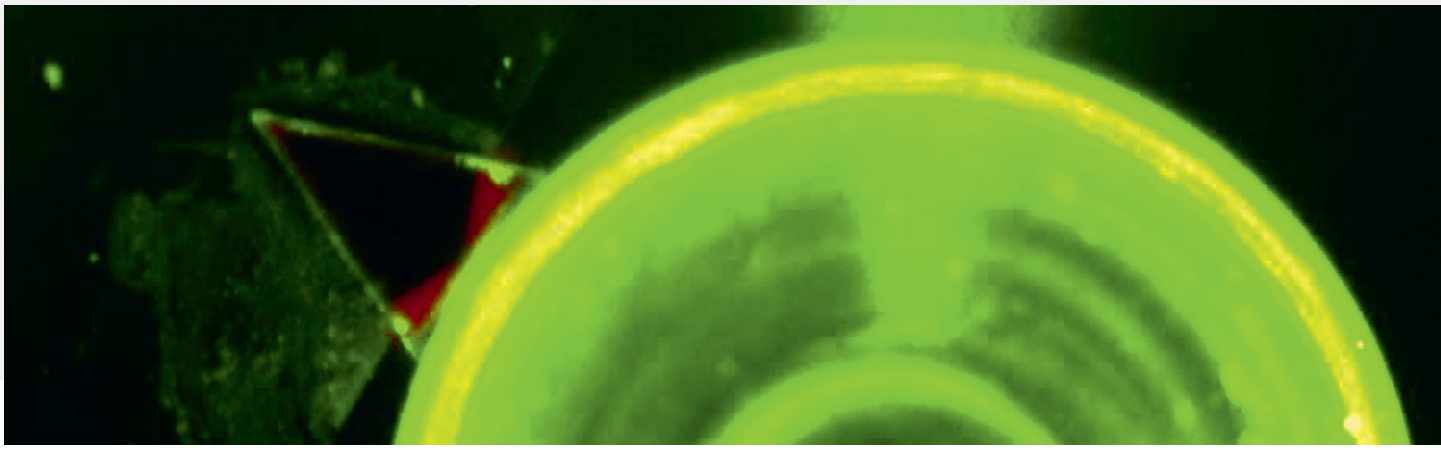
DOMINIQUE ELSER, CHRISTOPH MARQUARDT, GERD LEUCHS
MAX-PLANCK-INSTITUT FÜR DIE PHYSIK DES LICHTS, ERLANGEN

Quanten-Engineering mit optischer Technologie



Die Quantentechnologien versprechen technische Lösungen mit Eigenschaften, die keine andere Technologie bietet: Quantencomputer werden bestimmte Aufgaben lösen können, an denen bisher selbst Supercomputer scheitern, und die Quantenkryptographie kann nachweisbar abhörsichere Kommunikation gewährleisten. Trotz des Versprechens künftiger technischer Anwendungen sind die Quantentechnologien nach wie vor bedeutende Felder der Grundlagenforschung – und damit eine Domäne der Max-Planck-Gesellschaft, die den Namen des Entdeckers der Quantenphysik trägt. Ein wichtiger Teilaspekt ist der Beitrag der Optikwissenschaft zu den Quantentechnologien. Dies betrifft insbesondere die Themen Quantenkommunikation und -kryptographie. Von diesen Themen, die am Max-Planck-Institut für die Physik des Lichts in Erlangen erforscht werden, soll hier die Rede sein.

Verbunden mit der Quantenphysik ist die Heisenbergsche Unschärferelation. Die Quantenphysik erlaubt in der Regel nur Wahrscheinlichkeitsaussagen und keine präzisen Vorhersagen für Messungen an einem einzelnen Quantensystem. Dies hört sich eher nach einem Show-Stopper als nach einem Vorteil an. Doch die Tatsache, dass ein Quantensystem in einem unbekannten Zustand durch Messungen nicht eindeutig charakterisiert werden kann, birgt andererseits auch ungeahnte Möglichkeiten. Eine Charakterisierung ließe sich nur im Mittel über viele identische Messungen bewerkstelligen, wenn genau der gleiche Zustand sehr oft präpariert und gemessen wird. Diese Eigenschaft ist einzigartig. Man findet sie nur bei Quantensystemen, und sie bietet einen unschätzbaren Vorteil: Die Grundgesetze der Natur erlauben es nicht, perfekte Kopien eines Quantensystems herzustellen.

