Abschlussbericht

zum Teilvorhaben Hochdimensionalität durch Pulsmoden

im Verbundprojekt Quantum Information and Communication with High-Dimensional Encodings

Zuwendungsempfänger: Universität Paderborn

Förderkennzeichen: 16KIS1120

Laufzeit des Vorhabens: 01.03.2020-28.02.2024

Teil I: Kurzbericht

Quantentechnologien der neuesten Generation bieten Vorteile für verschiedenste Anwendungsfelder. Insbesondere sind derzeit Quantencomputer stark in den Medien vertreten. Zum einen wegen ihrem potenziellen Nutzen in Anwendungen wie der Material- und Medikamentenentwicklung, zum anderen auch wegen ihrer Implikationen für Sicherheitsanwendungen. Derzeit genutzte Verschlüsselungsmethoden werden, so es einen leistungsfähigen Quantencomputer gibt, obsolet.

Die Quantenschlüsselverteilung (Englisch: quantum key distribution; QKD) stellt eine Lösung für die Sicherheitsproblematik dar. Sie ermöglicht den Austausch eines absolut abhörsicheren Schlüssels, welcher dann in einem nächsten Schritt genutzt werden kann, um sensible Daten zu verschlüsseln. Dabei beruht die Sicherheit der QKD nicht auf mathematischen Algorithmen, sondern quantenmechanischen Prinzipien, insbesondere dem „Beobachtereffekt“. Dieser besagt, dass jegliche Messung an einem Quantenobjekt zu einer Beeinflussung führt, was es erlaubt, Lauscher zuverlässig zu erkennen. Obwohl erste QKD-Systeme derzeit kommerziell erhältlich sind, sind ihre Leistungskennzahlen noch nicht in einem Bereich, der sie für echte Anwendungen relevant macht. Schlüsselraten sind sehr gering und die erreichbare Sicherheit ist durch experimentelle Fehler und Umwelteinflüsse kompromittiert.

In diesem Projekt ging es um die experimentelle Untersuchung hochdimensionaler (HD) Zeit-Frequenz-QKD. Hierbei bedeutet hochdimensional, dass Information nicht nur wie bei herkömmlicher QKD in Nullen und Einsen kodiert wird, sondern ein größeres Alphabet zur Verfügung steht. Dies hat zwei Hauptimplikationen: zum einen ermöglicht ein größeres Kodierungsalphabet eine höhere Schlüsselrate, zum anderen ist eine hochdimensionale Kodierung weniger anfällig für experimentelles Rauschen. Damit adressiert HD QKD die Limitierungen bisher kommerziell eingesetzter QKD-Systeme. Eine Kodierung im Zeit-Frequenz-Bereich ist dabei besonders attraktiv, da Information weiterhin in einer einzigen räumlichen Feldverteilung transmittiert wird. Damit sind Zeit-Frequenz-Kodierungen mit der existierenden Kommunikationsinfrastruktur, welche auf Einmodenfasern basiert, kompatibel.

Zu Beginn des Projekts gab es allerdings keine Dekoder, welche hochdimensionale Information in Zeit und Frequenz hätten auslesen können. Die Entwicklung und Verifizierung eines solchen Bauteiles war eines der Hauptziele dieses Projekts und wurde erfolgreich erreicht. Unser Dekoder

basiert auf einem sogenannten multi-output Quantenpulsgatter (mQPG). Hierbei handelt es sich um ein integriert-optisches Bauteil, in welchem ein Eingangssignal bei Wellenlängen im Telekommunikationsbereich (C-Band) mittels einer Summenfrequenzerzeugung mit klassischen Lichtpulsen bei Wellenlängen von 860nm zu grünen Wellenlängen umgesetzt wird. Die Besonderheit des mQPG ist einerseits die Anpassung der Wellenleiterdispersion (das Eingangssignal und das Pumplicht haben die gleiche Gruppengeschwindigkeit) und andererseits die besondere Mikrostrukturierung, welche es erlaubt, verschiedene Eingangssignale zu verschiedenen Ausgangsfrequenzen umzusetzen. Zuletzt adressiert das mQPG einstellbare Zeit-Frequenz-Überlagerungen. Hierdurch können hochdimensional kodierte Eingangssignale zu verschiedenen Ausgangsfrequenzen konvertiert und anschließend ausgelesen werden. Im Experiment wurde nachgewiesen, dass dieser Prozess mit einer Güte von mehr als 99% realisiert werden kann.

Weiterhin wurde im Projekt eine maßgeschneiderte Quantenlichtquelle für maximal Zeit-Frequenz-verschränkte Photonenpaare entwickelt. Derartige Quantenzustände können die Basis fortgeschrittener QKD-Protokolle sein. Das Besondere an der hier entwickelten Quelle ist, dass die Dimensionalität der Verschränkung programmatisch zwischen zwei und 21 eingestellt werden kann. Somit kann die Quelle flexibel verschiedene Anwendungen bedienen, ohne dass die verwendete Hardware angepasst oder ausgetauscht werden muss.

Schließlich wurde eine Architektur für HD QKD entwickelt, welche eine Senderstation und den Dekoder beinhaltet. Die Arbeitsweise des Dekoders wird hier so gewählt, dass passiv und zufällig eine von zwei Messbasen gewählt wird, eine Grundlage der QKD. Zusammen mit Projektpartnern wurden eine optimierte Kodierung erarbeitet, welche alle experimentellen Fehler mit in Betracht zieht. Diese Architektur wurde patentrechtlich geschützt, da sie als extrem vielversprechend für zukünftige Zeit-Frequenz-QKD erachtet wird.

Die Kernergebnisse des Projekts sind zusammengefasst die Realisierung einer maßgeschneiderten, flexiblen Verschränkungsquelle für Zeit-Frequenz-QKD, die Implemetierung eines hochdimensionalen Zeit-Frequenz-Dekoders für QKD, sowie die Identifizierung einer optimierten Architektur für HD QKD, welche die experimentellen Leistungskennzahlen der entwickelten Bauteile mit berücksichtigt.

Abschlussbericht

zum Teilvorhaben Hochdimensionalität durch Pulsmoden

im Verbundprojekt Quantum Information and Communication with High-Dimensional Encodings

