten Basen von Alice und Bob und der zugehörigen Bitwerte durch Überlagerung
- Interface zum Erstellen einer individuellen Nachricht aus 25 Bits
- Interface zum Ver- und Entschlüsseln von Nachrichten mit dem zuvor generierten Schlüssel
- Interface zur Aufnahme, Export & Löschen von Messdaten

Beschreibung der Funktionalität:

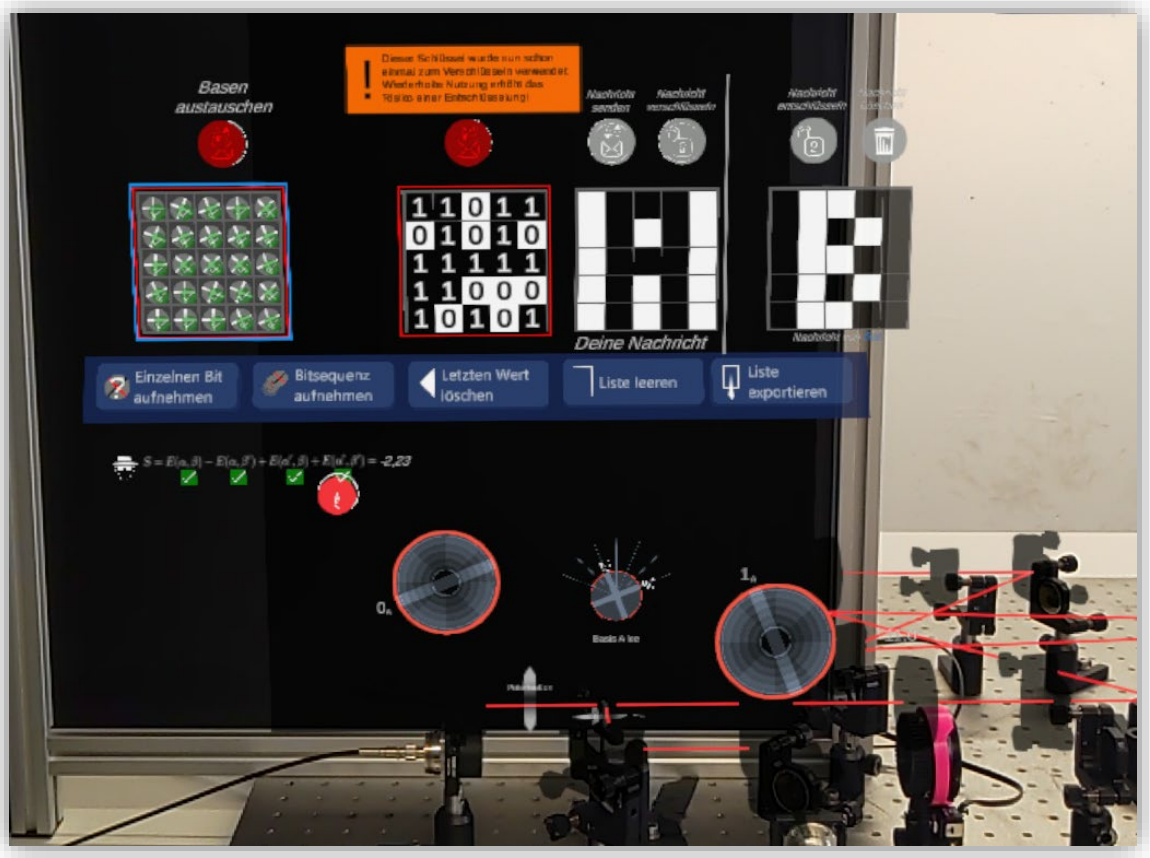
In diesem Versuchsteil sollen die Studierenden auf Grundlage der vorherigen Aufgaben und der zuvor eingeführten Visualisierungen möglichst eigenständig den Schlüsselaustausch nach dem Ekert-91-Protokoll durchführen. Bevor der Schlüsselaustausch stattfindet, können Alice und Bob jeweils eine individuelle Nachricht aus 25 Bits codieren, die später verschlüsselt und versendet werden kann.