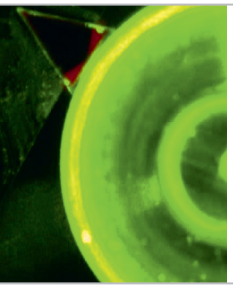
Das bedeutet einerseits, dass bereits der Versuch einer Messung sichtbare Spuren hinterlässt: Ein unerwünschter Abhörer kann also nicht im Verborgenen werkeln. Auf der anderen Seite können zwei Quantensysteme aber trotzdem miteinander verschränkt sein. Das bedeutet, dass zwar jedes System für sich genommen sehr unscharfe Messresultate liefert, dass aber die richtigen Messungen an den beiden Systemen perfekt miteinander korreliert sein können. Nur wenn man den Wert der ersten Messung kennt, kann man die Messung am zweiten System exakt vorhersagen. Das ist eine der Grundlagen für den Quantencomputer.

Ein dritter Aspekt, der nicht nur für die Kryptographie wichtig ist, ist die Erzeugung von perfekten Zufallszahlen. Die heute von Computern erzeugten Zufallszahlen werden durch Algorithmen erzeugt und sind daher im Prinzip reproduzierbar – daher der Name „Pseudo-Zufallszahlen“. Die Zufälligkeit des Ergebnisses einer Quantenmessung aber ist nach heutigem Stand des Wissens vollkommen. Die Quantenphysik erlaubt es sogar, Aussagen darüber zu machen, ob eine zweite Partei über identische Zufallszahlen verfügen kann: Wenn ein Quantensystem in einem reinen Quantenzustand ist, dann kann es mit keinem anderen System verschränkt sein. Die Zufallszahlenreihe ist dann einzigartig.

Nun wird es höchste Zeit zu präzisieren, was ein Quantensystem ausmacht. Generell gesprochen ist ein Objekt oder „System“ dann ein Quantensystem, wenn seine Eigenschaften von der Quantenphysik dominiert werden. Beispiele dafür sind einzelne Quantenobjekte wie einzelne Photonen, einzelne Atome, einzelne Fehlstellen in einem Festkörper oder einzelne Elektronen. Aber auch in einem Ensemble vieler solcher Objekte können die Quanten-

eigenschaften dominieren: Zum Beispiel viele Millionen von Atomen, wenn sie ein Bose-Einstein-Kondensat darstellen, viele Elektronen, wenn sie in einem supraleitenden Zustand sind, oder viele Photonen, wenn sie sich wie in Laserlicht in einem kohärenten Zustand befinden.

Die Forschung am Max-Planck-Institut für die Physik des Lichts (MPL) beschäftigt sich sowohl mit den Quellen, das heißt mit der Erzeugung photonischer Quantensysteme, als auch mit der Implementierung von Kommunikationsprotokollen sowie mit der Charakterisierung der Quantensysteme durch Messungen. In der Anwendung werden natürlich alle drei Aspekte benötigt. Der besondere Charme der optischen Quantentechnologien ist, dass sie die Plattform der weit fortgeschrittenen optischen Telekommunikation nutzen können, von optischen Faserverbindungen bis hin zur sogenannten kohärenten Kommunikation über Satelliten.



QUANTENCOMPUTER WERDEN AUFGABEN LÖSEN KÖNNEN, AN DENEN BISHER SELBST SUPERCOMPUTER SCHEITERN. DIE QUANTENKRYPTOGRAPHIE KANN AUCH DANN NOCH NACHWEISBAR ABHÖRSICHERE KOMMUNIKATION GEWÄHRLEISTEN.

