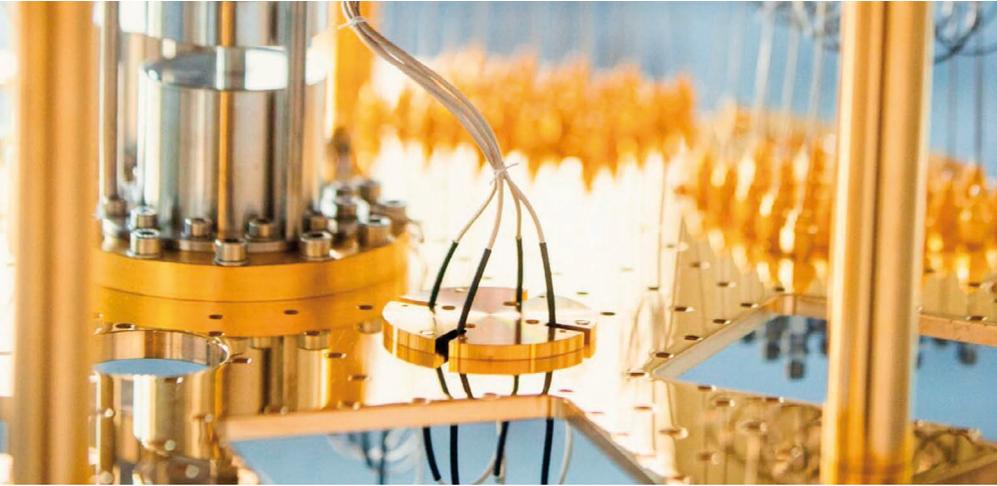


# Quantencomputer – Das Rechnen mit Quanten



Supraleitende Qubits © BADW/Kai Neunert

### Zusammenfassung: Teil 1 und Teil 2

Unter einem Quantencomputer, einem Quantenprozessor, verstehen wir einen Prozessor, der die Gesetzmäßigkeiten der Quantentheorie nutzt. Der klassische Rechner arbeitet mit elektrischen Strömen und der Quantenprozessor arbeitet auf der Basis von quantenmechanischen Zuständen, wie dem Superpositionsprinzip oder der Quantenverschränkung. Zur Nutzung dieser Effekte sind ganz spezielle Versuchsaufbauten notwendig. Um die Quantensysteme von äußeren Einflüssen zu isolieren, sind für die Versuchsaufbauten extrem niedrige Temperaturen notwendig, derzeit noch nahe dem absoluten Nullpunkt. So besteht eine Aufgabe der Forschung darin, die Technik so weiterzuentwickeln, dass sie auch bei „Normaltemperatur“ eingesetzt werden kann.

Quantencomputing wird als eine Schlüsseltechnologie des 21. Jahrhunderts angesehen. So investieren viele Regierungen und Forschungsorganisationen, als auch Computer- und Technologiefirmen weltweit in die Entwicklung dieser Technologien. Man geht davon aus, dass mit Quantencomputern manche komplexe Berechnung schneller gelöst werden kann als mit herkömmlichen Rechenzentren.

### Architektur des Quantencomputing

In diesem Artikel wollen wir uns die Architektur eines Rechnersystems näher anschauen, das mit einem Quantenprozessor als Rechenkern ausgestattet ist. Ausgangspunkt ist die kleinste Quanten-Einheit, das Qubit. Anschließend betrachten wir den grundsätzlichen Aufbau des Prozessors, bevor wir näher auf die Auswertung der Ergebnisse eingehen. Dabei werden auch Begriffe wie Treffergenauigkeit oder Verifikation der Ergebnisse berücksichtigt.

### Quantenbit

Das klassische Bit ist eine einstellige binäre Zahl, die also nur ‚0‘ oder ‚1‘ oder ‚ein‘ oder ‚aus‘ darstellen kann. Das ist die kleinste Einheit, mit der traditionelle Rechner arbeiten.

Im Quantenprozessor ist die kleinste logische Einheit das Quantenbit, kurz Qubit genannt. Das Qubit ist ein Zweizustands-Quantensystem, also ein System, das nur zwei Zustände hat, die sich mit einer Messung sicher unterscheiden lassen. Im Gegensatz zum klassischen Bit kann das Qubit aber unendlich viele Werte durch Superposition annehmen. Es dient als kleinstmögliche Speichereinheit und definiert gleichzeitig ein Maß für die Quanteninformation.

