idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Universität des Saarlandes
Thorsten Mohr

22.01.2014
http://idw-online.de/de/news570132

Forschungs- / Wissenstransfer, Forschungsprojekte
Informationstechnik, Physik / Astronomie
überregional

Was ist dran am Quantencomputer? Saarbrücker Quantenphysiker erklären den Stand der Technik

Vor Kurzem haben Medien über die Entwicklung eines Supercomputers auf Grundlage der Quantentechnologie berichtet, mit dem der US-Geheimdienst NSA sämtliche Kommunikation der Welt mitlesen könnte, egal, wie gut sie auch verschlüsselt wäre. Saarbrücker Physiker sehen für solche Bedenken derzeit keine Grundlage. „Es ist nichts bekannt geworden, was solche Befürchtungen auslösen sollte", sagt Jürgen Eschner. Der Professor für Quanten-Photonik ist einer von fünf Experten an der Saar, die sich im Schwerpunkt Quantenoptik und -information um die Welt der kleinsten Teilchen kümmern. Damit ist Saarbrücken einer der wenigen Orte bundesweit, die sich in dieser intensiven Weise dem Thema widmen.

Seit Jahren geistert er durch die Medien: der Quantencomputer. Mal ist er der Hoffnungsträger für eine bessere Zukunft, mal das Orwell'sche Schreckgespenst in den Händen des totalitären Staates. Im Moment überwiegt die negative Sichtweise auf die Wunder-Rechenmaschine. Jüngst erregten Medienberichte über ein Programm der NSA viel Aufmerksamkeit, wonach der US-Geheimdienst an der Entwicklung eines solchen Computers arbeite. Damit könnten die Geheimagenten alle Verschlüsselungsmechanismen der Welt knacken, und kein Geheimnis wäre mehr vor ihnen sicher. Experten indes mahnen in dieser Debatte zur Sachlichkeit, da von einer Serienreife eines solchen Supercomputers, der jeden Code der Welt knacken kann, noch lange nicht die Rede sein kann.

„Das heute gängigste Verschlüsselungsverfahren, die RSA-Kryptografie, basiert auf der Multiplikation zweier Primzahlen. Das ist eine Rechenaufgabe, die sehr leicht durchzuführen ist, aber sehr schwer umzukehren ist", erklärt Frank Wilhelm-Mauch, Professor für Quanten- und Festkörpertheorie an der Saar-Uni. „Wenn man zum Verschlüsseln beispielsweise eine 100-stellige Zahl als Produkt zweier Primzahlen erhält und ein Codeknacker eine Stunde mit einem herkömmlichen Supercomputer braucht, um die Zahl in ihre beiden Primfaktoren zu zerlegen, so braucht er bei einer 101-stelligen Zahl bereits 1000 Stunden und bei einer 102-stelligen Zahl bereits eine Million Stunden. Das bedeutet also: Der Codierer gewinnt das Wettrüsten."

Sein Kollege Christoph Becher, Professor für Quantenoptik, erklärt, worin vor diesem Hintergrund theoretisch die Gefahr eines Quantencomputers liegt: „Für einen Quantencomputer existiert – auf dem Papier – ein Algorithmus, der diese Primfaktorzerlegung effizienter und damit in kürzerer Zeit als ein herkömmlicher Computer erledigen kann." Auch wenn man die Zahl um ein paar Stellen länger machte, dauerte es nur wenig länger, bis ein serienreifer Quantencomputer die Verschlüsselung geknackt hätte.

Es gibt allerdings zwei Gründe, weshalb die Saarbrücker Experten solche Erwartungen an einen Quanten-Supercomputer für übertrieben halten: „Der größte Quantencomputer, den es bisher gibt, umfasst gerade einmal 14 Quanten-Bits, und die größte Primzahlfaktorisierung, die man bislang mit einem Quantencomputer berechnen konnte, ist 15 = 3*5. Anders gesagt: Mit Papier und Bleistift könnte man Codes derzeit noch deutlich besser brechen als mit der Quantentechnologie", sagt Frank Wilhelm-Mauch. Heute gängige Verschlüsselungsverfahren verwenden Zahlen mit mehr als 100 Stellen. „Um solche Zahlen effizient in ihre Primfaktoren zu zerlegen, bräuchte man Computer

mit Tausenden Q-Bits, die alle perfekt funktionieren", so der Experte. Und davon ist die technische Entwicklung noch weit entfernt: „Verglichen mit der Entwicklung der herkömmlichen Computertechnologie sind wir auf dem Gebiet der Quantencomputer irgendwo bei den Elektronenröhren der 50er Jahre", erklärt Christoph Becher.
Der zweite Grund, weshalb die Saarbrücker Experten einen Quantencomputer nicht als allzu große Gefahr einstufen, ist, dass die Verschlüsselung von Informationen mittels Quantentechnologie derzeit deutlich weiter ist als die Bemühungen, mit Quantentechnologie Verschlüsselungen zu knacken. „Verschlüsselung und Codebrecher laufen auf völlig unterschiedlicher Hardware und funktionieren nach anderen Prinzipien", erklärt Jürgen Eschner. „Eine Verschlüsselung ist sehr viel einfacher, da dies ein serieller Prozess ist. Der muss einfach nur sehr häufig hintereinander gemacht werden. Ein Quantencomputer hingegen, der Verschlüsselungen knacken soll, muss sehr viel mehr leisten. Hier laufen die Prozesse parallel ab, das macht die Sache ungemein kompliziert."