Die Heisenbergsche Unschärferelation hat zur Folge, dass die Messung eines Quantensystems innerhalb gewisser Grenzen zufällige Werte liefert. Diese Zufälligkeit unterscheidet sich prinzipiell von dem aus dem Alltag bekannten Zufall, beispielsweise dem Ziehen einer Spielkarte. Die gezogene Karte erscheint uns nur deswegen zufällig, weil wir das Mischen der Karten nicht exakt nachverfolgen können. Beim Kartenspiel am Computer verbirgt sich die Erzeugung des Zufalls zwar vor unseren Augen, allerdings nutzen Computer mathematische Berechnungen, um Pseudo-Zufallszahlen zu erzeugen. Insofern scheinen auch solche Prozesse nur dann zufällig, wenn wir nicht alle Parameter der Algorithmen kennen.

Anders verhält es sich, wenn wir die Messung an einem Quantensystem zur Erzeugung von Zufall nutzen. Hier basiert der Zufall nicht auf unzureichender Kenntnis des erzeugenden Prozesses, dieser Prozess ist im Gegenteil sogar vollständig bekannt. Der Zufall entsteht durch den quantenmechanischen Messprozess selbst. Das MPL arbeitet an der technischen Umsetzung eines solchen Zufallsprozesses unter Verwendung von Quantenzuständen des Lichts. Der Messprozess ist hierbei als sogenannte Homodyn-Messung ausgeführt. Dabei wird das eigentliche Signal mit einem starken Laserstrahl überlagert. So kann man auch ein sehr empfindliches Signal erfassen. Die Homodyn-Messung erlaubt es, an vielen identisch erzeugten Lichtzuständen den Zustand durch Mittelung präzise zu bestimmen.

Bei einer einzelnen Messung an einem Quantensystem herrscht also der Zufall. Um diesen sozusagen als perfekten Würfel auszunutzen, ist es nicht einmal notwendig, ein Lichtsignal in den Detektor zu schicken. Denn auch wenn das Signal am Eingang des Detektors „Null“ ist, wenn also der geringste mögliche Pegel vorliegt, dann gibt es immer noch die unvermeidbare Quantenunschärfe des Feldes. Führt man an diesem „Vakuumzustand“ nun eine Folge von Homodyn-Messungen durch, erhält man eine beliebig lange Reihe von echten und einzigartigen Zufallszahlen.

Die Umsetzung des Zufallszahlengenerators nach dem Homodyn-Prinzip erlaubt es, auf existierende Technologien der integrierten Optik zurückzugreifen. Dadurch ist es denkbar, die Funktionalität im Größenbereich eines USB-Sticks zu implementieren. Zusammen mit dem Austrian Institute of Technology und der Firma Roithner Lasertechnik arbeitet das MPL derzeit an einer solchen Miniaturisierung.

Quanten-Zufallszahlen-Generatoren sind bislang noch nicht weit genug entwickelt und miniaturisiert, um den breiten Massenmarkt zu erreichen. Dabei wären die Anwendungsfälle für echte, nicht vorhersagbare Zufallszahlen vielfältig. So sind beispielsweise Simulationen technischer Systeme sowie Klima- und Finanzmodelle oftmals auf Zufallszahlen hoher Qualität angewiesen. Die Verwendung von computergenerierten Pseudo-Zufallszahlen kann hierbei unbemerkt zu fehlerhaften Modellaussagen führen. Auch im Bereich Datensicherheit sind echte Zufallszahlen von unschätzbarer Bedeutung. Die heutzutage weitreichend im elektronischen Datenverkehr eingesetzten kryptographischen Schlüssel basieren auf Zufallszahlen. Schwache Zufallszahlen erleichtern Angreifern das Handwerk und eröffnen somit unbemerkte Sicherheitslücken.