Zuwendungsempfänger: Universität Paderborn

Förderkennzeichen: 16KIS1120

Laufzeit des Vorhabens: 01.03.2020-28.02.2024

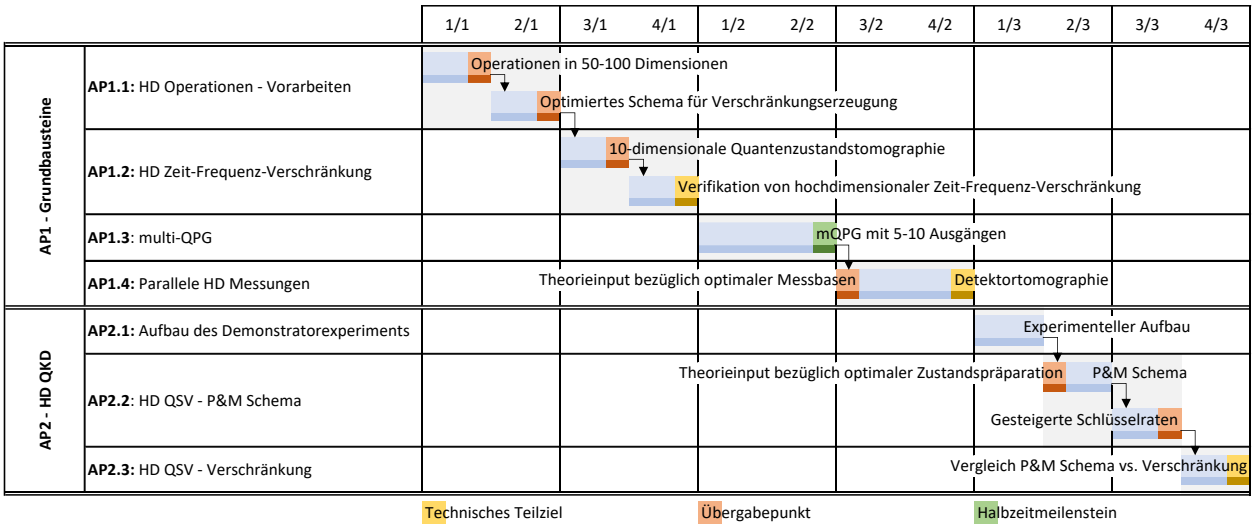
Teil II: Ausführlicher Sachbericht

Zusammenfassung: Im Rahmen des QuantERA Verbundes QuICHE untersuchte die Universität Paderborn (UPB) in diesem Teilprojekt hochdimensionale Quantenschlüsselverteilung mit Zeit-Frequenz-Kodierungen.
Gemäß dem Arbeitsplan wurde eine Quantenlichtquelle entwickelt, welche Zeit-Frequenz-verschränkte Photonenpaare mit einer einstellbaren Dimensionalität – diese entspricht der Größe des Kodierungs-Alphabets – erzeugt. Experimentell wurden Dimensionalitäten zwischen eins und 21 nachgewiesen.
Weiterhin wurde ein mehrdimensionaler Dekoder entwickelt, der verschiedene Zeit-Frequenz-Kodierungen auslesen kann. Bei diesem Bauteil können Größe des Kodierungsalphabets sowie die Art der Kodierung rein softwareseitig, das heißt, ohne Änderung der experimentellen Hardware, ausgewählt werden, was eine bisher unerreichte Flexibilität gewährt.
In Zusammenarbeit mit Verbundpartnern wurde weiterhin eine optimierte Architektur für experimentelle hochdimensionale Quantenschlüsselverteilung identifiziert, welche mit den entwickelten Bauteilen kompatibel ist. Der in dieser Architektur verwendete Dekoder wurde inzwischen patentrechtlich geschützt.
Die Arbeiten in diesem Projekt verliefen überwiegend gemäß der Teilvorhabenbeschreibung. Allerdings konnte die finale experimentelle Demonstration der hochdimensionalen Quantenschlüsselverteilung aufgrund von Verzögerungen bei der Lieferung von Kernkomponenten des experimentellen Aufbaus nicht fertiggestellt werden. Dies wird derzeit im Nachgang des Projekts fertiggestellt.

1. Motivation und Arbeitsplan

Dieses Projekt hatte zum Ziel, hochdimensionale Quantenschlüsselverteilung (Englisch: quantum key distribution; QKD) mit einer Zeit-Frequenz-Kodierung zu untersuchen. Quantenschlüsselverteilung erlaubt es, absolut abhörsichere Kommunikationskanäle zu realisieren, deren Sicherheit auf quantenmechanischen Prinzipien beruht. Hochdimensionale Quantenschlüsselverteilung, bei der ein Kodierungsalphabet zum Einsatz kommt, das mehr Einträge als „0“ und „1“ enthält, erlaubt eine höhere Datenrate und Robustheit im Hinblick auf experimentelle Fehler und damit eine größere Sicherheit in realistischen Anwendungsszenarien.

Hierzu sollten im Projektverlauf eine maßgeschneiderte Quantenlichtquelle, ein hochdimensionaler Dekoder, sowie eine optimierte Architektur für hochdimensionale Quantenschlüsselverteilung realisiert werden. Die Arbeiten waren gemäß dem Arbeitsplan auf zwei sukzessive Arbeitspakete (APs) verteilt und innerhalb der APs in Arbeitsschritte unterteilt.



AP1 – Grundbausteine deckt hierbei die Entwicklung der Quantenlichtquelle und des Dekoders ab, während sich die Arbeiten in AP2 – HD QKD auf die optimierte Architektur konzentrieren.

2. Darstellung der Arbeiten

AP1.1: HD Operationen – Vorarbeiten

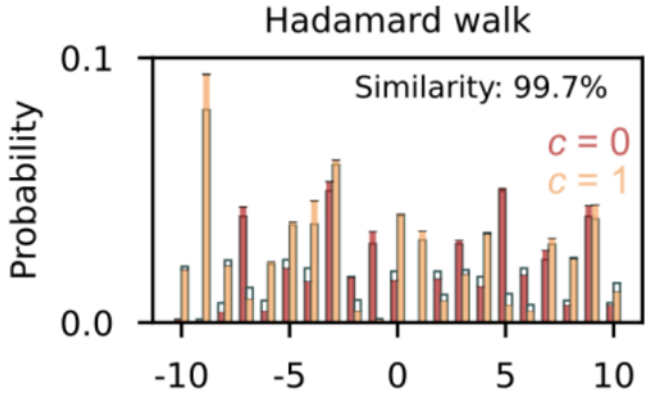


Abb. 1. *Messergebnis eines frequenzkodierten Quantenwalks. Theorie (schwarze Linien) und Experiment (farbige Balken) weißen eine Übereinstimmung von 99.7% auf.*

Unter Verwendung eines sogenannten Quantenpulsgatters (QPGs) wurden hochdimensionale unitäre Operation auf 64 Frequenz-Bins implementiert. Dabei wurden Güten von mehr als 98% erreicht. Bei einer Skalierung zu 128 Frequenz-Bins sinkt diese Güte auf 80%. Im Experiment wurden die Eingangs-Frequenz-Bins bei einer Zentralwellenlänge von 1540nm mit einer spektralen Breite von 40GHz und sogenannten Schutzbanden von 36GHz zwischen benachbarten Bins definiert. Das Pumplicht, welches die QPG-Operation bestimmt, hatte eine Zentralwellenlänge von 860nm, die weiteren Parameter der Pump-Bins sind gleich derer des Signals. Als Anwendungsszenario wurden Quantenwalk-Operationen realisiert, da diese ein wohlbekanntes Testsystem darstellen. Abbildung 1 zeigt exemplarisch eine Messung. Theorie und Experiment stimmen exzellent überein.

AP1.2: HD Zeit-Frequenz-Verschränkung

In diesem Arbeitsschritt wurde eine in Zeit und Frequenz maximal verschränkte Photonenpaarquelle mit bis zu 21 Dimensionen implementiert. Die Quelle basiert auf parametrischer Fluoreszenz (Englisch: parametric down-conversion; PDC) in einem periodisch gepolten Wellenleiter in Kaliumtitanylphosphat mit maßgeschneiderter Dispersion und erzeugt Photonen bei einer Zentralwellenlänge von 1540nm, ideal für Quantenschlüsselverteilung.

Der durch PDC erzeugte Biphotonen-Zustand wird vollständig durch seine gemeinsame spektrale Amplitude (Englisch: joint spectral amplitude; JSA) beschrieben, die durch spektrale Formung der Pumppulse angepasst werden kann. Das Formen des Pumpspektrums als so genannte Kosinus-Kernel-Funktion (Englisch: cosine kernel; CK) der Ordnung n ermöglicht die Erzeugung eines $(n+1)$-dimensionalen, maximal verschränkten Zustands. Das Einstellen der Dimensionalität des Zustands durch spektrale Formung ermöglicht es, die gewünschte Dimensionalität des Systems programmatisch und ohne Hardwareänderungen zu wählen. Die spektrale Formung von CK-Moden höherer Ordnung erfordert aufgrund ihrer schnelleren oszillatorischen Anteile einen Wellenformer mit höherer Auflösung. Ein entsprechend optimierter Wellenformer für die Erzeugung von CK-Moden der Ordnung 21 wurde implementiert.

Um die modale Struktur des erzeugten Bi-Photonen-Zustands genau zu charakterisieren, sollte man eine Schmidt-Zerlegung der experimentellen JSA durchführen: Die effektive Dimensionalität des Zustands wird durch die Schmidt-Zahl K beschrieben, und der maximal verschränkte Zustand wird durch das Vorhandensein von K Schmidt-Moden mit gleicher Gewichtung verifiziert. Eine vollständige Charakterisierung der JSA wäre jedoch sehr ressourcenaufwändig.

Aus diesem Grund wurde die Dimensionalität des erzeugten verschränkten Zustands durch

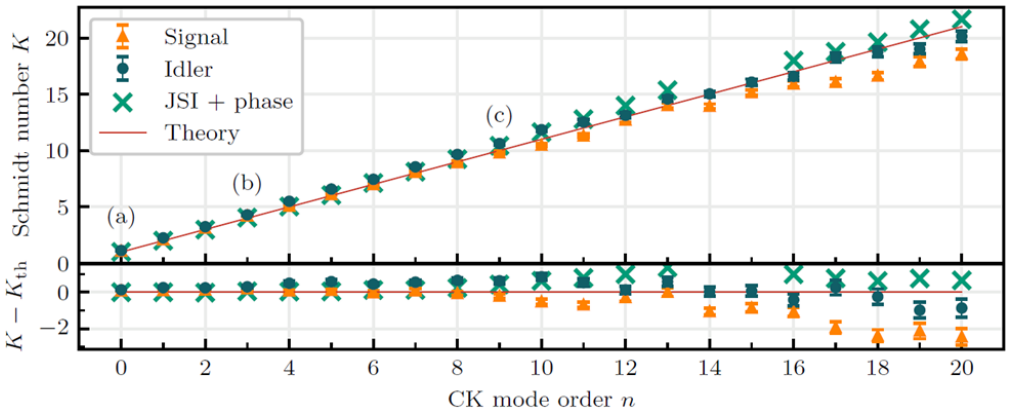


Abb. 2. *Experimentell ermittelte Dimensionalität* K *der erzeugten Zustände als Funktion der Ordnung* n *der CK-Mode des Pumpspektrums. Die verschiedenen Symbole beschreiben verschiedene Messmethoden, die rote Linie zeigt den Verlauf für ideale, maximal verschränkte Zustände.*

ressourceneffiziente Korrelationsmessungen zweiter Ordnung (g(2)) verifiziert. Das g(2) ist mit der Photonenzahlstatistik der Quelle verknüpft, die ihrerseits von der effektiven Dimensionalität der erzeugten Zustände abhängt. Allerdings liefern g(2)-Messungen allein nicht ausreichend Informationen, um maximale Verschränkung zu verifizieren. Aus diesem Grund wurde neben den g(2)-Messungen noch die sogenannte gemeinsame spektrale Intensität (Englisch: joint spectral intensity; JSI) aufgenommen. Die JSI ist das Betragsquadrat der JSA. Zusammen mit der Kenntnis der Phase des geformten Pumpspektrums kann von der JSI auf die zugrundeliegende JSA geschlossen werden. Diese kann dann mithilfe einer Schmidt-Zerlegung analysiert werden. Zusammen mit den g(2)-Messungen lässt es diese Methode zu, die erzeugten Zustände zu verifizieren.

