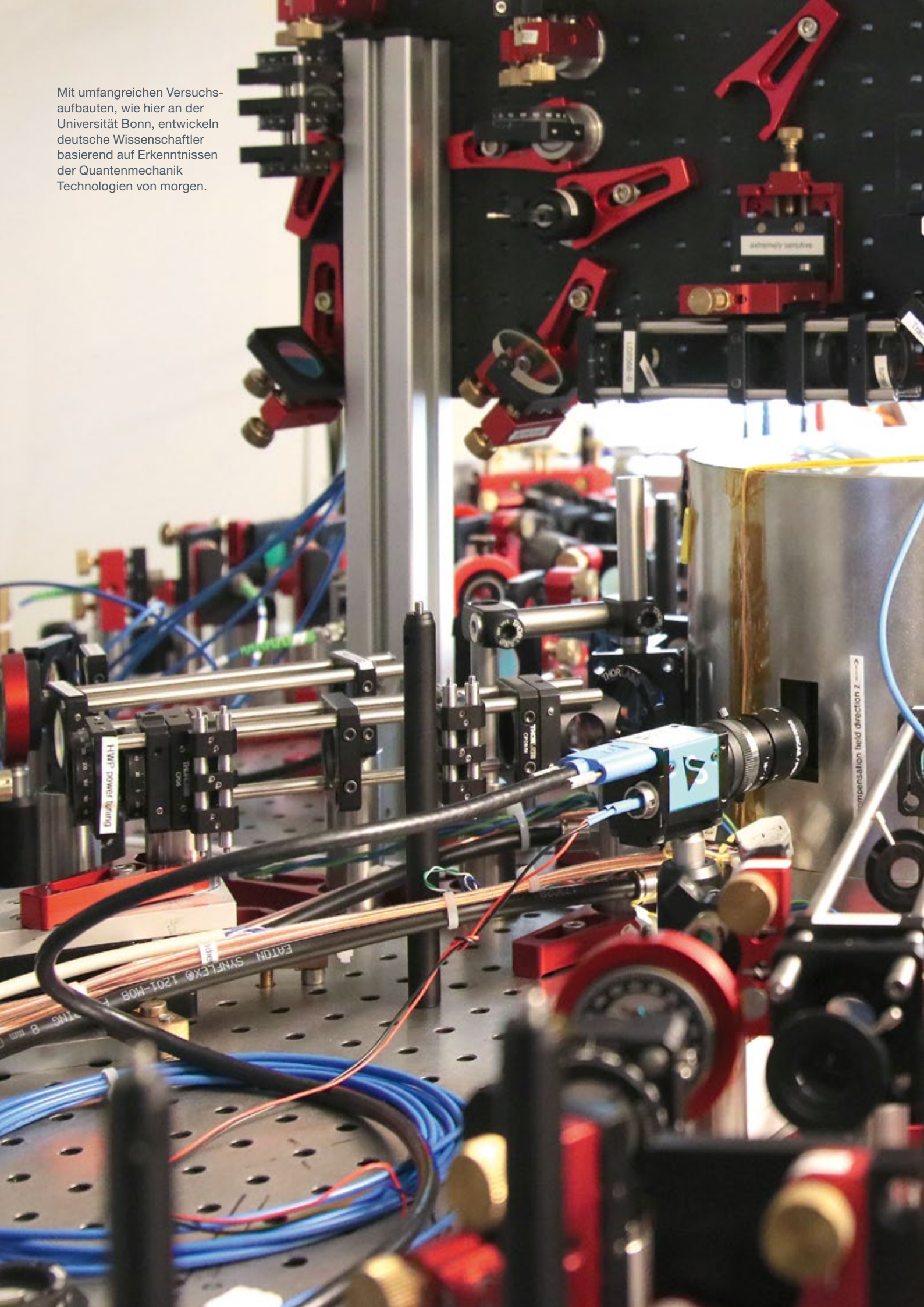
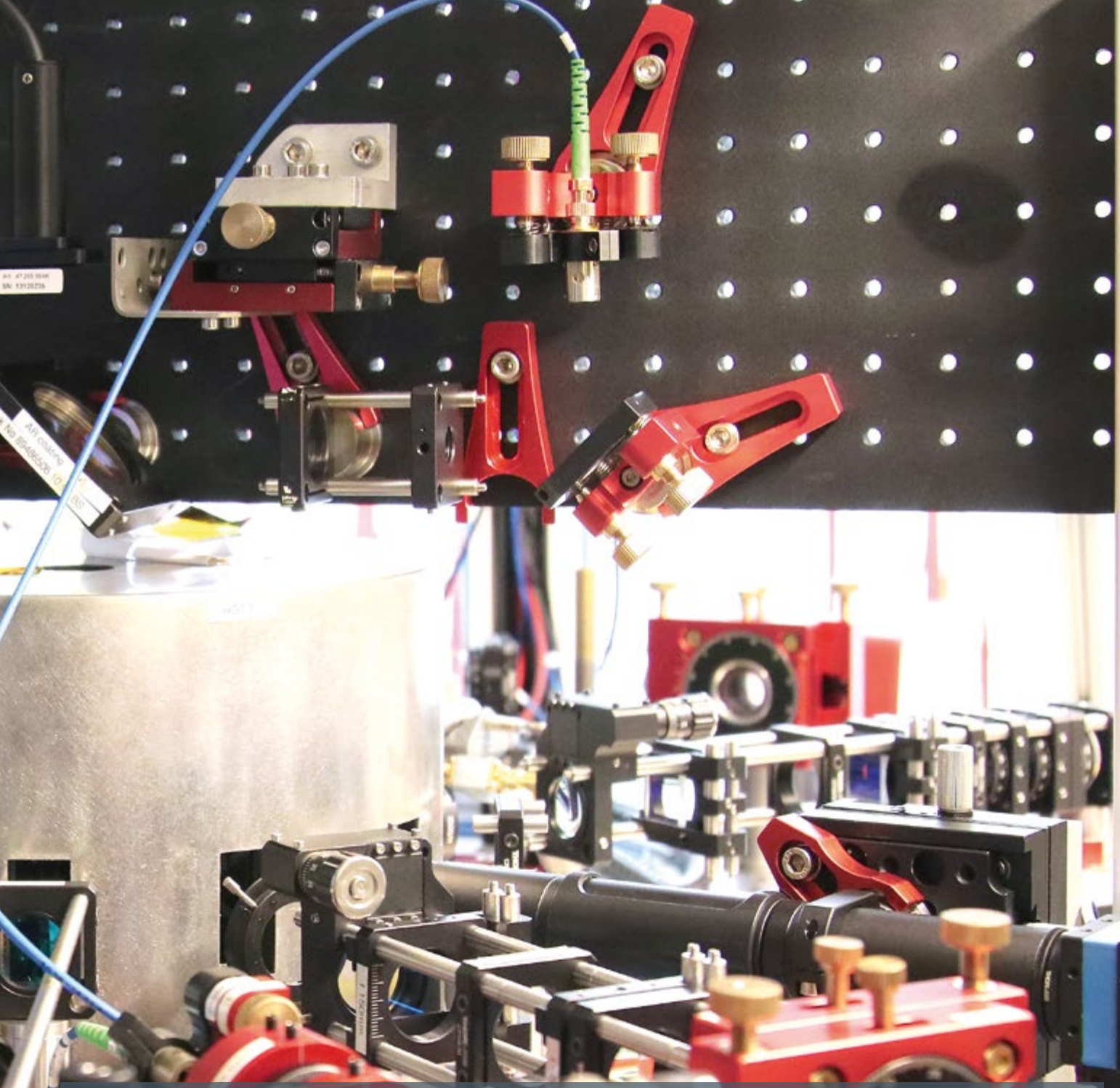