Die einmalige Verwendung von echten Zufallszahlen könnte bei Kryptographie-Systemen verhindern, dass ein Angreifer die Verschlüsselung bricht. Allerdings ist es in Ermanglung echter und einzigartiger Zufallszahlenreihen bei den bisher eingesetzten Systemen so, dass sie für ihre Schlüssel

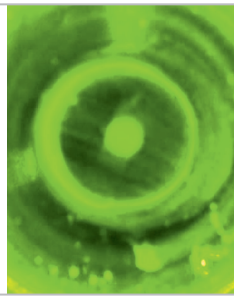
Pseudozufallszahlen benutzen, die mittels mathematischer Methoden erzeugt werden. Die Latte kann für einen unerwünschten Abhörer dadurch sehr hoch gelegt werden, dass entsprechend viel Rechenleistung benötigt wird, um die Schlüssel zu knacken. Auf diese Weise wird aber keine absolute Sicherheit gewährleistet. Auch wenn Angreifer heutzutage noch nicht über die notwendige Rechenleistung verfügen und der Nutzer sich in Sicherheit wiegt, können Angreifer den Datenverkehr mitschneiden, um die Verschlüsselung zu einem späteren Zeitpunkt zu brechen, sobald die benötigte Rechenleistung zur Verfügung steht. Für manche sensible Daten ist dies aber einfach nicht akzeptabel.

Perfekte Zufallszahlen allein reichen für eine sichere Datenübertragung nicht aus, wenn nur der Sender über sie verfügt. Der geheime Schlüssel muss zudem zwischen Sender und Empfänger ausgetauscht werden, ohne dass ein Abhörer darauf zugreifen kann. Für den Schlüsselaustausch werden heute asymmetrische algorithmische Verfahren verwendet, die unter dem Sammelbegriff „Public Key Verfahren" fallen. Die meisten algorithmischen Verfahren zur sicheren Schlüsselverteilung sind erwiesenermaßen unsicher, sobald ein Quantencomputer mit ausreichender Größe des Quanten-Rechenregisters verfügbar sein wird. Bei anderen Verfahren ist die Sicherheit noch nicht bewiesen.

Abhilfe kann auch hier die Heisenbergsche Unschärferelation schaffen. Der Informationsaustausch zwischen zwei Parteien zur Erzeugung eines Schlüssels geschieht dann nicht mehr auf der Basis von digitalen Bits, sondern mit Hilfe von Quantenzuständen. Im Gegensatz zu digitalen Bits können Quantenzustände aufgrund der Unschärferelation nicht perfekt kopiert werden. Ein Angreifer kann somit nicht unbemerkt Informationen über den erzeugten Schlüssel abgreifen. Hier gewährleisten also physikalische Gesetze, dass kein Unbefugter verschlüsselte Kommunikation belauschen und erlangen kann. Man spricht von informationstheoretischer Sicherheit im Gegensatz zu der schwächeren Sicherheit, die auf nicht ausreichend zur Verfügung stehender Rechenleistung beruht und die oben diskutiert wurde. Mit der Quanten-Schlüsselverteilung erreicht man beides: Sie liefert perfekte Zufallszahlen und es wird eine informationstheoretisch sichere Schlüsselverteilung erreicht.

Es gibt verschiedene quantenoptische Methoden zur Umsetzung eines Quanten-Schlüsselaustauschs. Die bekannteste Methode arbeitet mit diskreten Lichtteilchen, den Photonen. Diese Methode ist in den letzten 30 Jahren weltweit in zahlreichen theoretischen Arbeiten und Experimenten erforscht worden. Bei der Umsetzung in die Praxis sind allerdings mehrere Herausforderungen deutlich geworden: Die Einzelphotonen-Methode benötigt speziell entwickelte Hardware, die sich nicht ohne weiteres in bestehende Telekommunikations-Infrastruktur integrieren lässt. Synergieeffekte mit der weit verbreitenden optischen Datenkommunikation sind dadurch eher gering. Anders verhält es sich bei der vergleichsweise neueren Quantenkommunikation mit kontinuierlichen Variablen, die unter anderem am MPL entwickelt wird. Anstelle von diskreten Lichtteilchen basiert diese Methode auf Eigenschaften von Lichtwellen, die anders als deren Energie kontinuierlich veränderlich sind, wie beispielsweise die Amplitude – also die Auslenkung der Wellen. Die Heisenbergsche Unschärferelation erlaubt dabei nicht nur die Erzeugung von echtem Zufall, sondern auch dessen Verteilung zwischen zwei entfernten Parteien. Auf Basis dieses verteilten Zufalls lässt sich dann ein geheimer Schlüssel erzeugen.