Abb. 2 zeigt die Dimensionalität *K* der erzeugten Zustände als Funktion der Ordnung *n* der CK-Mode des Pumpspektrums. Die Messungen bestätigen die Erzeugung maximal Zeit-Frequenz-verschränkter Zustände mit einer wählbaren Dimensionalität bis *K*=21. Abb. 3 zeigt weiterhin exemplarisch einige gemessene JSI-Verteilungen, welche mit etablierten Bildbearbeitungsalgorithmen nachbearbeitet wurden, um die feinen Features auflösen zu können.

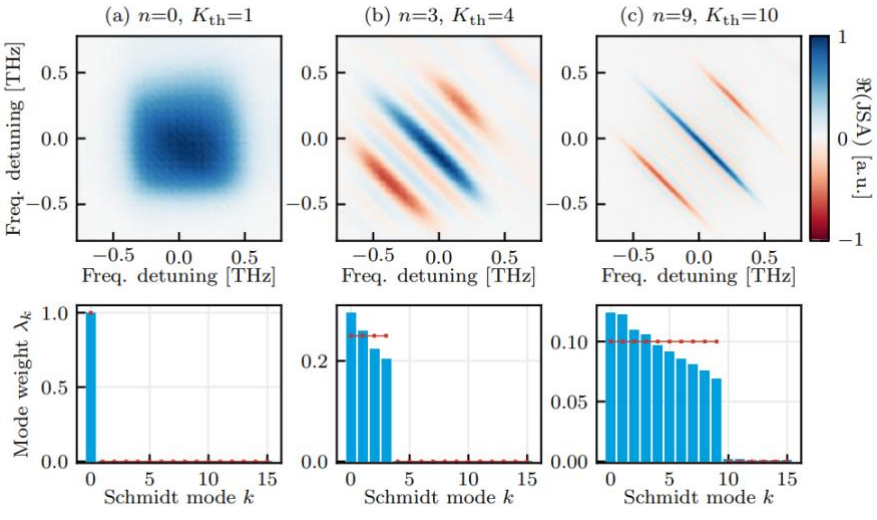


Abb. 3 *Exemplarische Darstellung der JSI der erzeugten Photonenpaare für drei verschiedene Pumpmoden. Die untere Zeile zeigt die Gewichtung der einzelnen Anteile der Zustände, die rote Linie ist wieder der Verlauf für ideale, maximal verschränkte Zustände..*

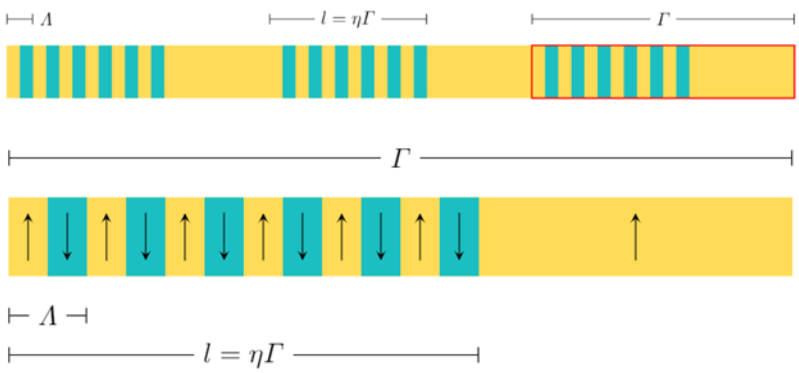


Abb. 4. *Schemazeichnung der mQPG-Wellenleiterstruktur, in der periodisch gepolte Bereich (gelb-grün) und nicht-gepolte Bereiche (gelb) alternieren.*

AP1.3: multi-QPG

Zur Dekodierung hochdimensionaler Zustände in Zeit-Frequenz QKD wurde ein sogenanntes multi-output QPG (mQPG) entwickelt. Dieses Bauteil basiert auf einer Wellenleiterstruktur mit einer Superpolung, wie in Abb. 4 dargestellt. Hierbei wechseln sich Bereiche mit und ohne periodische Polung ab. Dies führt zu einer Phasenanpassungskurve mit mehreren Peaks, deren Anzahl, Breiten und Abstände ausschließlich durch die geometrischen Parameter der Superpolung definiert sind (siehe Abb. 5). Diese Peaks entsprechen den Ausgangskanälen des Dekoders.

Gemäß diesem Zusammenhang wurden neue Lithografiemasken entworfen und entsprechende Proben vor Ort in Paderborn hergestellt. Die nachstehende Tabelle zeigt eine Aufstellung der optimierten Parameter der mQPG-Struktur.

Parameter	**Gewählter Wert**	**Zugehörige Größe**	**Resultierender Wert**
Probenlänge *L*	4 cm	Peakbreite	25 GHz
Superpolungs-Periode *Γ*	2 mm	Abstand der Peaks	0.49 THz
Gepolte Länge einer Einheit *l*	0.4 mm	Breite der Einhüllenden	2.44 THz

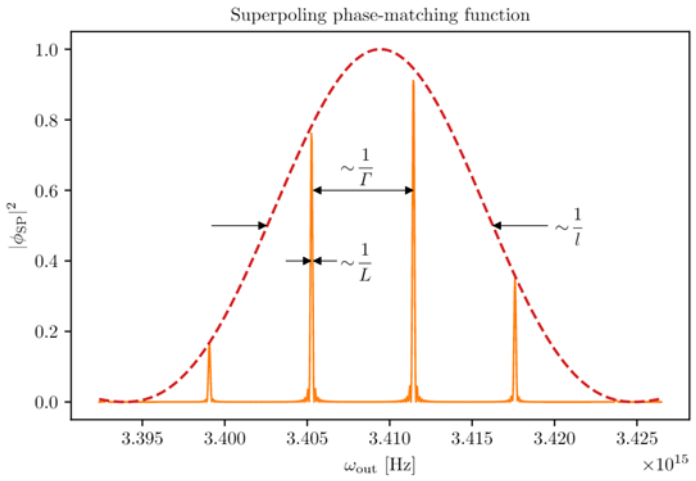


Abb. 5. *Die resultierende Phasenanpassungskurve (orange) des mQPGs ist durch die geometrischen Parameter der Polungsstruktur vollständig definiert.*

Nach der Herstellung der mQPG-Proben wurde diese in den Laboren der UPB charakterisiert. Zunächst wurde die experimentelle Phasenanpassungsintensität durch einen Wellenlängenscan charakterisiert, bei dem die Pumpwellenlänge von 834 bis 874nm in Schritten von 8nm und die Eingangswellenlänge von 1500 bis 1600nm in Schritten von 0,5nm bewegt wurde (siehe auch AP2.1 – Aufbau des Demonstratorexperiments). Diese Messung ergab eine exzellente Übereinstimmung mit der Theorie, ein Resultat der hohen Probenqualität (siehe Abb. 6).

Im Anschluss an die Verifizierung der Probenfunktionalität, wurde das mQPG in den experimentellen Aufbau für die vorläufigen Messungen zur hochdimensionalen Zeit-Frequenz Dekodierung eingebaut.

AP1.4 – Parallele HD Messungen

<u>2-dimensionale Messungen.</u> Um die Realisierung paralleler, hochdimensionaler Messungen mittels des mQPG zu verifizieren, wurde zunächst eine 2-dimensionale Operationsweise gewählt. Diese entspricht der klassischen Qubit-Kodierung und dient als Benchmark für die nachfolgende höher-dimensionale Operation des mQPG.
Für diese erste Demonstration wurde ein kommerzieller CCD-Spektrograph zur Detektion des Ausgangslichts des mQPG verwendet. Als Kodierungs-Basis wählten wir Hermit-Gauß (HG) Moden und ihre Überlagerungen. In diesem Beispiel betrug die charakteristische Frequenzbreite der HG-Moden 0,30THz.