Mit umfangreichen Versuchsaufbauten, wie hier an der Universität Bonn, entwickeln deutsche Wissenschaftler basierend auf Erkenntnissen der Quantenmechanik Technologien von morgen.



GRUNDLAGENFORSCHUNG MADE IN GERMANY

Mit Quantentechnologie in die Zukunft

Quantentechnologie ist derzeit eines der angesagtesten Themen in Wissenschaft und Technik. Vor allem über die Entwicklung von Quantencomputern wird viel diskutiert, und wenn diese neuartigen Rechner eines Tages sehr leistungsfähig geworden sind, wird die Kryptographie sich wieder einmal neu erfinden müssen. Während Quantencomputer – neben vielen anderen Einsatzmöglichkeiten – heute gängige Kryptoverfahren bedrohen, zielt das Forschungsgebiet der Quantenkommunikation auf neue, hochsichere Verschlüsselungsmethoden ab. Was viele nicht wissen: Spitzenforschung rund um Quantentechnologien findet mitten in Deutschland statt. Mit Professor Dieter Meschede und Professor Christof Wunderlich hat secuview zwei der einflussreichsten Wissenschaftler auf diesem Gebiet besucht, die mit ganz unterschiedlicher Zielsetzung Grundlagenforschung betreiben.

Derzeit lässt sich angewandte Quantenphysik auch als mediales Spektakel erleben: Zumindest aus akademischer Perspektive gibt es einen enormen Medienrummel, der den Wettlauf der beiden US-amerikanischen Technologie-Giganten Google und IBM zum nächsten Meilenstein der Quantencomputer-Forschung begleitet. In erster Linie geht es darum, wer den ersten Quantencomputer realisiert, der bei der Lösung bestimmter Aufgaben – dabei handelt es sich tatsächlich um eng begrenzte Spezialaufgaben – klassischen Computern überlegen ist. Die Existenz eines solchen Rechners wird als Wendepunkt angesehen, der mit dem Begriff „Quantum Supremacy“ belegt worden ist.