Zur Erzeugung des Schlüssels arbeiten die Studierenden mit den Visulisierungen der Einzel-Bit-Darstellungen. Sie nehmen zunächst insgesamt 25 Bits auf und wählen für jedes Bit zufällig aus den Basen der CHSH-Ungleichung aus. Nach dem öffentlichen Vergleich der Messbasen können im Interface die Basen mit ungleichen Winkeln verworfen werden. Danach werden die freien Plätze im Raster durch weitere Messungen gefüllt. Dies wird solange wiederholt, bis ein vollständiger Schlüssel aus 25 Bits entstanden ist. Mit diesem Schlüssel kann dann die eigene Nachricht verschlüsselt bzw. erhaltene Nachrichten entschlüsselt werden.

Die Anwendung ermittelt aus den verworfenen Messwerten automatisch den Wert der zugehörigen Korrelationsfunktion. Sobald alle vier Kombinationen der CHSH-Ungleichung vorhanden sind, wird ein Zahlenwert für den Bell-Parameter angezeigt. Verletzt der so erhaltene Wert die

CHSH-Ungleichung, können die Studierenden sicher sein, dass kein Spion mithört. Die Studierenden können in diesem Versuchsteil verschiedene Informationen öffentlich senden. Neben den gewählten Basen beinhaltet dies die erhaltenen Bits, sowie die eigene Nachricht in ver- und entschlüsselter Form. Sollten die Studierenden jedoch Informationen öffentlich preisgeben, die die Abhörsicherheit des Schlüssels oder der Nachricht selbst gefährden, werden Sie durch ein Popup-Fenster darüber informiert, dass die Übertragung nun nicht mehr sicher ist und der Schlüsselaustausch muss erneut durchgeführt werden.

Screenshot zum Versuchsteil „Kryptographie“: Schlüsselerzeugung



Kapitel 7: Produktzustand

Aufgabe: Untersuche, wie ein Spion im Aufbau enttarnt werden kann.

Tätigkeiten & Zielsetzung:

- Anwenden der zuvor erworbenen Kenntnisse auf einen Produktzustand
- Vergleich der Ergebnisse mit denen des verschränkten Zustandes
- Interpretieren der unterschiedlichen Ergebnisse im Kontext von abhörsicherer Kommunikation

Visualisierungen:

- Auf Ebene einzelner Messereignisse:
    - Raster-Darstellung für 25 aufgenommene Messereignisse und die jeweils zugeordneten Bitwerte
- Interface zum Vergleich der gewählten Basen von Alice und Bob und der zugehörigen Bitwerte durch Überlagerung
- Interface zum Erstellen einer individuellen Nachricht aus 25 Bits
- Interface zum Ver- und Entschlüsseln von Nachrichten mit dem zuvor generierten Schlüssel
- Interface zur Aufnahme, Export & Löschen von Messdaten

Beschreibung der Funktionalität:

Damit die Studierenden reflektieren können, warum das Ekert-91 Verfahren intrinsisch abhörsicher ist, sollen sie im letzten Versuchsteil untersuchen, wie sich die Anwesenheit eines Spions im Aufbau auf die Schlüsselübertragung auswirkt. Der Spion wird durch zwei zusätzliche Polfilter im Aufbau simuliert, der aus dem verschränkten Zustand einen Produktzustand erzeugt. Die Studierenden führen erneut den Schlüsselaustausch durch. und beobachten, welche Unterschiede sich ergeben. Beispielsweise wird der erhaltene Wert für die CHSH-Ungleichung nun unter dem klassischen Grenzwert von 2 liegen. Außerdem werden aufgrund der weniger starken Korrelationen vermehrt Fehler im Schlüssel auftreten. Diese Gegenüberstellung soll den Studierenden die Unterschiede zwischen verschränktem und klassischem Zustand noch einmal vor Augen führen.