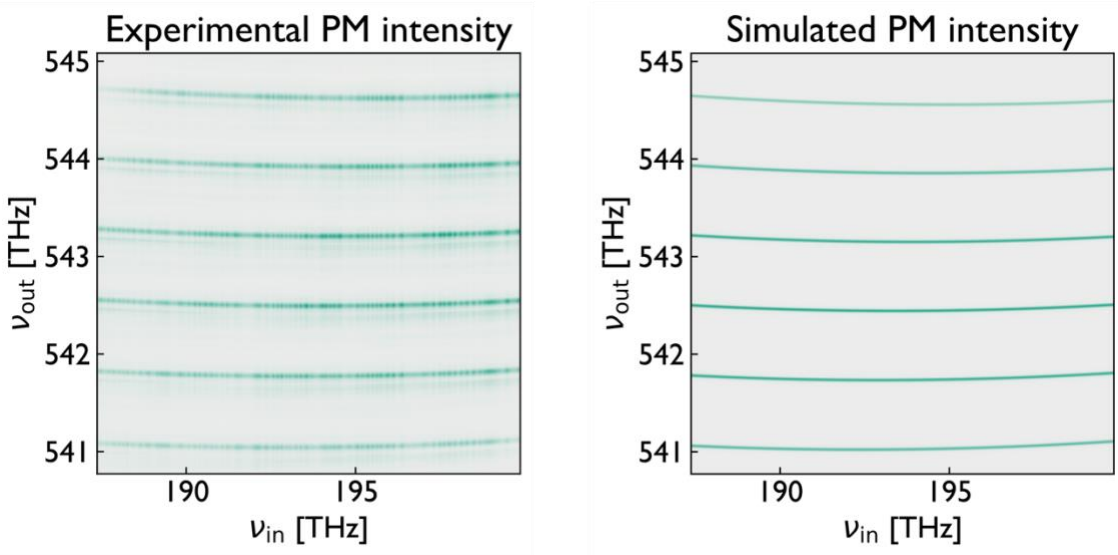


Abb. 6. Vergleich der experimentellen (links) und simulierten (rechts) Phasenanpassungsintensität für einen Wellenleiter mit denselben Polungsparametern.

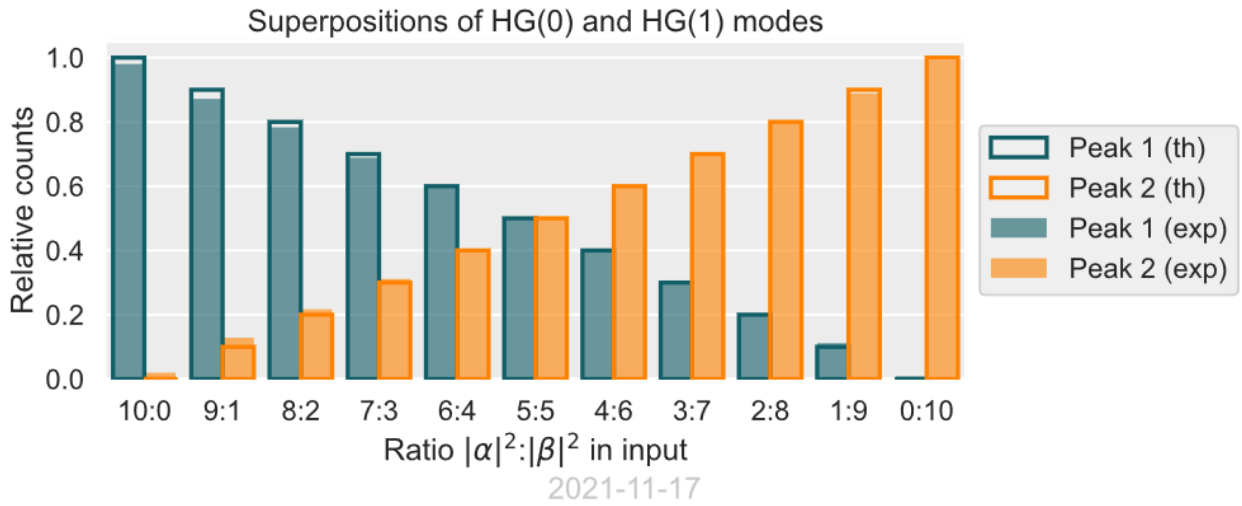


Abb. 7. Experimentelle Daten des zweidimensionalen Betriebs des mQPG bei einer Überlagerung von Eingangszuständen $\alpha|HG_0\rangle + \beta|HG_1\rangle$. Die Grafik zeigt die relative Intensität in den beiden mQPG Ausgängen als Funktion der Gewichtungskoeffizienten des Eingangszustands.

Um die 2-dimensionale Operation zu charakterisieren, wurde ein Eingangszustand der Form $\alpha|HG_0\rangle + \beta|HG_1\rangle$ erzeugt. Dieser beschreibt eine kohärente Superposition einer fundamentalen und ersten höheren HG-Mode, mit Gewichtungsfaktoren α und β. Dieser wurde dann in das mQPG gesendet, welches derart eingestellt war, dass es den $|HG_0\rangle$ Anteil in einen der beiden Ausgänge konvertierte und den $|HG_1\rangle$ Anteil in den anderen. Mittels des Spektrographen wurden die beiden Ausgänge detektiert und ihre relative Intensität ermittelt. Die Ergebnisse dieser Messungen sind in Abb. 7 dargestellt. Es zeigt sich, dass Theorie und Experiment auch in diesem Fall hervorragend übereinstimmen, das mQPG also sehr gut in der Lage ist, HG-Moden Qubits zu dekodieren.

In einem nächsten Schritt wurde verifiziert, dass das mQPG auch auf konjugierten Basen operieren kann. Diese bestehen aus kohärenten Superpositionen der Vektoren der ursprünglichen Kodierungsbasis und sind essenziell für die Sicherheit von Quantenschlüsselverteilung. Im Experiment erzeugen wir zuerst ein Eingangssignal der Form $|HG_0\rangle$ und senden es in das mQPG. Das mQPG dekodiert zunächst die originale Basis (vgl. Abb. 7). Danach stellen wir es auf die zwei

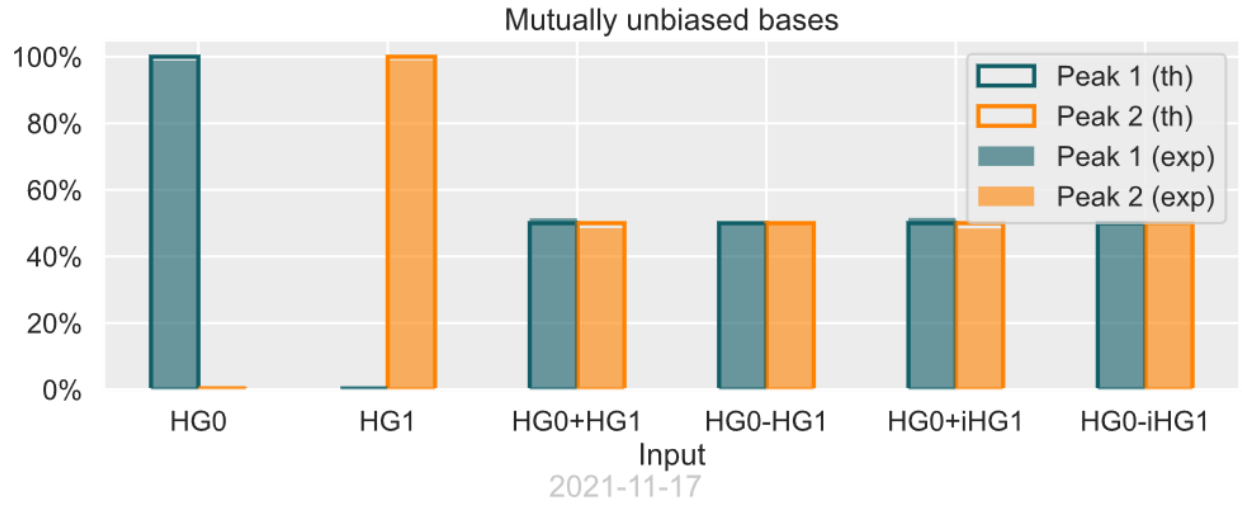


Abb. 8. Experimentelle Daten des zweidimensionalen Betriebs des mQPG auf einem Satz von konjungierten Basen. Die Grafik zeigt die Anzahl der relativen Ausgansintensitäten des mQPG für die verschiedenen Elemente der konjungierten Basen eines zweidimensionalen Hilbert-Raums.