Allerdings ist es gar nicht so einfach nachzuweisen, wann dieser Punkt erreicht ist. Und selbst wenn er erreicht ist, steht die größte Aufgabe noch bevor: der Bau eines sogenannten universellen Quantencomputers, der leistungsfähig genug ist, um nicht nur Spezialaufgaben, sondern ein großes Spektrum von Rechenoperationen auszuführen. Ein solcher Rechner wird eines Tages voraussichtlich in einigen Bereichen – aber wohl nicht in allen – dramatisch besser abschneiden als klassische Computer.

Bei ihrem Rennen um die „Quantum Supremacy“ stellen die beiden IT-Riesen immer wieder eine Zahl in den Vordergrund, die die Leistungsfähigkeit eines ihrer Systeme anzeigen soll: die Anzahl der Qubits. „Dabei handelt es sich um eine öffentlichkeitswirksame Reduktion“, erklärt Professor Christof Wunderlich, der den Lehrstuhl Quantenoptik an der Universität Siegen innehat. Wunderlichs Team ist Teil der internationalen Spitzenforschung rund um Quantencomputer. Um einen Blick auf die Zukunft der Computertechnologie zu werfen, muss man also keineswegs über den Atlantik schauen.

„Die Anzahl der Qubits ist sicherlich einer von vielen Indikatoren für einen leistungsfähigen Quantencomputer, aber daneben gibt es noch viele andere“, so Wunderlich. „Die PS-Zahl eines Autos sagt ja zum Beispiel noch nichts über Fahrverhalten und Alltagstauglichkeit des Fahrzeugs aus. Nicht einmal dessen Höchstgeschwindigkeit hängt ausschließlich von der Anzahl der PS ab. Ähnlich verhält es sich mit Quantencomputern.“

Mit Qubits rechnen

Vereinfacht gesagt sind Qubits Informationseinheiten analog zu den klassischen Bits, die aber im Gegensatz zu diesen quantenmechanische Zustände nutzen, um Informationen zu codieren. Dabei nutzen sie die Tatsache, dass es in der Quantenwelt, zum Beispiel im Bereich atomarer und subatomarer Teilchen, auch Überlagerungszustände („Superpositionen“) gibt. Dies bedeutet, dass ein Qubit nicht nur die Werte Eins oder Null annimmt, sondern auch in beliebigen Kombinationen dieser beiden Werte existieren kann. Die einzelnen Werte sind dann jeweils mit Wahrscheinlichkeiten belegt (oder genauer mit Wahrscheinlichkeitsamplituden, wobei dann das Quadrat dieser Amplituden Wahrscheinlichkeiten ergibt).

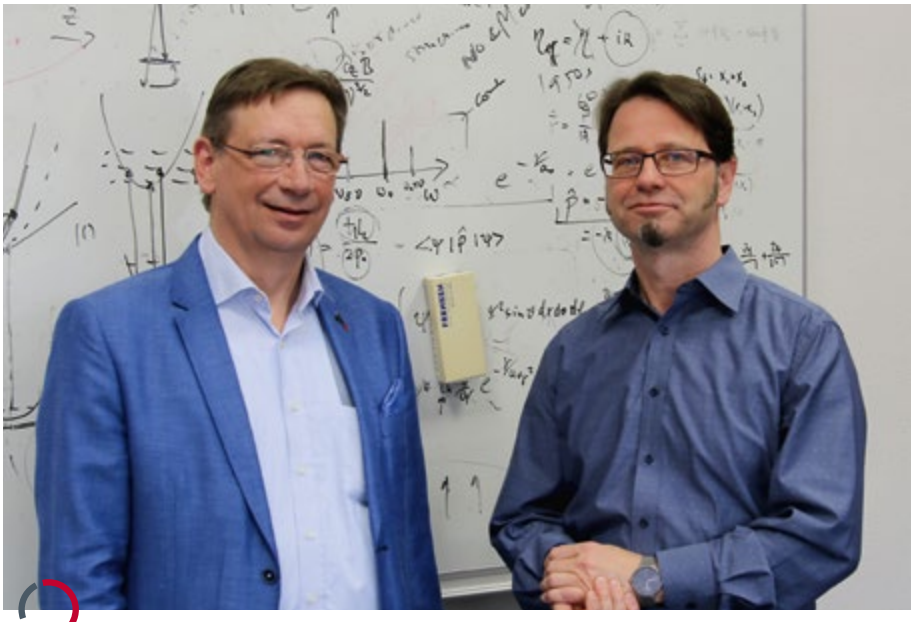
Verbindet man mehrere Qubits miteinander, lassen sich damit logische Operationen durchführen wie mit klassischen Bits – nur auf ganz andere Weise: Die Beschränkung herkömmlicher Rechner auf Einsen und Nullen sowie der Zwang zum seriellen Rechnen entfallen. Quantencomputer müssen nicht Schritt für Schritt vorgehen, sondern beschreiten viele mögliche Lösungswege gleichzeitig. „Was für Lösungswege gilt, gilt auch für Lösungen: Gibt es davon mehrere, findet der Quantencomputer sie alle gleichzeitig – und dann ist es Sache ausgeklügelter Algorithmen, die Rechenoperationen so einzugrenzen, dass verwertbare Ergebnisse dabei herauskommen“, so Wunderlich.