Das Quantensystem Qubit wird als Information interpretiert und besitzt, mathematisch gesehen, einen zweidimensionalen Zustandsraum  $\mathbb{C}^2$ . Der Nobelpreisträger Felix Bloch hatte diesen für die Darstellung eines quantenphysikalischen Zwei-Zustands-Systems entwickelt, die sog. Bloch-Kugel (Bild 2).

### Beschreibung der Bloch-Kugel

Die Vektoren beschreiben die Zustände eines Quantenbits und sind normiert, d. h. sie haben alle die Länge 1. Deshalb bilden die Endpunkte aller möglicher Vektoren die dreidimensionale

Oberfläche einer Kugel in einem vierdimensionalen Raum. Für mathematische Berechnungen ist dieser Ansatz sehr gut geeignet - aber anschaulich ist das nicht mehr darstellbar. Der Übergang zur Bloch-Kugel ist vergleichbar mit dem Übergang zwischen Kreis und Kreisgleichung  $x^2 + y^2 = r^2$ .

### Voraussetzung für das System Quantenprozessor

Um Qubits herzustellen, zu manipulieren und auszulesen, werden derzeit unterschiedliche technische Ansätze verfolgt. Im Prinzip kann jedes quantenmechanische Zweizustandssystem als Qubit verwendet werden. In der Praxis jedoch sind viele Systeme ungeeignet, da sie nicht in ausreichendem Maße manipulierbar sind oder zu stark von der Umgebung gestört werden. Auch die Skalierbarkeit ist eine notwendige Voraussetzung für den Einsatz. Daher muss heute ein sehr hoher und spezieller technischer Aufwand betrieben werden. Typische Rahmenbedingungen sind beispielsweise Temperaturen in der Nähe des absoluten Nullpunkts und/oder starkes Vakuum. Beides sind große Herausforderungen für den praktischen Einsatz.

### Ergebnisse verbessern

Damit man physikalische Qubits möglichst fehlerfrei nutzen kann, schließt man diese zu großen Ensembles zusammen, um die Ergebnisse von Berechnungen zu verbessern. Je nach Anwendung benötigt man dafür eine hohe Anzahl solcher physikalischer Qubits (bis zu 10.000 oder sogar noch mehr), um ein einziges fehlerkorrigiertes, logisches Qubit zu erzielen. Das bedeutet eine große Aufgabe für die Entwicklung in den jeweiligen Ansätzen.

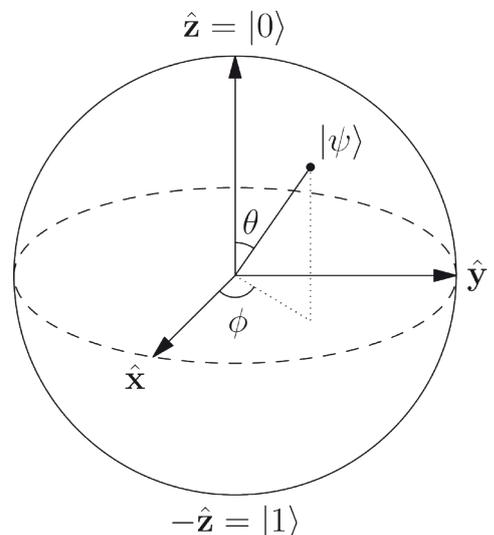


Bild 2: Die Bloch-Kugel

Autoren:  
Günter Kornmann  
Tom Weber

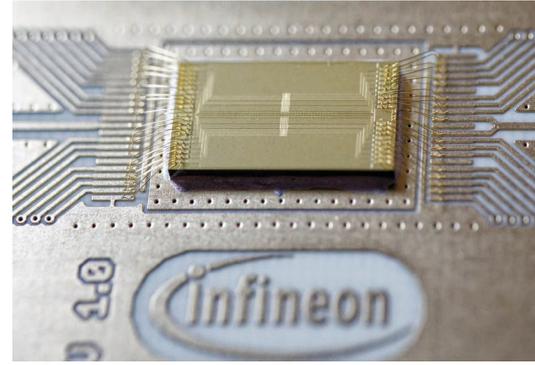


Bild 3: Ionenfallen-Qubits © Infineon

dieses einzelnen Elektrons ist ein natürliches Quantensystem, bei dem die Spinrichtung die Information repräsentiert, die das Qubit trägt.