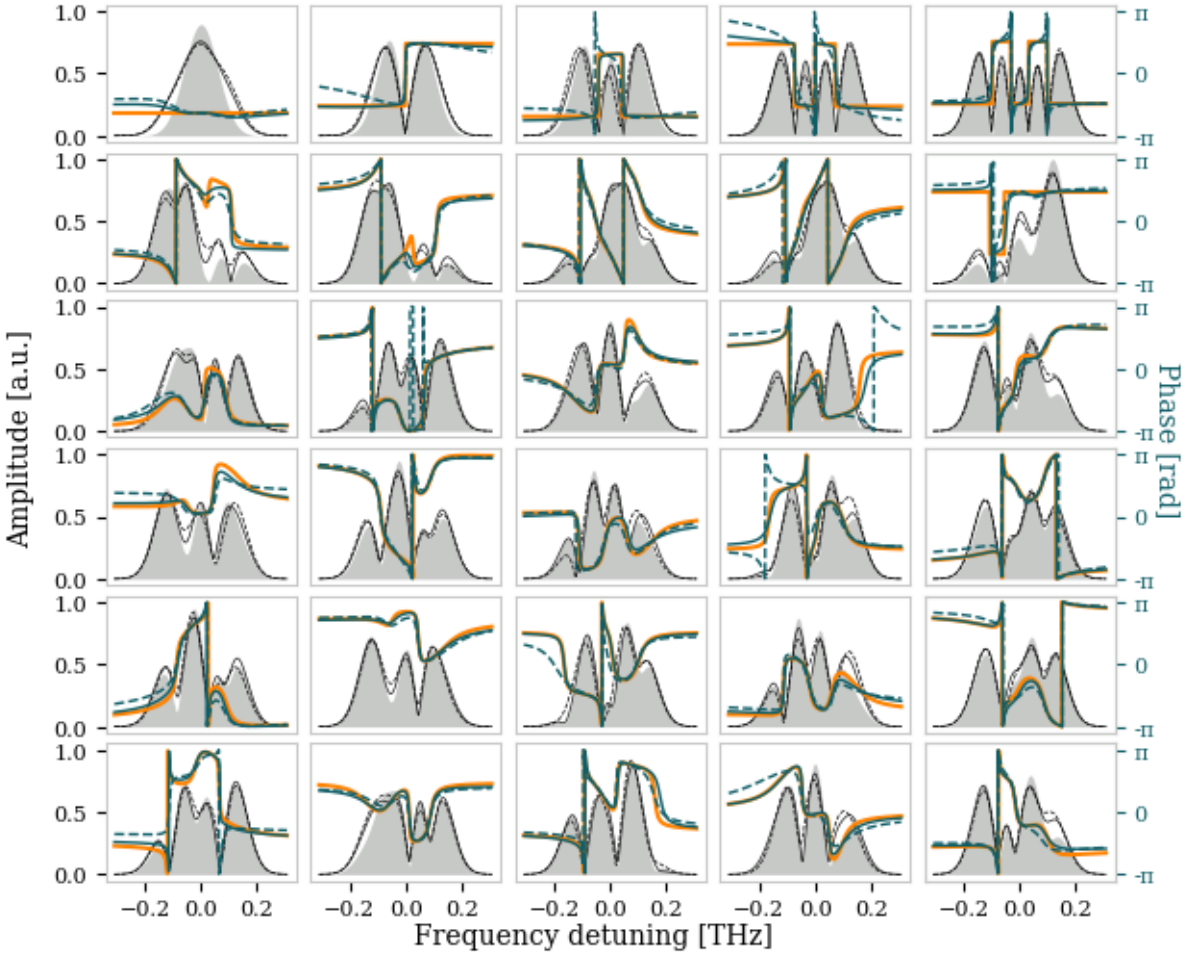


Abb. 9. Erste Eigenmoden der POVM-Elemente (5 für jede der 6 konjungierten Basen). Details zur Darstellung können dem Text entnommen werden.

möglichen konjugierten Basen ein. Erwartungsgemäß messen wir für die konjugierten Basen die gleiche Intensität in den beiden Ausgängen des mQPG. Danach werden die Messungen für ein Eingangssignal in $|HG_1\rangle$ wiederholt. Dier Ergebnisse sind in Abb. 8 gezeigt und bestätigen, dass das mQPG auf konjugierten Basen operieren kann. Damit ist das mQPG grundsätzlich als Dekoder für Quantenschlüsselverteilung geeignet.

5-dimensionale Detektortomographie. In einem nächsten Schritt wurde das mQPG jetzt als Dekoder für hochdimensionale Signale verwendet. Dazu wurde der CCD-Spektrograph durch ein Einzelphotonen-Spektrometer (vgl. AP 2.1) ersetzt und die Intensität des Eingangssignals reduziert, um im Schnitt 0,1 Photonen pro Signal zu erreichen. Weiterhin wurden jetzt fünf Ausgänge des mQPG verwendet, welche die fünf möglichen Symbole eines fünfdimensionalen Alphabets dekodieren.
Um diesen Betriebsmodus zu verifizieren wurde eine sogenannte Quanten-Detektortomographie durchgeführt. Hierfür wird das mQPG sukzessive so programmiert, dass es auf den sechs möglichen konjugierten Basen eines 5-dimensionalen Hilbertraums operiert. Für jede Einstellung werden dann Eingangssignale erzeugt, die aus den 5 x 6 = 30 möglichen Elementen der konjugierten Basen bestehen. Diese werden nacheinander in das mQPG gesendet und die korrespondierenden Ausgangsintensitäten (die Zahl der konvertierten Photonen) in den fünf Ausgängen gemessen. Ein vollständiger Datensatz besteht aus 6 x 30 = 180 Messungen.
Mit Hilfe einer sogenannten „least squares“ Methode können die Messoperatoren (positive operator

valued measurements, POVMs) des mQPG rekonstruiert werden. Diese beschreiben die Messung, welche das mQPG durchführt, in der Sprache der Quantenmechanik. Vergleichen wir die rekonstruierten POVMs mit den idealen POVMs, so finden wir eine durchschnittliche Güte von 0,81. Dabei stellt sich heraus, dass diese Güte durch die limitierte spektrale Auflösung des Einzelphotonen-Spektrometers begrenzt ist. In einer Kontrollmessung wurde dieses durch den bereits verwendeten CCD-Spektrographen ersetzt und die Messung bei hohen Eingangsintensitäten wiederholt. Hieraus ergab sich eine durchnittliche Güte von 0,96, was belegt, dass das mQPG hervorragend als Dekoder für hochdimensionale Quantenschlüsselverteilung geeignet ist.
Die rekonstruierten POVMs des mQPG sind in Abb. 9 grafisch dargestellt. Hierbei zeigen die grauen Bereiche und orangenen Linien die idealen POVMs. Die blauen und schwarzen Linien sind die rekonstruierten POVMs. Durchgezogenen Linien sind für das Einzelphotonen-Spektrometer, gestrichelte Linien für den CCD-Spektrographen.

AP2.1 – Aufbau des Demonstratorexperiments

Im Lauf des zweiten Projektjahres wurde der experimentelle Aufbau zum Betrieb des mQPG aufgebaut. Der Aufbau basiert auf ähnlichen Aufbauten für Standard-QPGs, wurde aber speziell im Hinblick auf die Besonderheiten des mQPG konzipiert und optimiert. Eine Schemazeichnung des Aufbaus ist in Abb. 10 gezeigt.
Der Aufbau kann in zwei Hauptteile unterteilt werden, nämlich das System zur Erzeugung des Eingangssignals und den hochdimensionalen Zeitmoden (TM)-Dekoder. Der Dekoder selbst besteht aus der mQPG-Probe auf einer Justageplattform, dem Pulsformungssytem für den Pumpstrahl und der spektral aufgelösten Messung der mQPG-Ausgänge.