DER BESONDERE CHARME DER OPTISCHEN QUANTENTECHNOLOGIEN IST ES, DASS SIE DIE PLATTFORM DER WEIT FORTGESCHRITTENEN OPTISCHEN TELEKOMMUNIKATION NUTZEN KÖNNEN.



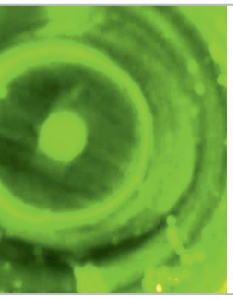
Die Schlüsselverteilung mit kontinuierlichen Variablen lässt sich im Wesentlichen unter Verwendung von herkömmlichen optischen Telekommunikations-Komponenten umsetzen und daher auch einfach in bestehende Kommunikations-Netze integrieren. Der Unterschied zwischen der weit verbreiteten optischen Kommunikation und der Quantenkommunikation besteht dann vor allem in der Rolle, die die Unschärferelation spielt. Während die Quantenunschärfe in der optischen Datenkommunikation als Störung zu fehlerhafter Übertragung führen kann, wird sie in der Quantenkommunikation bewusst ausgenutzt, um einen geheimen Schlüssel zu erzeugen.

Die Quantenschlüsselverteilung mit kontinuierlichen Variablen ist darüber hinaus auch sehr unempfindlich gegenüber Störeinflüssen anderer Lichtquellen. Dadurch ergibt sich die Möglichkeit, Quantenkommunikation parallel zur optischen Datenkommunikation ohne gegenseitige Beeinflussung zu

betreiben. An der Umsetzung dieses Verfahrens in Glasfasernetzen außerhalb des Labors arbeitet das MPL zusammen mit Firmen aus den Bereichen Informationstechnik und Datensicherheit.

Neben der Übertragung durch optische Glasfasern benötigen Kommunikationsnetze auch Freiraumkanäle, also Kanäle für die Übertragung durch Luft oder Vakuum, beispielsweise um mit beweglichen Objekten zu kommunizieren. Das MPL ist weltweit führend in der Übertragung von kontinuierlichen Quantenzuständen durch die Atmosphäre. Es konnte gezeigt werden, dass selbst empfindliche Quanteneigenschaften die Reise durch eine turbulente Atmosphäre relativ unbeschadet überstehen können. Unter Einsatz einer speziell hierfür entwickelten Technik, die unter anderem auf dem Homodyn-Verfahren basiert, wurden kontinuierliche Quantenzustände über eine Strecke von 1,6 km über den Häusern und Straßen von Erlangen verschickt.

Die bereits demonstrierten Entfernungen scheinen zunächst keinen Vorteil zu bieten, wenn man sie mit der Länge der Strecken vergleicht, für die Quantenkommunikation in Glasfasern demonstriert wurde. Aber auf dem Weg nach oben zu einem Satelliten kommt man sehr schnell aus der Atmosphäre heraus. Die atmosphärischen Störungen auf diesem Weg sind nur etwa dreimal so groß wie auf der 1,6 km langen Demonstrationsstrecke. Der Erfolg der Machbarkeitsstudie deutet daher darauf hin, dass diese Technik auch über größere Übertragungsstrecken eingesetzt werden kann, wenn die Übertragung über Satelliten läuft.



WIR ARBEITEN GEMEINSAM MIT PARTNERN AN DER MINIATURISIERUNG EINES QUANTEN-ZUFALLS-ZAHLEN-GENERATORS. DIE ANWENDUNGEN FÜR ECHTE ZUFALLSZAHLEN SIND VIELFÄLTIG.

