Das Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen berichtet über neue Technologien

Quantenverschränkung in der Technik

Die Quantenmechanik beschreibt unsere Welt auf den kleinsten Skalen und bei den niedrigsten Energien, d. h. auf der Ebene von Atomen und Teilchen. Die Quantenverschränkung ist ihr zentraler und gleichzeitig „geheimnisvollster" Aspekt. Sie gehört zu den wesentlichen Phänomenen, die bei sogenannten Quantentechnologien ausgenutzt werden und ist damit eine wichtige Grundlage vieler neuer Technologie-Konzepte und -Entwicklungen, welche in ihrer Gesamtheit oft unter dem Begriff Quantenrevolution 2.0 zusammengefasst werden. Bereits in absehbarer Zeit ist hier mit einer zunehmenden Zahl praktischer Anwendungen zu rechnen.

Bei der Quantenverschränkung handelt es sich um eine fundamentale und vor allem instantane „Verbindung" zwischen Quantenobjekten, die u. a. dann auftritt, wenn zwei Teilchen miteinander wechselwirken: Diese tragen dann das „Wissen" um ihre „Begegnung" bis zur nächsten Wechselwirkung quasi weiterhin in sich. Untereinander verschränkte Teilchen können somit prinzipiell nicht mehr einzeln, sondern nur als Gesamtsystem beschrieben werden, auch wenn sie sehr weit voneinander entfernt sind.

Auf der Quantenverschränkung aufbauende Anwendungen lassen sich in zwei große Gruppen einteilen, die Quanteninformationstechnologien (z. B. Quantencomputer, Quantenkryptografie, Quantennetzwerke) und die Quantensensoren (z. B. Quantenbildgebung).

Die gegenwärtig weltweit erforschten, aber noch nicht praktikablen Quantencomputer nutzen gerade die Quantenverschränkung, um bei bestimmten Berechnungen (für die ein entsprechender Quantenalgorithmus existieren muss) gegenüber klassischen Computern eine zum Teil exponentiell größere Leistungsfähigkeit zu erreichen. Diese entsteht insbesondere daraus, dass sie ihre Quantenbits (Qubits) miteinander verschränken, bevor Rechenoperationen darauf ausgeführt werden, wodurch die Anzahl der Zustände, die solche sogenannten Quantenregister annehmen können, exponentiell steigt. Mit Quantencomputern können andere Quantensysteme wie Atome, Moleküle und Festkörper effizient simuliert werden, was zu ganz neuen Möglichkeiten in der Entwicklung neuer Materialien führen könnte. Außerdem könnten sie Big-Data- und insbesondere KI-Anwendungen erheblich beschleunigen. Andererseits kann ein universeller Quantencomputer jedoch bestimmte gebräuchliche Verschlüsselungssysteme brechen, wie die im Internet verwendeten Public-Key-Verfahren, die u. a. auf dem Aufwand zur Faktorisierung großer Primzahlen beruhen, was jedoch mit Quantencomputern effizient möglich wird. Für einen nützlichen universellen Quantencomputer braucht man je nach auszuführendem Quantenalgorithmus mindestens einige 1.000 perfekte Qubits. Quantenverschränkung ist jedoch eine extrem flüchtige und kurzlebige Eigenschaft, gegen deren raschen Zerfall schon bei kleinsten Störungen aus der Umgebung aufwendige Quantenfehlerkorrekturverfahren angewendet werden müssen, die wiederum viele zusätzliche Hilfs-Qubits benötigen, um Fehler bei den zur Berechnung benutzen Qubits zu erkennen und rückgängig zu machen. Daher nimmt man an, dass mindestens etwa eine Million solcher imperfekten, physikalischen Qubits nötig sind. Mit nutzbaren universellen Quantencomputern ist somit wohl erst mittel- bis langfristig, d. h. frühestens in etwa 15 Jahren zu rechnen.

Die Quantenkryptografie nutzt quantenmechanische Effekte für neuartige Verschlüsselungssysteme, die aus physikalischen Gründen zumindest in der Theorie „unknackbar" sind. Als Grundlage dienen sogenannte Einmalschlüssel. Bei deren Anwendung ergibt sich jedoch das Problem, dass sie erst einmal sicher zwischen den Kommunikationspartnern ausgetauscht werden müssen. Hier kommt die Quantenverschränkung ins Spiel: Beim sogenannten Quantenschlüsselaustausch wird ausgenutzt, dass man mit einem geeigneten Verfahren beim Übertragen von verschränkten Quantenzuständen prinzipiell erkennen kann, wie viele Qubits auf ihrem Weg zum Empfänger von Dritten mitgelesen wurden. Ist diese Menge nicht zu groß, so kann anschließend die Information, die der Angreifer potenziell über den ausgetauschten Schlüssel hat, beliebig klein gemacht werden. Während kleinere Netzwerke zum optischen Quantenschlüsselaustauch über Glasfaserkabel in einigen Ländern schon im Betrieb sind, ist ein echtes Quantennetzwerk, das z. B. Quantencomputer an verschiedenen Orten miteinander verschränken und damit verbinden kann, noch Zukunftsmusik. In ca. fünf Jahren könnte immerhin mit einer ersten Demonstration des Prinzips mit mindestens drei Knoten über 50 bis 100 km Entfernung gerechnet werden.

Bei den verschiedenen Verfahren der Quantenbildgebung wird ganz allgemein die Quantenverschränkung zwischen Photonen als zusätzliche „Ressource" genutzt, um verschiedene Eigenschaften klassischer optischer Abbildungen zu verbessern. So soll es z. B. mit sogenannten quantenlithografischen Verfahren möglich werden, Halbleiterstrukturen für Computerchips zu fertigen, die viel kleiner sind als die Wellenlänge des zur Belichtung verwendeten Lichts. Bei Verfahren wie der Quantenbeleuchtung werden typischerweise durch nichtlineare optische Prozesse erzeugte verschränkte Photonenpaare genutzt, wobei die einzelnen Photonen eines Paares sehr unterschiedliche Wellenlängen haben können. So kann die Beleuchtung des Objekts durch Photonen einer Wellenlänge (z. B. im Ferninfraroten) und die Bildaufnahme durch die mit ihnen verschränkten Photonen einer anderen Wellenlänge (z. B. im Sichtbaren) erfolgen, wenn für letztere bessere Detektoren bzw. Bildsensoren existieren. Objekte können so auch vor starkem Hintergrundrauschen und vor allem mit sehr geringer Beleuchtungsstärke abgebildet werden, weil selektiv nur solche Photonen detektiert werden, die tatsächlich vom Objekt zurückgestreut wurden. Militärisch ist dieses Prinzip vor allem beim Konzept des sogenannten Quantenradars angedacht.

Zurzeit werden verschiedene Verfahren der Quantenbildgebung weiterentwickelt. Gleichzeitig wird intensiv nach praktischen Einsatzmöglichkeiten gesucht. Mit ersten Anwendungen, z. B. in der Medizintechnik, ist kurz- bis mittelfristig zu rechnen.

Dr. Oliver Gabel