## Kernspins in Molekülen und Festkörpern

Auch die Spins der Atomkerne in Molekülen können Qubits repräsentieren. Über Kernspinresonanz können sie manipuliert und ausgelesen werden. Dies ist eine technisch besonders einfache Methode, die jedoch nicht den oben genannten DiVincenzo-Kriterien entspricht. Insbesondere ist die Methode nicht skalierbar, da die Zahl der Spins pro Molekül beschränkt ist. Zudem kann hierbei nicht ein einzelnes System (also ein einzelnes Molekül) gemessen werden, sondern man hat es mit vielen gleichartigen Molekülen auf einmal zu tun. Allerdings kann man mit Kernspins in Festkörpern skalierbare Architekturen realisieren. Besonders vielversprechend sind hier z. B. die Kernspins von Fremdatomen in Silizium oder von Stickstoff-Fehlstellen-Zentren in Diamanten.

## Quantengatter

Klassische Rechner arbeiten mit elektronischen Gattern, wie beispielsweise UND- oder ODER-Verknüpfungen. Vergleichbar arbeitet der Quantenprozessor mit Quantengattern. Ein Quantengatter arbeitet jedoch mit quantenmechanischen Systemen, wie etwa dem Spin.

Das Quantengatter stellt in der Regel aber kein physisches Bauelement dar: Es ist eine zeitlich steuerbare Wechselwirkung der Qubits untereinander oder mit der Umgebung. Trotzdem ist es wünschenswert, dass - ähnlich wie beim klassischen Computer - einige elementare und einfach zu realisierende Quantengatter zur Verfügung stehen. Dies erleichtert die Realisierung von Recheneinheiten mit dem Quantenprozessor.

Praxisrelevant sind heute Quantengatter mit 1-Qubit Gatter (z. B. Beeinflussung des Spins) sowie 2-Qubit Gatter (CNOT, XOR, Phasenkontrolle). Gatter mit mehr als zwei Eingängen sind grundsätzlich denkbar, wegen der Mehrteilcheneffekte aber bedeutend schwieriger in der Umsetzung.

Mathematisch ist eine mit Quantengattern realisierte Operation eine umkehrbare (reversible) Transformation. Das hat zur Folge, dass

Unter dem Namen ‚DiVincenzo criteria‘ wurden 1996 Kriterien für Quantencomputer veröffentlicht. Das System muss somit wohldefinierte Qubits haben und skalierbar sein, d. h., es muss prinzipiell auf beliebig viele Qubits erweiterbar sein. Außerdem muss es möglich sein, die Qubits in einem reinen Zustand zu präparieren, d. h. in wohldefinierte Quantenstrukturen zu bringen (mindestens in den Zustand  $|00000\dots\rangle$ ).

Das System muss eine hinreichend lange Dekohärenzzeit aufweisen, d. h. dass in dieser Zeit keine Überlagerungen der Quantensysteme, wie Superpositionen, vorkommen. Auch muss es die Implementierung eines universellen Satzes von Quantengattern (siehe weiter unten) erlauben. Ein Beispiel wäre z. B. alle 1-Qubit-Gatter und zusätzlich das CNOT-Gatter. Zusätzlich ist es wichtig, dass jedes der einzelnen Qubits gezielt gemessen werden kann. Für einen ein-satzfähigen Quantenprozessor müssen alle diese Bedingungen erfüllt sein.

Für die Quantenkommunikation ist zudem die Möglichkeit erforderlich, stationäre und sich im Kommunikationskanal befindliche Qubits ineinander zu überführen sowie die Möglichkeit, Qubits über einen Kommunikationskanal über längere Strecken zu übertragen.

Erstaunlich ist, dass die konkrete Ausprägung der „rechnenden“ Quantenstrukturen oder „Teilen“ keine wesentliche Rolle spielt, egal ob es sich um Photonen handelt, Ionen, SQUIDs (superconducting quantum interference devices, dt. supraleitende Quanten-Interferenzgeräte) oder etwas ganz anderes. Es kommt nur darauf an, dass eine Quanteneigenschaft von ihnen die Rolle eines Qubits übernehmen kann. Das kann beispielsweise die Polarisation eines Photons, der Spin eines Ions oder die Stromrichtung im SQUID sein.

## Praktische Ansätze für die Realisierung von Qubits

Nachfolgend werden die Ansätze für Qubits beschrieben, an denen derzeit intensiv geforscht bzw. an deren Umsetzung konkret gearbeitet wird.