Gelingt es, mittels der Quantentechnologie ein zuverlässiges Verschlüsselungsverfahren zu entwickeln, wäre die Angst vor einem Quantencomputer, der in sämtliche Kommunikation der Welt einbrechen kann, ohnehin ad acta gelegt. „Wenn ein Codeknacker Sie abhört, dann merken Sie das und hören auf zu kommunizieren. Das hängt damit zusammen, dass schon die Beobachtung eines Quantensystems im Allgemeinen dieses Quantensystem verändert – ein tausendfach bestätigtes Naturgesetz", so Frank Wilhelm-Mauch. Könnte man also mit quantentechnischen Mitteln die Kommunikation verschlüsseln, könnte man ein so genanntes „One Time Pad" entwickeln, „einen Schlüssel, den man nur einmal anwendet – und wenn man merkt, dass man abgehört wird, würde man den entsprechenden Teil des Schlüssels verwerfen". Auch ein Quantencomputer, der die Kommunikation knacken möchte, wäre dann nutzlos.

Neben Sicherheitsfragen widmen sich die Saarbrücker Wissenschaftlerinnen und Wissenschaftler auch noch einer Reihe weiterer Anwendungen von Quantentechnologien, wie hochpräzises Messen, effiziente Simulation neuer Materialien und chemischer Prozesse und schnelle Datenbanksuche.

Hintergrund Quantentechnologie:

Zugrundeliegendes Prinzip der Quantentechnologie ist, dass ein Teilchen (z.B. ein Atom, Elektron, Lichtteilchen) zwei Zustände gleichzeitig einnehmen kann. Diese Zustände nennt man auch Überlagerungszustände. Auf die Computertechnologie übertragen bedeutet das, dass die Bits, aus denen eine Information auf einem normalen Computer besteht, die Zustände 1 oder 0 haben können, auf einem Quantencomputer hingegen die Zustände 1 und 0 gleichzeitig, in jeder beliebigen Kombination. Solche Quantenbits oder Qubits sind die Grundlage eines Quantencomputers. Rechnen kann man beispielsweise mithilfe von Atomen als Speichereinheit, indem man sie mit Laserlicht anregt und ihren Quantenzustand gezielt manipuliert. Eine Rechenoperation kann nun auf beiden Anteilen des Überlagerungszustandes (1 und 0) gleichzeitig oder parallel stattfinden. Ein Quantencomputer kann in derselben Zeit, in der ein herkömmlicher 32-Bit-Rechner einen seiner 232 möglichen Zustände verarbeitet, parallel alle diese Zustände verarbeiten. Der Quantencomputer rechnet also um ein Vielfaches schneller als ein normaler Computer. Diese hohe Rechenleistung lässt sich allerdings nur für spezielle Probleme ausnutzen, für die Rechenvorschriften (Algorithmen) entwickelt wurden.
Bei vielen der Überlagerungszustände befinden sich die Quantenbits in einem „verschränkten Zustand", d.h. sie lassen sich als Ganzes, nicht aber mehr als unabhängige Teilchen beschreiben. Sowohl verschränkte Zustände als auch Überlagerungszustände sind allerdings sehr empfindlich auf jede Wechselwirkung mit ihrer Umgebung und verlieren schnell ihren Quantencharakter. Für einen Quantencomputer bedeutet dies, dass man großen Aufwand für die Abschirmung von Umwelteinflüssen treiben muss – ein anderes Gebiet der Quantentechnologien nutzt aber genau diese Tatsache aus: in der Quantenkommunikation können geheime Nachrichten in verschränkten oder Überlagerungszuständen kodiert werden. Versucht ein Spion Kenntnis der Nachricht zu erhalten, zerstört er den Quantenzustand und der Abhörversuch fliegt auf.