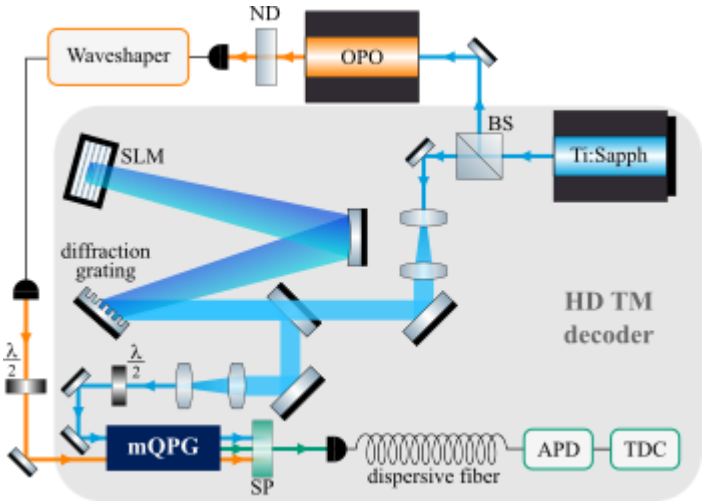


Abb. 10. Schema des Versuchsaufbaus. Die blaue Linie zeigt den Weg des Pumpstrahls, die orange Linie entspricht dem Eingangssignal und die grüne Linie zeigt das Ausgangsfeld des mQPG. Der graue Bereich zeigt die Komponenten unseres hochdimensionalen Dekoders.

Unser mQPG-Dekoder kann einen Eingangszustand gleichzeitig auf alle Elemente einer d-dimensionalen TM-Basis projizieren (wobei d die gewählte Dimensionalität des Dekoders ist) und liefert das Ergebnis jeder Projektion in einem separaten spektralen Ausgangskanal. Die Messbasis kann durch geeignete Formung des Pumpspektrums ausgewählt werden.
Im Experiment erzeugt ein Ti:Sa Oszillator ultrakurze Laserpulse, deren Trägerfrequenz 349THz entspricht (860nm) und die eine Wiederholrate von 80MHz aufweisen. Ein Teil des Strahls wird in einem selbstgebauten Pulsformer auf Basis einer sogenannten 4-f-Konfiguration mit einem räumlichen Lichtmodulator (Englisch: spatial light modulator, SLM) mit einer Auflösung von 10GHz geformt, um die Pumpzustände vorzubereiten. Das Pulsspektrum wird in d gleichmäßig verteilte Peaks zerlegt, die jeweils als Element der gleichen d-dimensionalen TM-Basis geformt werden. Der verbleibende Teil des Strahls pumpt einen optischen parametrischen Oszillator, der Pulse mit einer Trägerfrequenz von 194THz (1545nm) erzeugt. Diese Pulse werden durch einen Neutraldichtefilter

abgeschwächt und mit einem kommerziellen Waveshaper (Finisar) mit einer Auflösung von 1GHz geformt, um die Eingangssignale zu erzeugen. Beide Strahlen werden dann in den mQPG-Wellenleiter eingekoppelt. Das mQPG erzeugt Ausgangsfelder bei mehreren Frequenzen um 543THz (552nm). Anschließend werden die Ausgangsfelder mit Hilfe eines dichroitischen Spiegels von den restlichen Pump- und Eingangsfeldern getrennt, in eine Faser gekoppelt und mit einem fasergestützten Einzelphotonen-Spektrometer mit Laufzeitmessung gemessen, welches die Frequenz auf die Ankunftszeit am Detektor abbildet. Die Ankunftszeiten werden dann mit einer Avalanche-Photodiode (APD) in Kombination mit einem Zeit-Digital-Wandler gemessen.
Alternativ kann das Ausgangssignal des mQPG auch mit einem kommerziellen Einzelphotonen-sensitiven CCD-Spektrographen gemessen werden. Hiermit erhält man Information über das Ausgangsspektrum des mQPG, allerdings nicht auf einer Puls-zu-Puls Basis. Letztere ist für Anwendungen in der Quantenschlüsselverteilung allerdings unerlässlich, weshalb das Einzelphotonen-Spektrometer realisiert wurde.
Weiterhin wurde der Dekoder-Aufbau erweitert, um auch die Signalerzeugung realisieren zu können. Für eine erste Realisierung konzentrierten wir uns auf ein „Prepare and Measure“-Schema, bei dem die Signale, die vom Sender zum Empfänger übertragen werden, in schwachen kohärenten Pulsen mit einer durchschnittlichen Photonenzahl von weniger als eins kodiert sind. Abb. 11 zeigt eine schematische Darstellung des Systems.

Wir kodieren die Informationen in den komplexen Spektren der Lichtimpulse über einen Waveshaper mit einer langsamen Reaktionszeit in der Größenordnung von Millisekunden. Dies ist nicht ausreichend für QKD-Experimente mit hohen Raten, die eine zufällige Wahl des kodierten Zustands bei jedem einzelnen Übertragungsvorgang erfordern. Wir überwinden diese Herausforderung durch den Einsatz eines mehrkanaligen Waveshapers, mit dem wir bis zu acht Lichtpulse parallel formen können. Diese werden in ein schnelles 8x1-Schaltnetz eingespeist, das mit einer zufälligen Steuersequenz angesteuert wird, so dass bei jedem Experiment ein zufälliger Puls übertragen und an den Dekoder gesendet wird. Die Komponenten des Schaltnetzes wurden geliefert und getestet. Aufgrund verzögerter Lieferungen und einer benötigten Reparatur einer der Komponenten konnte der Gesamtaufbau nicht in der Projektlaufzeit fertiggestellt werden. Dies wird derzeit, im Nachgang des Projekts, finalisiert.

Auf der Empfängerseite besteht das System aus den Dekoder aus AP 2.1, der das Licht in die gedrehte Messbasis (X-Basis) umwandelt, die sich aus Überlagerungszuständen von Frequenzbins zusammensetzt. Das übertragene Signal wird durch das mQPG geleitet und an ein Flugzeitspektrometer gesendet. In diesem Spektrometer werden verschiedene Frequenzbins (Z-Basis) auf verschiedene Ankunftszeiten an einem Photonendetektor abgebildet. Das Gleiche gilt

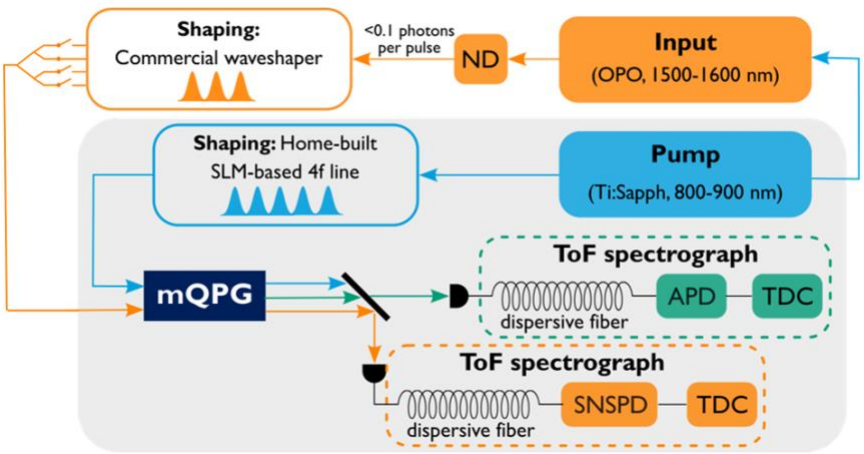


Abb. 11. *Schematische Darstellung des Gesamtexperiments zur Untersuchung von P&M QKD (vgl. AP 2.2).*

für die verschiedenen Ausgänge des mQPGs. Diese Konfiguration bietet zwei wesentliche Vorteile: Erstens ermöglicht sie den Betrieb auf einer „Pulse-by-Pulse“-Basis, da jedes gesendete und detektierte Photon ein gültiges Messergebnis liefert; zweitens implementiert ein mQPG mit einer Konversionseffizienz von weniger als 100% eine inhärent zufällige Wahl der Messbasis, da jedes einzelne Photon entweder gesendet (Z-Basis-Messung) oder konvertiert wird (X-Basis-Messung). In der Tat ist in praktischen QKD-Protokollen die erforderliche Anzahl von X-Basis-Messungen kleiner als die von Z-Basis-Messungen, da erstere nur zur Erkennung eines Abhörers dienen, während letztere den geheimen Schlüssel tragen. Daher ist eine niedrige mQPG-Umwandlungseffizienz für diese Anwendung ein inhärenter Vorteil, da sie den geheimen Schlüssel maximiert. Darüber hinaus können wir das Verhältnis von X- und Z-Basis-Messung ändern, indem wir die Leistung des mQPG-Pumplichts anpassen, ohne das Experimentalsystem zu verändern.

Abb. 12 zeigt eine vorläufige Charakterisierung der Wahl der passiven Basis durch das mQPG. Die obere Zeile zeigt die Verteilung der Messereignisse in der X-Basis (auch Testbasis genannt), während die untere Zeile die Verteilung der Messereignisse in der Z-Basis (auch Schlüsselbasis genannt) zeigt. In der linken Spalte bereiten wir einen Eingangszustand im logischen 0-Zustand vor. Dies zeigt sich in der Messung in der Z-Basis, die eindeutig nur Ergebnisse in dem mit der 0 verbundenen Bin zeigt. Im Gegensatz dazu sind die Messergebnisse in der X-Basis gleichverteilt. Die rechte Spalte zeigt die umgekehrte Situation eines Zustands, der in einem der X-Basis-Eigenzustände präpariert und folglich in der Z-Basis-Messung gleichverteilt ist.