Mit ihrer parallelen Rechenweise sind Quantensysteme prinzipiell dazu geeignet, selbst sehr komplexe Aufgaben zu lösen. Aber es gibt ein Problem: Bei jeder Messung kollabieren die parallelen Zustände und fallen auf einen der möglichen Werte zusammen. Hier helfen die richtigen Algorithmen, um den Quantencomputer auf die Zustände zu „eichen“, die für die jeweilige Aufgabe maßgeblich sind, so dass bei der Messung mit hoher Wahrscheinlichkeit die gesuchten Werte erscheinen.

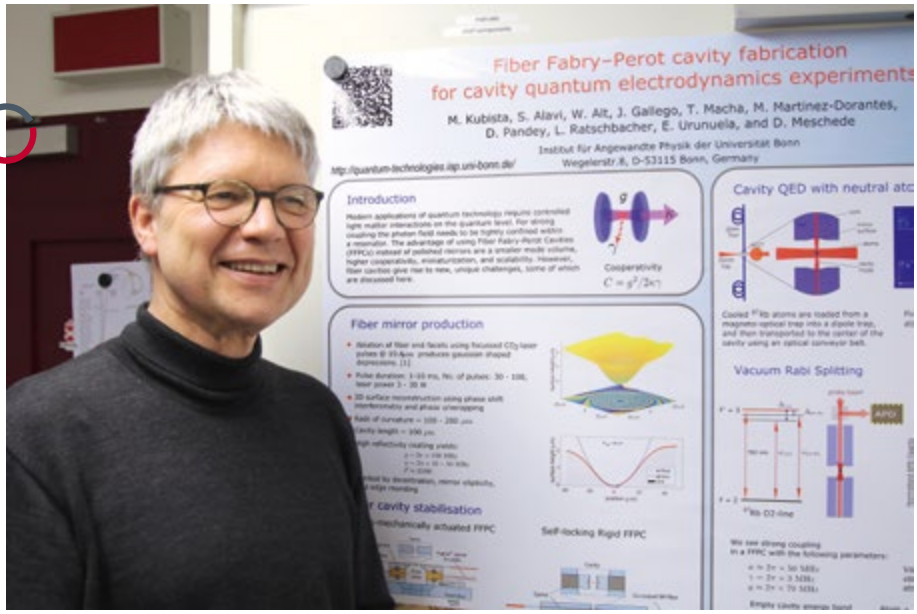
Quantencomputer im Uni-Labor

In Siegen haben Wunderlich und sein Team einen voll funktionsfähigen Quantencomputer mit einigen wenigen Qubits aufgebaut. Mit diesem Versuchsaufbau lassen sich also einfache Rechenoperationen durchführen – was ausreicht, um Quantencomputer weiter zu erforschen und Vorgänge darin zu veranschaulichen. Im Zentrum steht eine Ionenfalle, die einzelne elektrisch geladene Atome mittels Radiofeldern festhält. Quantenmechanische Eigenschaften dieser Ionen dienen in diesem Fall als Qubits. Die Ionen und damit die Qubits können gezielt manipuliert werden, um sie zu verschränken (mehr zum Phänomen der „Verschränkung“ weiter unten) und dann im Verbund Rechenoperationen mit ihnen durchzuführen.

Im Jahr 2000 hat Professor Dieter Meschede, der am Institut für Angewandte Physik der Universität Bonn forscht und lehrt, gemeinsam mit seinem damaligen Team eine neuartige Falle für Atome konstruiert: Damals gelang es dieser Forschergruppe, einzelne Cäsiumatome zu fixieren und kontrolliert zu bewegen – eine wichtige Voraussetzung zur



Dr. Rainer Baumgart zu Besuch bei Professor Christof Wunderlich (rechts) am Lehrstuhl Experimentelle Quantenoptik an der Universität Siegen



Professor Dieter Meschede am Institut für Angewandte Physik der Universität Bonn

Realisierung von Prozessen für Quantencomputer. Die Physiker nutzten Laserstrahlen als „optische Pinzette“, um die Atome festzuhalten und zu manipulieren.

Mit Mikrowellen Atome einfangen

Bei der Ionenfalle im Siegener Quantencomputer indes nutzen Professor Wunderlich und sein Team keine Laser-, sondern Mikrowellenstrahlen. „Ein Vorteil von Mikrowellen ist, dass die notwendige Präzision für die Steuerung von Qubits leichter zu erreichen ist als mit Laserstrahlen, um für Quantencomputer nutzbare Ergebnisse zu erzielen“, erläutert Wunderlich. „Außerdem ist die Technik in der Breite verfügbar. Im Prinzip enthält jedes Smartphone die Komponenten, die man für die Manipulation von Ionen braucht.“ Zwar kommen auch im Siegener Quantencomputer Laserstrahlen vor, jedoch dienen sie hauptsächlich dem Auslesen der Zustände der Ionen, also zum Beispiel der Ergebnisse einer Rechenoperation.