### Supraleitende Qubits

Supraleitende Qubits (Aufmacherbild) sind, historisch betrachtet, die erste technologische Plattform, mit der in einem Experiment ein Geschwindigkeitsvorteil von Quantencomputern nachgewiesen werden konnte.

Von Supraleitung wird gesprochen, wenn Ströme ohne jeglichen elektrischen Widerstand fließen. Das ist bei vielen supraleitenden Materialien erst bei sehr niedrigen Temperaturen in der Nähe des absoluten Nullpunkts der Fall. Sie ist ein makroskopischer Quantenzustand. Mit modernen Kryostaten, also sehr guten Kühlschränken, können Temperaturen nahe dem absoluten Nullpunkt mittlerweile mit vertretbarem Aufwand erreicht werden. Typische supraleitende Materialien in der Herstellung dieser Schaltkreise sind Aluminium, Niobium oder Tantalum.

Aus den Supraleitern lassen sich Schaltungen formen, die sich sehr ähnlich zu Atomen verhalten. Diese Schaltungen können als supraleitende Kondensatoren, lineare, sowie nicht-lineare Induktoren verstanden und als Qubits verwendet werden. Die Zustände dieser Schaltungen oder künstlichen Atome wiederum können mit Mikrowellen und damit rein elektrisch manipuliert und ausgelesen werden.

In einer speziellen Geometrie als supraleitende, ringförmige Systeme, sogenannte SQUIDs, die aus zwei oder mehreren parallelen speziellen Kontakten bestehen, ergibt sich eine Abhängigkeit von der relativen Phase.

### Ionenfallen-Qubits

Der Ionenfallen-Ansatz ist bereits relativ weit fortgeschritten. Hierbei werden einzelne Ionen durch elektromagnetische Felder im Vakuum wie an einer Perlenkette aufgereiht. Die Qubits werden dabei durch jeweils zwei langlebige interne Zustände der einzelnen Ionen gebildet.

Die Zahl der Qubits ist identisch mit der Zahl der Ionen in der Falle. Die Manipulation der Qubits erfolgt über Laser, die mit den einzelnen Ionen wechselwirken. Über die Bewegung der Ionen in der Falle lassen sich die Qubits miteinander koppeln und verschränken.

Dafür werden zuverlässige und leistungsfähige Quanten-CCD-Implementierungen entwickelt (CCD: charge-coupled device, deutsch „ladungsgekoppeltes Bauteil“), bei denen Ionen durch spezialisierte Prozessor-Zonen verschoben werden. Infineon ist es mit einem Technologie-Demonstrator (Bild 3) mit einer Speicherkapazität von 18 einzelnen Ionen erstmals gelungen, die parallele Bewegung zweier Ionen-Arrays zu demonstrieren.

Ionenfallen-Qubits arbeiten bei Temperaturen von circa 10 Kelvin (K), also bei etwa  $-263\text{ °C}$ , also einem Temperaturniveau, das mit einem vergleichsweise geringen Aufwand realisierbar ist.

### Halbleiterbasierte Spin-Qubits [1]

Ein weiterer Ansatz ist die Verwendung von Quantenpunkten, um Qubits zu Erzeugen. Quantenpunkte sind Halbleiterstrukturen, in denen die Bewegungsfähigkeit von Elektronen so stark reduziert ist, dass die nur noch diskrete Zustände einnehmen können (Bild 4).

Silizium-Prozesse sind in der Halbleitertechnik bestens bekannt und leicht handhabbar. In Verbindung mit dem Halbleitermaterial Germanium lassen sich Strukturen realisieren, um einzelne Elektronen oder deren Gegenspieler, sogenannte Löcher, einzufangen und als Qubit zu verwenden.

Ein Vorteil der Quantenpunkt-Technologie ist, dass bei der Herstellung erprobte Halbleiter-Prozesse verwendet werden. Bei der Herstellung eines Quantenpunktes wird ein zweidimensionaler See aus Elektronen mit Hilfe geeigneter Gatter-Elektroden derart eingeschnürt, dass schließlich nur ein einziges Elektron übrig bleibt. Der Spin

# Quantencomputing

die Funktion jedes Quantengatters mit einem anderen Quantengatter rückgängig gemacht werden kann. Deshalb kann ein Quantengatter auch nicht mehr Eingänge als Ausgänge haben, sonst ginge ein Qubit irgendwo verloren.