Folgende Wissenschaftlerinnen und Wissenschaftler sind in den vergangenen Jahren nach Saarbrücken gekommen, um den Schwerpunkt Quantenoptik und Quanteninformation zu bilden:

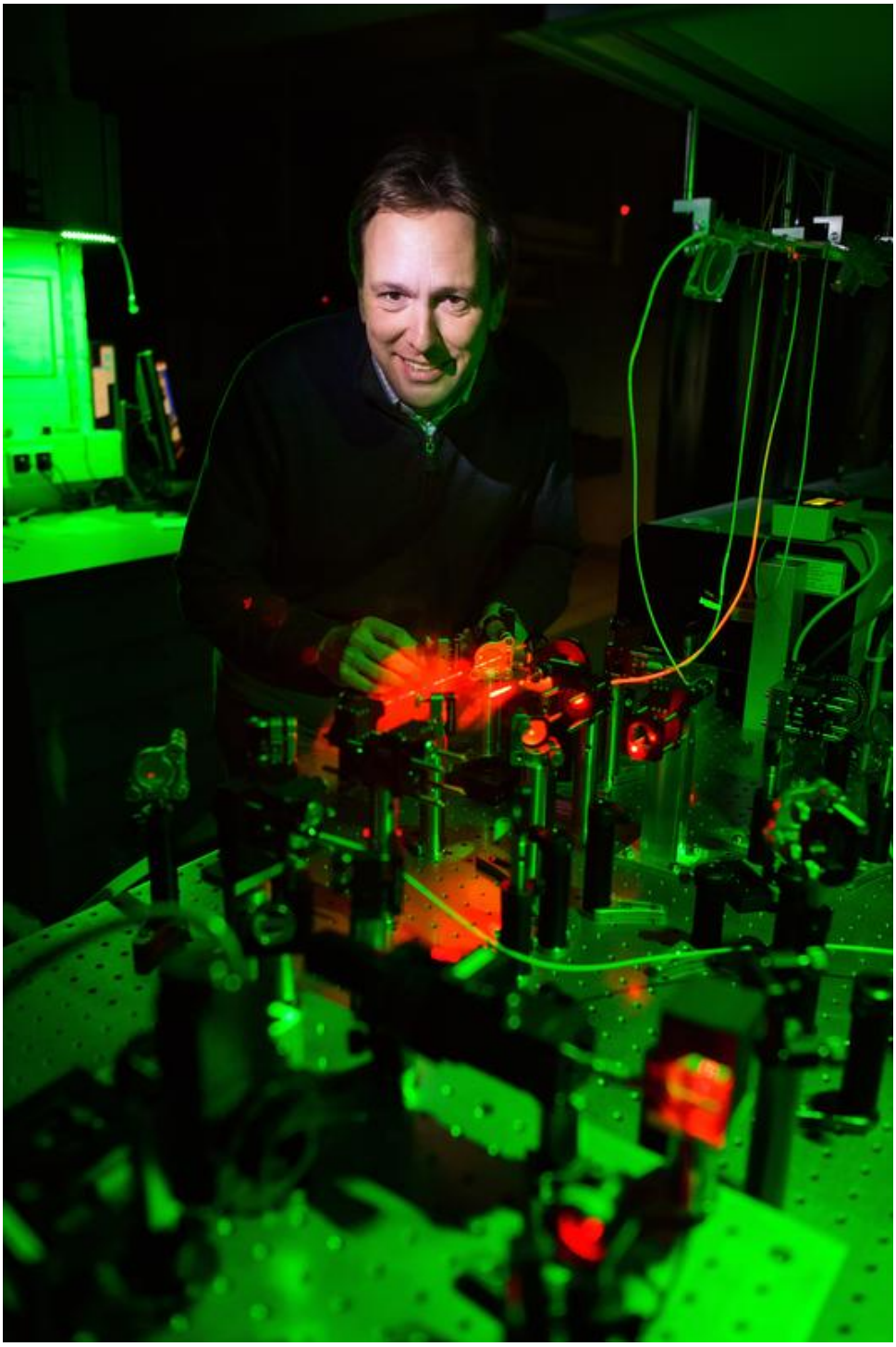
Christoph Becher: Am Lehrstuhl des Professors für Quantenoptik entwickeln die Physiker Technologien für die Quantenkommunikation, beispielsweise neuartige Lichtquellen mit künstlichen Atomen in Diamant und Frequenzwandler, die Lichtteilchen in einen anderen Wellenlängenbereich umsetzen können.

Jürgen Eschner: Der Professor für Quanten-Photonik forscht an seinem Lehrstuhl daran, den Kommunikationsprozess zwischen lokalen Speichern für Quanteninformation (Atomen) und dem Übertragungsmedium (Lichtteilchen; Photonen) zu kontrollieren.

Giovanna Morigi: Die Professorin für Theoretische Quantenphysik erforscht an ihrer Lehrstuhl an grundlegende Konzepte der Quanteninformationsverarbeitung und der Quantenmetrologie.

Frank Wilhelm-Mauch: Der Professor für Quanten- und Festkörpertheorie erforscht an seinem Lehrstuhl die Theorie für die Hardware des Quantencomputers.

Pavel Bushev: Der Juniorprofessor für Experimentelle Festkörperphysik erforscht in der Arbeitsgruppe „Mikrowellen-Quantensysteme“ Quanteninformationsspeicher in Kristallen mit Selten-Erd-Atomen und die Übertragung von Quanteninformation mit Mikrowellen.



Christoph Becher ist einer von fünf Quantenphysikern an der Saar-Uni, die den Stand der Technik in Sachen Quantencomputer beurteilen können.
Foto: Oliver Dietze