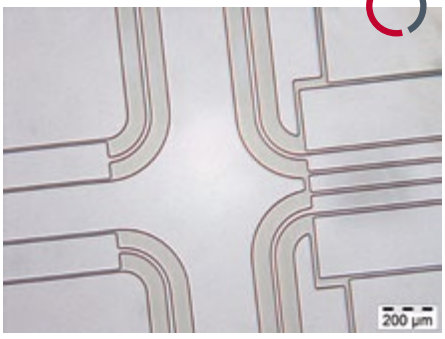
Neben der Realisierung von Qubits mit gespeicherten („eingefangenen“) Atomen und Ionen gibt es noch weitere vielversprechende Ansätze, zum Beispiel den, der von Google und IBM verfolgt wird. Dabei kommen keine einzelnen Atome zum Einsatz, sondern Supraleiter, mit denen sich quantenmechanische Zustände erreichen lassen, obwohl es sich um makroskopische Strukturen handelt. „Welcher dieser Ansätze sich letztendlich als der tauglichste erweist, ist derzeit noch völlig offen“, so Meschede. „Auf jeden Fall sind die Ionenfallen die Vorreiter, und im Vergleich zu den Supraleitern liefern sie sehr gleichmäßige Qubits und arbeiten vergleichsweise stabil.“

Quantenrechner im großen Stil

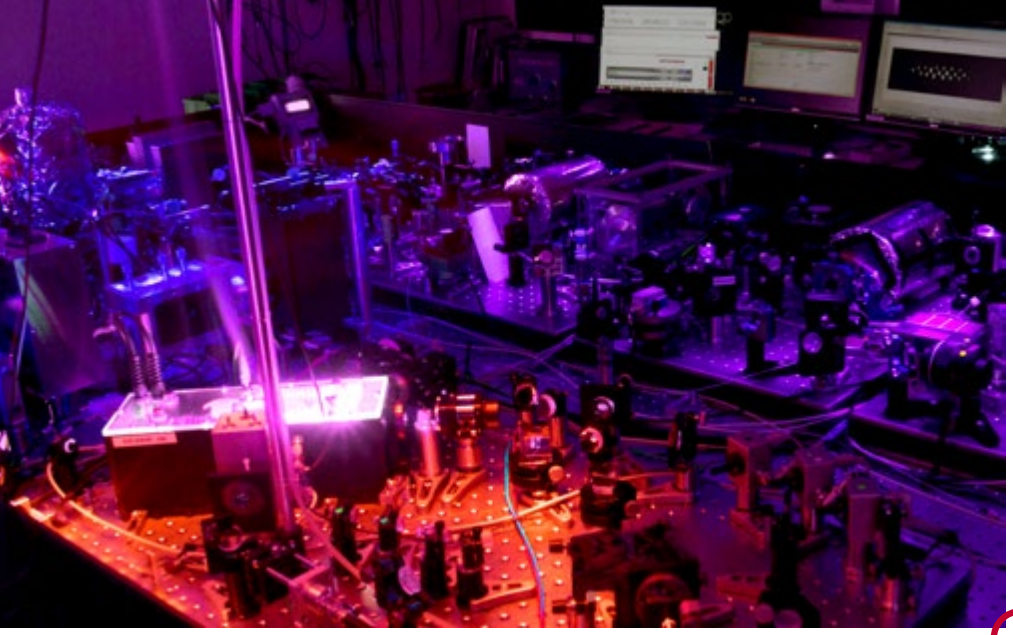
Das Team um Professor Wunderlich hat sich auch der Frage gewidmet, wie sich Versuchsrechner wie der im Siegener Labor zu großen, leistungsfähigen Quantencomputern hochskalieren lassen. Dazu hat die Forschungsgruppe einen eigenen Ansatz entwickelt, bei dem grob vereinfacht mehrere Ionenfallen so nebeneinander platziert werden, dass die darin enthaltenen Ionen in Wechselwirkung treten können. Eine britische Forschergruppe hat sich bereits der Aufgabe verschrieben, im Rahmen eines Unternehmens nach dieser Blaupause Quantencomputer zu bauen. Die Tatsache, dass sich dafür Investoren finden ließen, demonstriert die potenzielle Bedeutung der Forschung aus Siegen für die Wirtschaft.