Während bei einem konventionellen Rechner die Leitung von einem Bit beliebig häufig aufgeteilt werden kann, ist dies bei einem Quantencomputer nicht möglich. Daher gibt es in einem Quanten-Schaltkreis genau eine Leitung pro Qubit.

## Quantencomputing mit definiertem Versuchsaufbau

Der Quantenprozessor nutzt die Fähigkeiten und Phänomene der Quanten und der sich daraus bildenden Quantensysteme. Dabei kommen im Wesentlichen das Superpositionsprinzip und die Quantenverschränkung (siehe Teil 2) zum Tragen.

Für die korrekte Eingabe gewünschter Daten müssen entsprechende Maßnahmen vorbereitet werden. Die notwendigen Qubits müssen zur Startzeit die gewünschten Daten repräsentieren. Beim Quantencomputing legen daher die notwendigen experimentellen Vorgaben beispielsweise die Richtungen fest, in denen sich die Photonen (welche ein Qubit für die Verarbeitung transportieren) im Quantenprozessor bewegen können. Dadurch werden nur noch zwei Parameter benötigt, welche die Polarisation bestimmen.

Diese Zustände werden durch normierte Vektoren (mit der Länge 1) repräsentiert. Diese Vektoren bilden die Oberfläche der dreidimensionalen Bloch-Kugel; ihre Koordinaten sind durch deren Längen- und Breitengrad bestimmt. Ist der Zustand nicht exakt bekannt, dann liegt er im Inneren der Bloch-Kugel. Ein Wert im Mittelpunkt der Kugel beschreibt die Existenz eines Qubits, dessen Zustand aber völlig unbekannt ist.

## Ablaufende Prozesse

Die Qubits sind in allen Fällen Eigenschaften von Quanten, z. B. Photonen oder Ionen. Nach-

folgend wollen wir am Beispiel von Ionen zeigen, welche Prozesse im ablaufen:

- Zur Dateneingabe werden die Ionen durch genau berechnete Laserpulse in die gewünschten Zustände gebracht und miteinander verschränkt.
- Die einzelnen Ionen liegen anschließend nicht mehr vor, sie haben sich zu einem ganzheitlichen Quantensystem vereinigt. In diesem System sind sehr viel mehr Zustände möglich, als die einzelnen Ionen selbst bilden könnten.
- Weitere Laserimpulse wirken auf die ganzheitlichen Quantensysteme ein und verändern damit deren gemeinsamen Zustand.
- Die gezielte Abfolge der Lasereinwirkungen entspricht einem Programm-Ablauf im traditionellen Rechner.

Andere Versuchsaufbauten erfordern entsprechend andere Initialisierungen oder Eingriffe in die Quantensysteme, z. B. Steuerung durch gezielte elektromagnetische Einwirkungen.

## Quantencomputing ist reversibel

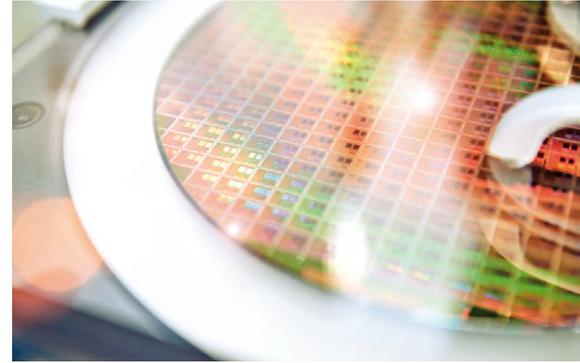
Betrachtet man einen konventionellen, logischen Schaltkreis, welcher zwei Zahlen miteinander multipliziert, dann liefert dieser das Produkt der beiden Eingabewerte. Dieser Schaltkreis ist in aller Regel irreversibel aufgebaut - d. h. aus dem Ergebnis kann ein klassischer Rechner nicht einfach die Ausgangswerte ermitteln. Beispiel: Das Ergebnis 20 könnte z. B. aus der Operation  $4 \times 5$ , oder  $2 \times 10$  oder  $1 \times 20$  entstanden sein.

Im Gegensatz dazu sind die quantischen Zustände in einem Quantenprozessor während des Rechenprozesses von der Außenwelt isoliert. Die Veränderungen dieser Quantenstrukturen oder Quantensysteme sind während des Rechenvorganges reversibel, d. h. sie können nach einer gewissen Weile auch wieder den Ausgangszustand annehmen. Das kommt daher, weil während des gesamten Rechenablaufs kein Faktum entsteht, sondern "nur" permanent quantische Veränderungen stattfinden. Ein Faktum entsteht erst durch die Interaktion mit der Umwelt.