Weltweit gibt es derzeit das ambitionierte Ziel, Quantenkommunikation über Satelliten zu betreiben. Insbesondere China und Japan, aber auch Kanada investieren in großem Maßstab in solche Vorhaben. Dies hat den folgenden Grund: Bisher funktioniert Quantenschlüsselverteilung in Glasfaserkabeln über Entfernungen, die für Großstädte typisch sind. Doch die Anbindung dieser Großstädte an ein weltweites Quanten-Netzwerk ist derzeit über Glasfaserverbindungen nicht praktikabel. Im Gegensatz zur optischen Datenkommunikation können Quantenzustände nämlich nicht zwischenverstärkt werden – eine klassische Verstärkung entspricht im Prinzip einem Kopieren der Information, was bei der Quanteninformation grundsätzlich nicht geht.

Optische Freiraumverbindungen im Weltall können hingegen aufgrund der wesentlich geringeren Signalverluste ohne Zwischenverstärker auskommen und damit wesentlich größere Strecken überbrücken. Satelliten mit Fähigkeiten zur Quantenkommunikation sind sowohl aus Sicht von zukünftigen Anwendungen als auch für die Grundlagenforschung sehr interessant. Auf der Anwendungsseite können Satelliten das Rückgrat für den weltweiten Austausch von Quantenschlüsseln bilden.

Neben dieser anwendungsbezogenen Perspektive eröffnet die Quantenkommunikation mit Satelliten auch ganz neue Möglichkeiten in der Grundlagenforschung. Zurzeit wird darüber spekuliert, dass Quantenkommunikation und Quanten-Informationsverarbeitung vom Gravitationsfeld auch auf eine bisher nicht bekannte Weise beeinflusst werden, und dass sich dies zukünftig bei Anwendungen mit erhöhter Empfindlichkeit bemerkbar machen könnte. Dafür gibt es bereits erste theoretische Ansätze. Experimentelle Daten, die mittels satellitenbasierter Quantenkommunikation gewonnen werden, könnten wichtige Impulse geben.

Auch im Bereich der Satellitenkommunikation profitieren Methoden, die auf kontinuierlichen Variablen beruhen, von bereits entwickelter Technologie zur optischen Datenkommunikation. Die deutsche Firma Tesat-Spacecom hat zusammen mit dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) ein System zur optischen Datenkommunikation mit Satelliten entwickelt. Es basiert im Wesentlichen auf denselben Methoden wie sie am MPL Erlangen für die Quantenkommunikation mit kontinuierlichen Variablen eingesetzt werden. Dadurch ergibt sich bereits bei existierenden Satelliten-Systemen die Option, sie für Quantenkommunikation aufzurüsten. Mit diesem Ansatz sattelt die Umsetzung von satellitenbasierter Quantenkommunikation auf bereits vorhandenen Investitionen auf und bedarf keiner so kostenintensiven Neuentwicklungen, wie sie in anderen Ländern getätigt werden.

In Zusammenarbeit mit Tesat-Spacecom und dem DLR evaluiert das MPL derzeit diesen Ansatz mittels Testmessun-

gen an optischen Satellitenverbindungen, die seit kurzem bestehen. Aus diesen Messungen können die optimalen Betriebsparameter für satellitenbasierte Quantenkommunikation bestimmt werden, so dass künftige Satelliten-Systeme entsprechend aufgerüstet werden können.

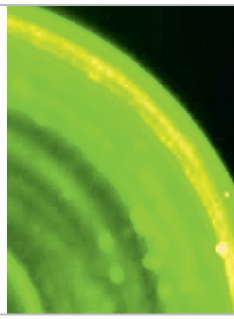
Die Heisenbergsche Unschärferelation bezieht sich auf zwei „komplementäre" Größen wie beispielsweise den Ort und die Geschwindigkeit. Es ist physikalisch erlaubt, die Unschärfe in einer der beiden Größen zu reduzieren, allerdings auf Kosten einer größeren Unschärfe in der komplementären Größe. Man spricht hier bildlich vom Quetschen der Unschärfe, wie vom Quetschen eines Luftballons in einer Richtung, der sich dann aber senkrecht dazu ausdehnt. Dieses Konzept lässt sich auch auf Lichtstrahlen anwenden und kann dort die Messgenauigkeit erheblich steigern. Gequetschte Lichtstrahlen können die Empfindlichkeit von Interferometern erhöhen und gehören beispielsweise zum Repertoire der Betreiber von Gravitationswellen-Detektoren, denen kürzlich der große Durchbruch gelungen ist.