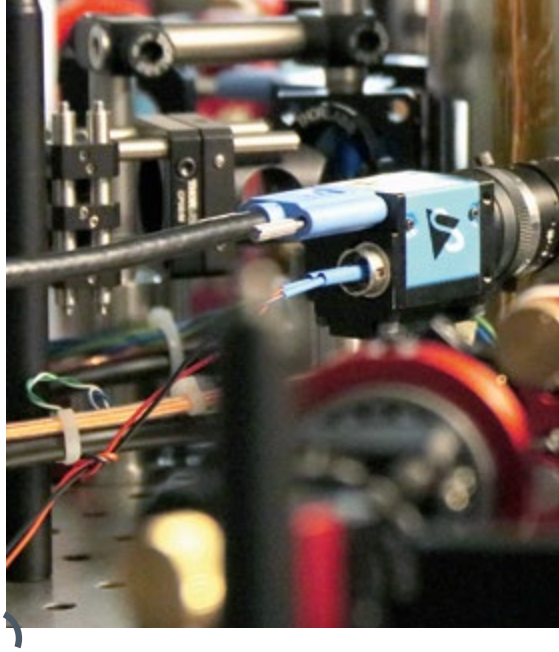
Wofür werden Quantencomputer eingesetzt werden, und wann sind sie verfügbar? Wunderlich: „Ein Anwendungsgebiet, das wahrscheinlich schon in naher Zukunft praktische Relevanz haben wird – voraussichtlich in weniger als zehn Jahren –, ist die Simulation komplexer physikalischer Systeme. Dies kann für die naturwissenschaftliche Forschung, aber auch etwa für die Pharmazie von großer Bedeutung sein.“ Mit weitergehenden Voraussagen tut Wunderlich sich schwer: „Zwar gehe ich davon aus, dass sämtliche wissenschaftlichen Erkenntnisse vorliegen, um große, leistungsfähige Quantencomputer mit gespeicherten Ionen zu konstruieren. Das heißt, es sind keine fundamentalen physikalischen Hürden mehr zu erwarten. Doch wann es tatsächlich zur Realisierung eines sehr leistungsfähigen, universellen Quantenrechners kommt, steht auf einem anderen Blatt. Denn bei derartig

Teilaufnahme eines Fallenchips, den die Siegener Forscher in naher Zukunft testen werden



Diese Aufnahme des Siegener Forschungsteams zeigt eine Kette einzelner Yb+ Ionen.





In den Labors des Lehrstuhls für Quantenoptik in Siegen (links) und des Instituts für Angewandte Physik in Bonn (Mitte) wird untersucht, wie sich quantenmechanische Phänomene technisch nutzen lassen.

innovativen Technologien ist kaum absehbar, auf welcher Zeitskala die weiterhin notwendige Forschung und Entwicklung, auch in den Ingenieurswissenschaften, erfolgreich sein wird."

Gefahr für RSA & Co.

Um einen Quantencomputer zu bauen, der beispielsweise in der Lage ist, heute gängige Kryptoverfahren wie RSA zu brechen, ist wahrscheinlich ein Verbund von Millionen von Qubits nötig. Um dieses Ziel eines Tages zu erreichen, ist noch sehr viel Entwicklungsarbeit nötig. Dennoch ist die IT-Branche gut beraten, sich bereits heute um alternative Verschlüsselungsverfahren zu bemühen, solange die neue Technologie zwar am Horizont erscheint, aber noch nicht ausgereift ist.

Professor Meschede von der Universität Bonn, der mit seinen Forschungen zum Quantencomputer indirekt dazu beigetragen hat, dass die Kryptographie wieder unter Zugzwang gerät, bemüht sich indes mit seinem neuesten Forschungsgegenstand auch in gegenteiliger Perspektive: nämlich um sichere Kommunikation. Die Bonner Forschungsgruppe entwickelt aktuell unter seiner Leitung eine Erweiterung für den sogenannten Quantenschlüsselaustausch (QKD, Quantum Key Distribution). Das Grundprinzip dieses Kryptoverfahrens ist schon seit Jahrzehnten bekannt. Es macht sich eines der faszinierendsten, aber auch bizarrsten Quanteneffekte zunutze: die Verschränkung.

„Spukhafte Fernwirkung"

Dabei handelt es sich um das Phänomen, dass sich bestimmte Eigenschaften von zwei oder mehr Teilchen als Gesamtsystem verhalten, auch wenn die betreffenden Teilchen weit, mitunter viele Kilometer, voneinander entfernt sind. Die fraglichen Eigenschaften der einzelnen verschränkten Teilchen sind zunächst unbestimmt, so wie dies in der Quantenwelt häufig der Fall ist. Doch bei einer Messung werden ihre Eigenschaften auf einen von zwei oder mehr möglichen Werten „projiziert", das heißt sie nehmen diesen bestimmten Wert an. Der entscheidende Punkt ist, dass diese Projektion auf einen bestimmten Wert bei einem verschränkten Teilchenpaar immer gemeinsam („korreliert") geschieht, obwohl es gemäß unserer Alltagserfahrung keinerlei Verbindung zwischen den beiden Teilchen geben dürfte, zum Beispiel weil sie eine große Distanz trennt. Albert Einstein zweifelte in der Frühzeit der Quantenphysik an der Realität der Verschränkung und nannte sie eine „spukhafte Fernwirkung". Jedoch wurde in den darauffolgenden Jahrzehnten nachgewiesen, dass sie tatsächlich existiert.