Mathematisch gesehen wird der Zustandsvektor in einem Raum (mit sehr großer Dimension) durch Drehen gemäß des Versuchsaufbaus beeinflusst. Das beabsichtigte Ergebnis wird durch eine Messung oder Beobachtung zu einem Faktum. Diese Messung ist dann aber irreversibel. Dieses gemessene Faktum kann wieder zum Initiieren eines neuen reversiblen Quantenprozesses genutzt werden.

## Zusammenfassung

Halten wir fest: Klassische Rechner arbeiten seriell und das Ergebnis kann jederzeit ausgelesen werden. Quantenprozessoren arbeiten massiv parallel und das Auslesen beendet den Rechenprozess.



**Bild 4: Halbleiter basierte Spin-Qubits © Infineon**

Nennt man den quantischen Aufbau eine "Schaltung", dann arbeiten Quantencomputer also auf der Basis von reversiblen (d. h. umkehrbaren) Schaltungen. Das heißt, mit Hilfe der Ausgaben eines Systems kann man stets wieder auf die Eingaben schließen. Auch Quantengatter sind reversibel oder repräsentieren eine reversible Operation. Damit kann sowohl Multiplikation, als auch Faktorisierung, als Problem des Grundzustands verstanden und mit Methoden der Quantenprozessoren gelöst werden.

Nebenbei bemerkt: Auf Grund des No-Cloning-Theorems sind reversible Operationen nicht kopierbar.

## Die exakte Lösung – Validierung der Ergebnisse

Das durch die Messung entstandene Faktum kann grundsätzlich nicht alle Möglichkeiten des Quantensystems widerspiegeln. Also ist zu prüfen, ob das beobachtete Ergebnis ein ausreichend gutes Ergebnis ist.

Dazu ein Beispiel: Der Shor-Algorithmus ist dafür entwickelt worden, eine Zahl  $N$  in ihre Primzahlen zu zerlegen. Liefert ein Quantenprozessor mit dem Shor-Algorithmus für den Eingabewert 2406507 beispielsweise das Ergebnis 89, 137 und 199, dann ist das nicht korrekt, wie sich mit einem Taschenrechner schnell überprüfen lässt. (Die korrekte Lösung wäre 87, 139 und 199.)

Wenn es also auf eine exakte Lösung ankommt, dann ist eine Prüfung unbedingt notwendig. Mit einem konventionellen Computer kann diese Prüfung sehr viel schneller erfolgen, als die eigentliche Berechnung. Denn wie am obigen Beispiel bereits gezeigt, ist es sehr viel schneller möglich, große Zahlen miteinander zu multiplizieren, als eine große Zahl in ihre Primfaktoren zu zerlegen. Das Multiplizieren ist immer schneller als das Dividieren. Wenn der Quantencomputer ein mögliches Ergebnis liefert, dann kann man es mit den klassischen Rechnern leicht überprüfen.

Die Validierung des Ergebnisses hängt natürlich von der Fragestellung ab, welche Aufgabe der Quantenprozessor zu lösen hat. Der Shor-Algorithmus ist für quantische Lösung prädestiniert: denn die klassischen Algorithmen benötigen sehr viel Rechenleistung - während die

## Randbemerkung für mathematisch Interessierte

Hätten wir die vorgegebenen experimentellen Randbedingungen im Quantenprozessor nicht, müssten die abstrakten Zustände weiterhin im komplexen Raum  $\mathbb{C}^2$  behandelt werden. Da wir aber durch den Aufbau des Quantencomputers den Kontext festgelegt haben (z. B. die Richtung) ist vorbestimmt, auf welche Weise ein Photon durch die Blenden gelangen kann. Dadurch reichen zwei reelle Parameter, die zwei Winkel in der Bloch-Kugel, anstatt zweier komplexer Parameter. Das Rechenergebnis wird durch eine gezielte Beobachtung (Messung) ermittelt, wobei die möglichen Ergebnisse (mögliche Winkelverteilungen) auf einen Punkt gelegt werden, und somit einen faktischen Punkt bestimmen.

Lösungsvorschläge des Quantenprozessors damit sehr leicht verifizierbar sind.

Und wo ist die praktische Relevanz? Das Zerlegen von großen Zahlen in Primfaktoren ist die Grundlage von zahlreichen Verschlüsselungstechniken.