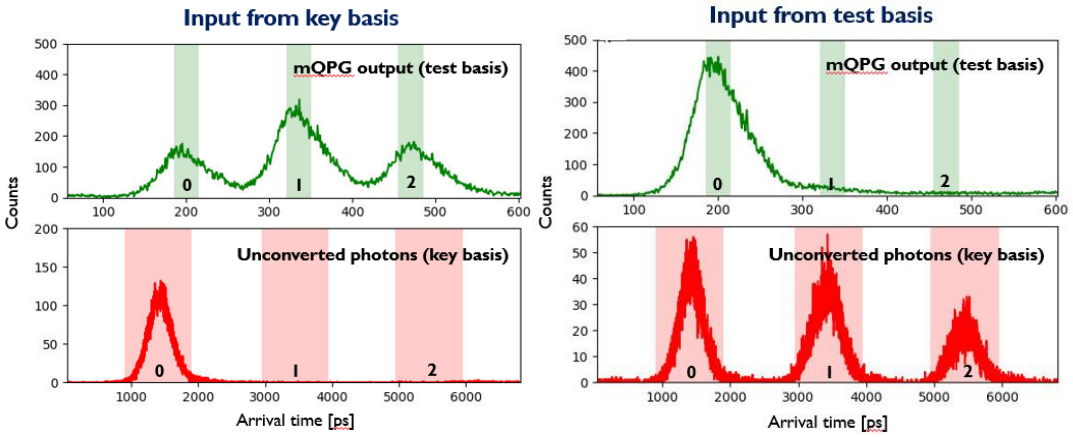


Abb. 12. *Vorläufige Messergebnisse des Dekodierungsschemas mit integrierter, passive Basisauswahl. Zustände einer Basis werden in der anderen Basis näherungsweise als Gleichverteilung gemessen.*

AP2.2: HD QSV – P&M Schema

5-dimensionale Zustandstomographie. Als ersten Schritt zur Realisierung hochdimensionaler Quantenschlüsselverteilung wurde die Fähigkeit des mQPG untersucht, hochdimensionale Zustände zu dekodieren. Dabei wurde, analog zur Quanten-Detektortomographie in AP1.4 eine sogenannte Quanten-Zustandstomographie durchgeführt. Dabei wurden 25 zufällige 5-dimensionale Eingangssignale erzeugt und mit dem mQPG charakterisiert. Hierfür wird das mQPG wieder sukzessive so programmiert, dass es auf den sechs konjungierten Basen des 5-dimensionalen Hilbertraums operiert. Dann werden Kopien der Eingangssignale in jeder der Basen vermessen und die resultierenden Photonen in den Ausgängen des mQPG mit Hilfe des Einzelphotonen-Spektrometers gezählt. Aus diesen Daten können dann die Eingangszustände rekonstruiert und mit den idealen Eingangszuständen verglichen werden.

Die Ergebnisse dieser Messungen sind exemplarisch für einen Eingangszustand in Abb. 13 gezeigt. Die linke Spalte zeigt Realteil und Imaginärteil des erzeugten Eingangszustands. Die mittlere Spalte zeigt die Rekonstruktion, wenn von einem idealen Betrieb des mQPG ausgegangen wird. Die rechte Spalte zeigt die Rekonstruktion basierend auf den echten POVMs des mQPG (vgl. AP1.4); man kann hier sinngemäß von einer Kalibration der Messung sprechen.
Für die 25 zufälligen Eingangssignale ergibt sich eine durchschnittliche Güte von 0.95, das mQPG eignet sich also gut zur Detektion und Charakterisierung hochdimensionaler Signale.

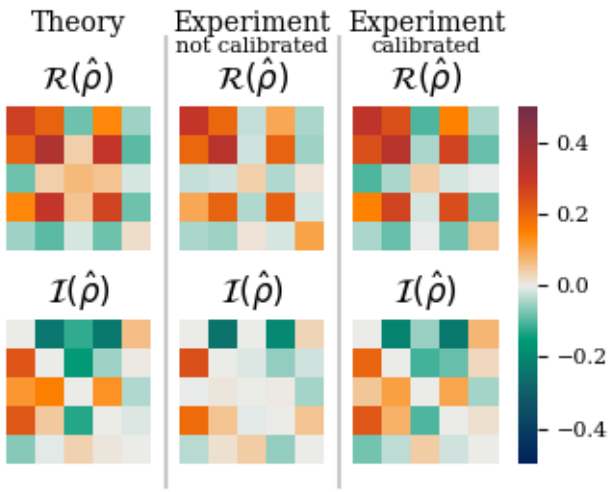


Abb. 13. *Beispiel für die Tomographie eines zufälligen Eingangszustands (gemessen mit dem Einzelphotonen-Spektrometer). Die Diagramme entsprechen dem Realteil (oben) und Imaginärteil (unten) der Dichtematrix des Signals. Von links nach rechts: der ursprüngliche Eingangszustand, der rekonstruierte Zustand unter Annahme perfekter Messungen und der Zustand, der mit den aus der Detektortomographie gewonnenen Kalibrierung rekonstruiert wurde.*

Alternative Kodierungen. In einem nächsten Schritt wurden alternative Kodierungen untersucht. Im Zeit-Frequenz-Bereich kann Information auf vielfältige Art und Weise kodiert werden. Beispiele sind die bisher verwendet Hermit-Gauß-Kodierung (hier: temporal modes; TM), die Kodierung auf Ankunftszeitbins (Englisch: time bins; TB) und die Kodierung in Frequenzbins (FB).

Im Rahmen des Porjekts wurde eine weitere Methode entwickelt, die sogenannten „Fancy Frequenzbins“ (FFB). Bei diesen werden breitere Frequenzbins geformt, welche allerdings nicht vollkommen unabhängig voneinander sind. Für Anwendungen in der QKD ist dies jedoch nicht relevant und es ist zu erwarten, dass breitere spektrale Features zu einer höheren Güte führen als alternative Kodierungen.

Um die am besten geeignete Kodierungsbasis für eine Demonstration von HD QKD abschließend zu identifizieren, haben wir alle möglichen Kodierungsbasen auf Einzelphotonenebene in drei und fünf Dimensionen getestet. Zu diesem Zweck wurde wiederum eine Detektortomographie durchgeführt und die durchschnittlichen Messgenauigkeiten im Vergleich zu idealen Messungen verglichen.

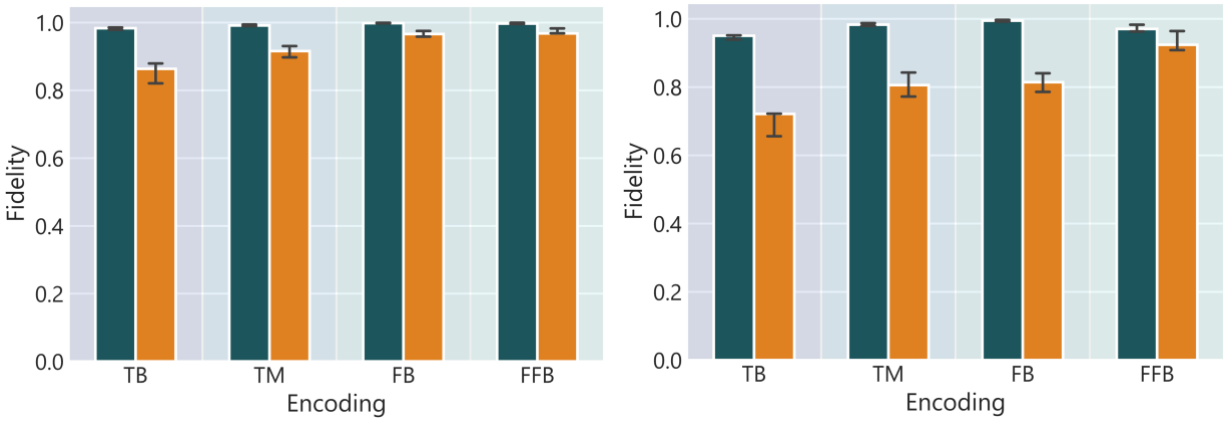


Abb. 14. *Güten der experimentellen mQPG Messungen für verschiedene Kodierungen (Zeitbins, Hermit-Gauß, Frequenzbins, Fancy Frequenzbins) für das Gesamtexperiment (Orange) und das mQPG an sich (Teal) in drei (links) und fünf (rechts) Dimensionen.*

Abb. 14 zeigt die Ergebnisse dieser Messungen für dreidimensionale Kodierung (links) und fünfdimensionale Kodierung (rechts). Die orangefarbenen Balken zeigen die Güte für das gesamte experimentelle System, während die dunkelgrünen Balken die intrinsische Güte des mQPG zeigen, wie sie mit einem hochauflösenden Spektrometer gemessen wurde (vgl. AP 1.4).