In Quantencomputern wird Verschränkung genutzt, um Qubits in Quantenregistern zu verbinden. In der Quantenkommunikation hingegen kann man diesen Effekt nutzen, um zwei Kommunikationsteilnehmer – klassischerweise Alice und Bob genannt – mit perfekt zufälligen, aber identischen Einmalschlüsseln zu versorgen, mit denen sie ihre Kommunikation verschlüsseln können. Die Einmalschlüssel werden als Folgen von verschränkten Photonenpaaren erzeugt, und Alice und Bob erhalten jeweils korrelierte „Teilchenpartner" per Glasfaserkabel. Wenn sie nun eine Messung vornehmen, erhält Alice eine vollkommen zufällige Folge von Nullen und Einsen, einen Zufallsschlüssel. Der Clou ist, dass Bob aufgrund der Verschränkung denselben zufälligen Schlüssel generiert. Somit haben die beiden einen perfekt zufälligen, aber identischen Schlüssel zur Verfügung!

Kryptographie mit Quanteneffekten

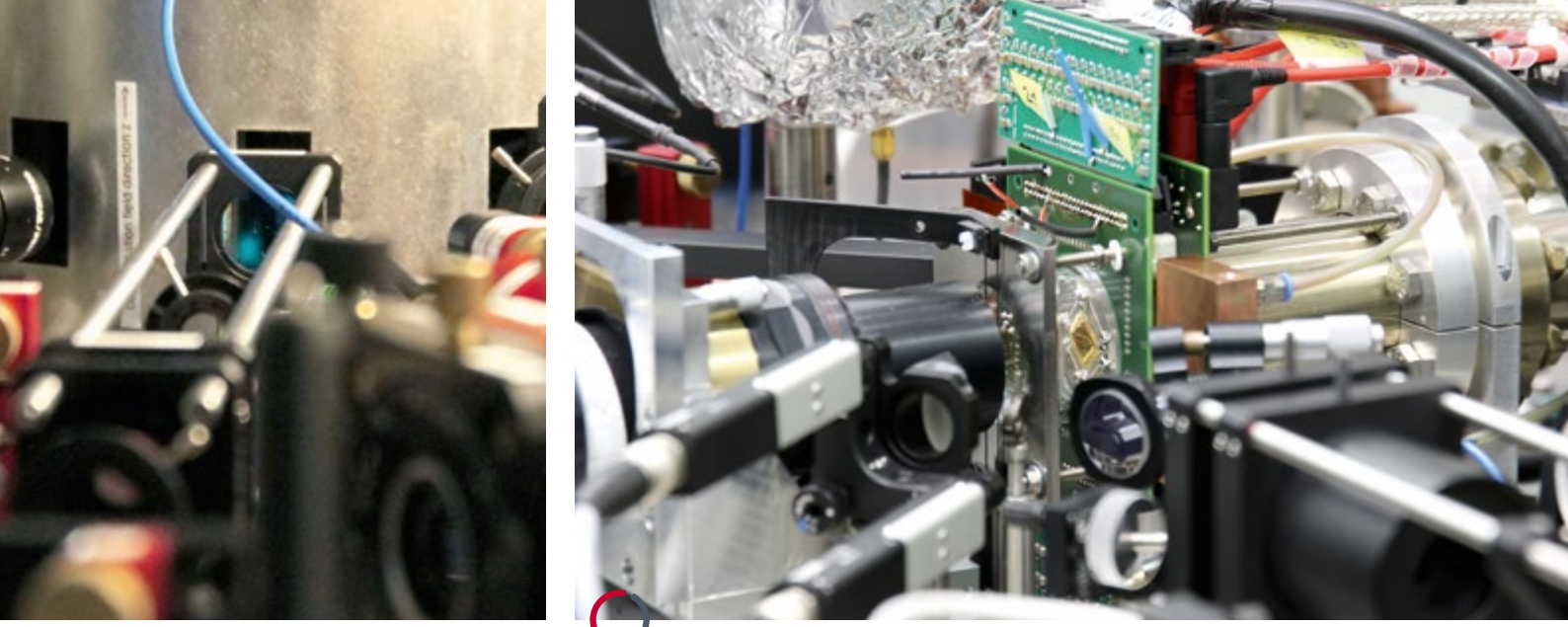
Wie können Alice und Bob nun sicher sein, dass der Schlüsselaustausch nicht von Eve, die einen Lauschangriff startet, mitgelesen wurde? Die Antwort ist, dass Eve mit ihrer Abhöraktion das Quantensystem stören und insbesondere die starke

POST-QUANTEN-KRYPTOGRAPHIE

In der letzten secuview Ausgabe haben wir beschrieben, wie Experten bereits jetzt Verschlüsselungsverfahren entwickeln, die auch in der künftigen Ära des Quantencomputers sicher sind. Auch wenn es wohl noch viele Jahre dauern wird, bis Quantencomputer realisiert werden können, die heute gängige Kryptoverfahren bedrohen, sind diese auf indirekte Weise bereits jetzt gefährdet: Schließlich lässt sich verschlüsselte Kommunikation heute speichern, um sie dann viele Jahre später mithilfe von Quantencomputern zu entschlüsseln.