## Bewertung der Ergebnisse

Oft existiert nicht eine einzige richtige Lösung, wie im Beispiel der Primfaktorzerlegung. Bei Optimierungsaufgaben ist eine gute Lösung oft ausreichend. So kann es durchaus sein, dass Quantenprozessoren, dank ihrer hohen Rechengeschwindigkeit, sehr schnell mehrere fast gleichwertige Lösungsvorschläge erarbeiten. Dann genügt vielleicht eine intelligente Auswahl der Vorschläge, oder eine gute Approximation an das gesuchte Optimum. In all diesen Fällen kommt es auf die Rechenleistung der Quantenprozessoren an, verbunden mit einer guten Bewertung der Vorschläge, zum Beispiel bei Wettervorhersagen.

## Rechengenauigkeit – fehlerfreier Quanten-Rechenprozess

Von den Quantenprozessoren erwarten wir natürlich auch, dass sie mit hoher Rechengenauigkeit arbeiten. Es dürfen keine Fakten entstehen, also Beeinflussungen von außen, bevor der Rechenprozess abgeschlossen ist. Dazu sind noch technische Herausforderungen zu lösen. Derzeit scheint die sicherste Vorgehensweise zu sein, dass man die Quantenprozessoren in der Nähe des absoluten Nullpunktes betreibt. Je kälter ein System ist, desto geringer ist die Wahrscheinlichkeit, durch das zufällige Auftreffen von Wärme-Photonen "Pseudo-Fakten" zu erzeugen.

Die extreme Empfindlichkeit der Qubits bedeutet noch viel Forschungs- und Entwicklungsarbeit, denn schon das geringste Einwirken von außen kann die Eigenschaften der Quantensysteme beeinflussen. So können magnetische sowie elektrische Felder, Licht, Temperaturen oder auch Erschütterungen den Rechenprozess manipulieren oder gar zerstören. Deshalb müssen die rechnenden Quantensysteme, auch die Qubits, aus denen sie aufgebaut sind, stabil gehalten werden. Die Aufgabe besteht darin, sie möglichst gut abzuschirmen. Gleichzeitig müssen sie auch manipuliert werden können, um überhaupt einen Rechenprozess erzielen zu können.

Dafür werden beispielsweise supraleitende Qubits bei Temperaturen nahe dem absoluten Nullpunkt von  $-273,15\text{ °C}$  verwendet und mehrfach von der Umgebung abgeschirmt. Aber selbst dann bleiben diese Qubits immer nur Bruchteile von Sekunden stabil – ein minimaler Zeitraum, in dem die Berechnungen stattfinden müssen.

Andere Qubit-Technologien, wie Ionen, sind wiederum zwar deutlich stabiler und behalten ihre Eigenschaften über Minuten oder sogar Stunden, dafür brauchen sie aber für einen einzelnen Rechenschritt deutlich länger.

Es gibt bereits erste Möglichkeiten zur Fehlerkorrektur in Quantenprozessoren, aber trotzdem ist es von hoher Wichtigkeit, auf fehlerfreie Rechenprozesse zu achten. Das Ziel für diese Prozessoren muss eine möglichst universelle Programmierbarkeit sein, und das erfordert fast beliebige Einstellungen. Das bedeutet, dass sehr genaue Anfangszustände erzeugt werden müssen und dass gezielte Eingriffe auch die gewünschten Ergebnisse liefern.

## Fehlerkorrektur beim Quantencomputing

Klassische Fehlerkorrekturen funktionieren mit Redundanz. Dazu werden einzelne Daten mehrfach gespeichert und bei Unterschieden wird auf die Mehrzahl zugegriffen. Quanteninformation zu kopieren, ist wegen des No-Cloning-Theorems nicht möglich und deshalb kommt diese Methode nicht in Betracht.

Es gibt aber bereits die ersten Ansätze für Fehlerkorrekturen im Quantenprozessor. Eine Vorgehensweise besteht darin, mehrere Prozesse parallel zueinander ablaufen zu lassen, die aber miteinander verschränkt sind. Wird ein Qubit durch eine unerwünschte Einwirkung verändert, dann kann durch einen Vergleich mit den anderen Qubits eine Korrektur vorgenommen werden. Es wird dabei angenommen, dass eine gleichzeitige Veränderung von mehreren Qubits unwahrscheinlicher ist, als nur von einem Qubit. Dies erfordert jedoch viel Redundanz.