Im Bereich Quantenkommunikation eröffnen sich durch das Quetschen von Lichtzuständen bisher kaum genutzte Parameter zur Steigerung der Effizienz. Hierbei ist allerdings zu beachten, dass gequetschtes Licht besonders empfindlich gegenüber Signalstörungen ist, wie sie gerade bei der Übertragung durch die Atmosphäre auftreten können. Das MPL hat daher eine Quelle für gequetschtes Licht entwickelt, deren Licht relativ unempfindlich gegenüber diesen Störungen ist. Der Nachweis der Eignung dieser Quelle konnte über die 1,6 km lange Teststrecke durch Erlangen erbracht werden.

In bestimmten Quantenkommunikations-Szenarien ist der Einsatz von einzelnen Photonen nach wie vor vorteilhaft. Damit verbunden ist allerdings ein höherer Entwicklungsaufwand für die entsprechenden Quellen. Ziel ist es daher, kompakte, stabile und gut einstellbare Quellen für Einzelphotonen zu entwickeln. Die Optik kann sich hierbei eines Prinzips bedienen, das in der Akustik schon längere Zeit bekannt ist: die Flüstergalerie.

Bekannte akustische Flüstergalerien befinden sich beispielsweise in den Kuppeln der St.-Pauls-Kathedrale in London oder des Petersdoms in Rom und der Jameh Moschee in Isfahan. Schallwellen können sich dort entlang der Kuppelwände ausbreiten, so dass Flüstern auf der einen Seite der Kuppel auf die andere Seite fokussiert und dort gut hörbar ist. Dieses akustische Prinzip lässt sich auf Lichtwellen übertragen. Optische Flüstergalerie-Resonatoren werden am MPL in hoher Qualität hergestellt, so dass sie sich für die effiziente Erzeugung von Einzelphotonen eignen. Die Wellenlänge der Photonen ist dabei einerseits schmalbandig, es entspricht also fast einer fest definierten Wellenlänge und damit einer reinen Lichtfarbe. Andererseits lässt sie sich in einem großen Wellenlängen-Bereich einstellen. Aufgrund dieser Eigenschaften eignet sich die Photonen-Quelle für vielfältige Anwendungen sowohl in der Quanteninformationstechnologie als auch in den Lebenswissenschaften.

QUANTENKOMMUNIKATION ÜBER SATELLITEN ZU BETREIBEN, IST DERZEIT NOCH EIN AMBITIONIERTES ZIEL. MEHRERE STAATEN INVESTIEREN JEDOCH IN GROSSEM MASSSTAB IN DERARTIGE PROJEKTE.



SCHLUSSBEMERKUNG

Die Quantentechnologie im Allgemeinen und die photonische Quantentechnologie im Besonderen bieten der Anwendung bislang nicht gekannte Möglichkeiten, die auf den gewöhnungsbedürftigen Konzepten der Quantenphysik beruhen. Dazu muss die Quantentechnologie anwendungstauglich gemacht werden und Ausbildungsprogramme müssen entsprechend angepasst werden.

Die Bedeutung dieser Entwicklung, die gerade begonnen hat, unterstreicht eine Studie, die 2015 die Nationale Akademie der Wissenschaften Leopoldina unter der Federführung von Wolfgang Schleich in Abstimmung mit den Partner-Akademien herausgegeben hat. Dort werden die Grundlagen der Quantentechnologie und die neuen Möglichkeiten, die durch sie eröffnet werden, einem breiteren Publikum vorgestellt. Die Max-Planck-Gesellschaft hat zudem einen Film zum Thema produziert:
https://www.youtube.com/watch?v=TkN1N6lDypo

Wir danken Frau Ulrike Bauer-Buzzoni für die sorgfältige Durchsicht des Manuskripts und die vielen hilfreichen Hinweise.