Hier können Sie secuview 2/2017 mit dem Überblicksartikel über Post-Quanten-Kryptographie kostenfrei herunterladen:

www.secunet.com/secuview



Mit dieser Ionenfalle im Labor des Lehrstuhls Experimentelle Quantenoptik an der Universität Siegen können einzelne Atome festgehalten und manipuliert werden.

quantenmechanische Korrelation zwischen den Teilchen vernichten würde, noch bevor Alice und Bob ihre Messung vornehmen, und das würden die beiden wiederum bemerken. Die QKD ist also ein abhörsicheres quantenmechanisches Kryptoverfahren, und auch ein leistungsfähiger Quantencomputer kann ihr nicht gefährlich werden.

So weit, so eindrucksvoll, aber bisher hatte dieses Verfahren einen Haken: Es ließ sich nur über kurze Distanzen anwenden, weil Lichtsignale im Glasfasernetz mit zunehmender Distanz immer stärker abgeschwächt werden. Für Photonen bedeutet das, dass nach 100 Kilometern nur noch eines von 100 Photonen ankommt. „Für klassische Signale baut man daher in Abständen von etwa 100 Kilometern Verstärker ins Netz“, erklärt Meschede. „Im Fall von Quanteninformationen würde das aber nicht funktionieren, weil klassische Verstärker so wie jede andere Manipulation das verschränkte System sofort stören und in sich zusammenfallen lassen würden.“

Mit Quantenrepeatern sicher kommunizieren

Hier setzt das vom Bundesministerium für Bildung und Forschung (BMBF) neu eingerichtete Forschungsprojekt Q.Link.X an, dem auch die Bonner Forscher zuarbeiten: Dabei geht es um sogenannte Quantenrepeater, die im Glasfasernetz zwischen Alice und Bob geschaltet werden können. Die Repeater können Quanteninformationen zwischenspeichern und dann spezielle Operationen durchführen („Bell-Messungen“), die die Verschränkung der beiden Teilstrecken so verknüpfen, dass die Endpunkte der Gesamtstrecke – Alice und Bob – miteinander verschränkt werden. So kann das QKD-Verfahren im Prinzip auf beliebig große Distanzen angewendet werden.

„Wir werden noch ein paar Jahre brauchen, um an der Technik zu feilen“, so Meschede. „Aber wenn wir das getan haben, wird ein Kommunikationskanal über weite Distanzen zur Verfügung stehen, der aus fundamentalen physikalischen Gründen abhörsicher ist. Daher bin ich mir sicher, dass sich der Aufwand lohnt.“

Ohne Mittel keine Erkenntnisse

An dieser Stelle kommt ein Thema ins Spiel, mit dem sich die meisten Forscher an öffentlichen Instituten beschäftigen müssen: Um ihre Studien fortführen zu können, sind Fördergelder und Drittmittel nötig. Die Wissenschaftler benötigen Kooperationspartner aus der Privatwirtschaft, und sie brauchen auch Fürsprecher, die an die Relevanz ihrer Forschungen glauben und dies gegenüber öffentlichen Geldgebern bezeugen. „Quantentechnologie erfordert einen langen Atem – und Investitionen“, sagt Meschede. „Aber es winken eben auch gewaltige Chancen.“ Dies dürfte bei einem derartigen Forschungsgegenstand gleichermaßen für die Wissenschaft wie auch für die Wirtschaft gelten.

WEITERFÜHRENDE LITERATUR

Zum Thema mikrowellenbasierte Ionenfallen, die in Quantencomputern Verwendung finden können:

Lekitsch, B., S. Weidt, A. G. Fowler, K. Mølmer, S. J. Devitt, C. Wunderlich and W. K. Hensinger (2017). „Blueprint for a microwave trapped ion quantum computer.“ Science Advances 3.

Piltz, C., T. Sriarunothai, S. S. Ivanov, S. Wölk and C. Wunderlich (2016). „Versatile microwave-driven trapped ion spin system for quantum information processing.“ Science Advances 2: e1600093.

Aktuell arbeitet Prof. Christof Wunderlich an einem Artikel, der die von dem Siegener Team verfolgten Forschungsarbeiten etwas allgemeinverständlicher erklärt als die beiden vorgenannten Veröffentlichungen.

Zum Thema Quantenkommunikation / Quantenrepeater:

Becher, C., Meschede,D., Michler,P. und Werner,R. (2016). „Sichere Kommunikation per Quantenrepeater.“ Physik in unserer Zeit 1/2016, Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim (https://doi.org/10.1002/piuz.201601418)