Beim Umkippen eines Zustands von  $|0\rangle$  in  $|1\rangle$  kann der Bit-Flip-Code eine Korrektur bewerkstelligen. Dafür sind jedoch drei Qubits erforderlich. Ebenfalls mit drei Qubits kann mit dem Sign-Flip-Code die Vertauschung von einem ‚Plus‘ in ein ‚Minus‘ korrigiert werden. Es ist auch möglich, beide Codes zu kombinieren. Dieser Code ist nach Peter Shor benannt, dem Entwickler des Shor-Algorithmus zur Faktorzerlegung. Dafür sind jedoch neun Qubits notwendig, um an einem Qubit beide möglichen Fehler zu beheben. An dem Qubit, mit welchem die eigentliche Rechnung durchgeführt wird, darf nicht direkt geprüft werden, das würde sofort ein Faktum erzeugen und den reversiblen Rechengang beenden. Diese möglichen Fehlerkorrekturen erhöhen die Anzahl der notwendigen Qubits im Quantenprozessor gewaltig, was wiederum den Aufbau des Prozessors erschwert.

Noch eine Bemerkung: Das Thema der Quantenalgorithmen wird derzeit noch völlig übergangen. Es existiert keine etablierte Software. Bisher sind nur die beiden Algorithmen zur Faktorisierung von Peter Shor und der Clover-Algorithmus bekannt.

## Einweg-Quantenprozessor

Ein interessanter Ansatz ist der des Einweg-Quantencomputers [2]. Dabei wird ein universeller verschränkter Quantenzustand aus vielen Qubits erzeugt. Entsprechend der Aufgabenstellung wird eine entsprechende Messung durchgeführt, d. h. es wird eine faktische Lösung

herbeigeführt. Die Bereitstellung von speziellen Qubits ist nicht notwendig.

Nach der Messung ist der universelle Quantenzustand zerstört, für die nächste Aufgabe wird ein neuer universeller Quantenzustand notwendig. Die Ergebnisse früherer Messungen bestimmen wahrscheinlich, welche weitere Messungen durchgeführt werden.

## Schlussfolgerung

Wir haben gesehen, dass beim Quantencomputing in sehr viel kürzerer Zeit ein Ergebnis vorliegt als im Vergleich zum klassischen Rechner. Auf das Ergebnis des klassischen Rechners können wir uns verlassen, das Ergebnis beim Quantenprozessor resultiert aus einem komplexen Vorgang innerhalb des Quantenprozessors, der so aufgebaut sein muss, dass die Messung mit hoher Wahrscheinlichkeit das richtige Ergebnis liefert. Das Ergebnis bedarf einer Verifikation, meist durch eine Bewertung mit dem klassischen Rechner. Kommt es auf Geschwindigkeit an, dann hat das Quantencomputing einen großen Vorteil.

Eine weitere Erkenntnis ist, dass Quantencomputing noch in den Kinderschuhen steckt und nur in der Symbiose mit klassischen Rechnern funktioniert. Aber trotzdem sollte man die spannende Entwicklung verfolgen, es steckt beim richtigen Einsatz ein riesiges Potential drin. Dies betrifft sowohl den Quantenprozessor als auch die Quantenalgorithmen.

## Ergänzende Literatur:

Görnitz Thomas, Quantentheorie verstehen – Grundlegende Vorstellungen und Begriffe, 2022, Carl Hanser Verlag, München

<https://www.infineon.com/cms/de/product/promopages/quantumcomputing>

<https://www.infineon.com/cms/de/discoveries/quantum-computing/>

## Referenzen

[1] <https://www.infineon.com/cms/de/product/promopages/quantumcomputing/#halbleiterbasierte-spin-qubits>

[2] Raussendorf R, Browne D E, Briegel H J (2002) The one-way quantum computer – a non-network model of quantum computation, Journal of Modern Optics, 49, 1299

## Wer schreibt:

Günter Kornmann ist Diplom-Mathematiker. Seine berufliche Heimat ist die Chipentwicklung. Über Stationen bei Siemens und Infineon war er einer der Innovationsmanager bei Intel. Seit einigen Jahren unterstützt er mittelständische Unternehmen bei der Umsetzung des Innovationsmanagements.

Tom Weber ist Dipl.-Ing. der Nachrichtentechnik. Er arbeitet seit 35 Jahren im Technischen Marketing und führt seit über zehn Jahren die einzige europäische Beratungsgesellschaft für technologische Unternehmensentwicklung. ◀