Wie erwartet, sind die Güten bei fünfdimensionaler Kodierung im Allgemeinen niedriger, da schmalere spektrale Features geformt werden müssen. Die intrinsische Güte des mQPG ist hoch, aber die begrenzte Auflösung des Flugzeitspektrometers schränkt die Gesamtleistung des Systems ein.

Anders verhält es sich bei der dreidimensionalen Kodierung. Hier sind die Güten für die FB- und FFB-Kodierungen sogar für das gesamte experimentelle System einschließlich der Flugzeitspektrometer hoch. Die TB-Kodierung weist eine geringere Güte auf, was auf Unzulänglichkeiten bei den X-Basis-Messungen zurückzuführen ist.

Dank der sorgfältigen Ausrichtung und Kalibrierung des Aufbaus stellen wir nun auch fest, dass die FFB-Kodierung, wie in der nachstehenden Tabelle aufgeführt, insgesamt die besten Ergebnisse liefert. Im Einzelnen führen wir die durchschnittliche intrinsischen Güte des mQPG (obere Zeile) und des gesamten experimentellen Systems (untere Zeile) auf.

	Drei Dimensionen	**Fünf Dimensionen**
Intrinsische mQPG-Güte	F=0.997±0.002	F=0.970±0.020
Güte des Gesatmssytems	F=0.968±0.027	F=0.924±0.076

Auf der Grundlage dieser Ergebnisse haben wir gemeinsam mit unseren Theoriepartnern die optimale Kodierung ermittelt. Eine größere Dimension führt zu einer besseren Fehlertoleranz, während eine höhere Güte zu einer höheren sicheren Schlüsselrate führt. Tatsächlich kann eine niedrige Güte zu einer Schlüsselrate von Null führen. Eine sorgfältige Abwägung dieses Kompromisses ergab, dass eine dreidimensionale Verschlüsselung mit der FFB-Kodierung die höchsten geheimen Schlüsselraten erwarten lässt.

AP2.3: HD QSV – Verschränkung

Dieses AP konnte im Projektzeitraum nicht abschließend bearbeitet werden. Allerdings lässt sich aus den Teilergebnissen ableiten, dass das P&M Schema derzeit noch vielversprechender für experimentelle HD QKD ist als eine verschränkungsbasierte Version.

Der Grund hierfür liegt in den Kodierungen. Die Quantenlichtquelle erzeugt maximal verschränkte Zustände mit einer TM-Kodierung, wohingegen der Dekoder am besten mit der FFB-Kodierung funktioniert. Mögliche Vorteile des verschränkungsbasierten Ansatzes würden durch die schlechtere Dekoderleistung wahrscheinlich negiert.

Aus diesem Grund wird im Nachgang der Projektlaufzeit das P&M Schema realisiert werden.

3. Wichtigste Positionen des zahlenmäßigen Nachweises

Personalkosten (0812)	Finanzierung des an der Forschung beteiligten Personals. Eine Doktorandin, die die konzeptionellen, theoretischen und experimentellen Arbeiten durchgeführt hat.
Gegenstände bis 410€ (0831)	Optische und optomechanische Komponenten, welche im Experiment verbaut wurden.
Dienstreisen (0846)	Reisen zu nationalen und internationalen Konferenzen zur Dissemination der Projektergebnisse. Weiterhin Reisen zu den Verbundtreffen zur gemeinsamen Diskussion des Projektfortschritts.

4. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die Quantenschlüsselverteilung stellt einen essenziellen Beitrag zur zukünftigen Cyber-Sicherheit dar. Quantencomputer werden in der Lage sein, herkömmliche Verschlüsselungen zu entschlüsseln. Die Quantenschlüsselverteilung erlaubt den Austausch eines absolut abhörsicheren Schlüssels, basierend auf den Prinzipien der Quantenmechanik. Erste kommerzielle Systeme sind bereits erhältlich, jedoch sind ihre Leistungskennzahlen noch nicht in einem Bereich, der sie für echte Anwendungen relevant macht.
Hochdimensionale Quantenschlüsselverteilung kann diese Leistungskennzahlen verbessern. Zum einen werden durch die Verwendung eines größeren Kodierungsalphabets höhere Schlüsselraten ermöglicht, zum anderen sind hochdimensionale Kodierungen resistent im Hinblick auf experimentelle Imperfektionen.
Um hochdimensionale Quantenschlüsselverteilung in die Anwendung zu bringen, braucht es jedoch weitergehende Forschungsarbeiten, sowohl auf theoretischer Seite als auch im Experiment. In diesem Projekt wurde hochdimensionale Quantenschlüsselverteilung mit Zeit-Frequenz-Kodierungen untersucht und grundlegende Bauteile entwickelt und verifiziert. Verschiedene Kodierungsformate bringen ihre Vor- und Nachteile mit sich, da sie individuelle Anforderungen an Quellen und Dekoder stellen. Unsere Forschungsergebnisse zeigen, dass der derzeitige Stand der Technik breitbandige Frequenzbins – sogenannte „Fancy Frequenzbins“ – in einer dreidimensionalen Kodierung am vielversprechendsten erscheinen lässt.
Der Grund hierfür ist, dass der im Projekt entwickelte Dekoder – basierend auf einem eigens implementierten multi-output Quantenpulsgatter – bei diesem Kodierungsformat die höchste Güte erreicht. Diese ist das definierende Maß für die erwartete Performanz der Quantenschlüsselverteilung.
Somit konnten die Projektarbeiten den Stand der Technik im Hinblick auf hochdimensionale Quantenschlüsselverteilung deutlich voranbringen und leisten somit einen wichtigen Beitrag zur zukünftigen Cyber-Sicherheit in Deutschland.

5. Verwertbarkeit der Ergebnisse

Die Ergebnisse werden im Sinne des Verwertungsplans wie folgt weiterverwertet:

- Wissenschaftliche Ergebnisse werden auf Konferenzen und in Fachjournalen veröffentlicht.
- Aus dem Projekt entstandene Ergebnisse werden, wo möglich, durch Patente geschützt. Dies ist für den hochdimensionalen Dekoder mit passiver Basiswahl bereits der Fall, welcher unter dem Aktenzeichen 10 2024 117 337.8 vorläufig geschützt ist.

- Weiterhin haben die Arbeiten des Gesamtverbunds zu einem starken Zusammenschluss internationaler Forschungspartner geführt. Nachfolgende Arbeiten sollen, wenn möglich, in einer ähnlichen Zusammensetzung durchgeführt werden und erste Diskussionen hinsichtlich geeigneter Forschungsthemen sowie Fördermöglichkeiten werden derzeit aktiv vorangebracht.

6. Fortschritt bei anderen Stellen

Uns sind keine Ergebnisse dritter bekannt, welche die hier erarbeiteten Ergebnisse wiederholen oder darüber hinausgehen.

7. Veröffentlichungen

1. L. Serino, J. Gil-Lopez, M. Stefszky, R. Ricken, C. Eigner, B. Brecht, C. Silberhorn, „Realization of a multi-output quantum pulse gate for decoding high-dimensional temporal modes of single-photon states", PRX Quantum **4**, 020306 (2023).
   Experimentelle Realisierung eines mQPGs sowie hochdimensionale Detektortomografie.

2. L. Serino, W. Ridder, A. Bhattacharjee, J. Gil-Lopez, B. Brecht, C. Silberhorn, „Orchestrating time and color: a programmable source of high-dimensional entanglement", arXiv:2406.04909 (2024), *akzeptiert in Optica Quantum.*
   Experimentelle Realisierung der hochdimensionalen maximal Zeit-Frequenz-verschränkten Photonenpaarquelle.

3. L. Serino, G. Chesi, B. Brecht, L. Maccone, C. Macchiavello, C. Silberhorn, „Complementarity-based complementarity", arXiv:2406.11395 (2024).
   Studie zur Bedeutung der Wahl verschiedener komplementärer Basen mit potenziellen Implikationen für die Quantenschlüsselverteilung.

4. L. Serino, C. Eigner, B. Brecht, C. Silberhorn, „Programmable time-frequency mode-sorting, of single photons with a multi-output quantum pulse gate", arXiv:2410.03606 (2024).
   Experimentelle Untersuchung verschiedener Zeit-Frequenz-Kodierungen inclusive der "Fancy Frequenzbins"