

RUHR-UNIVERSITÄT BOCHUM

RUB

# RUBIN

WISSENSCHAFTSMAGAZIN

## EISKALT

**Routiniert:** Warm bleiben im ewigen Eis

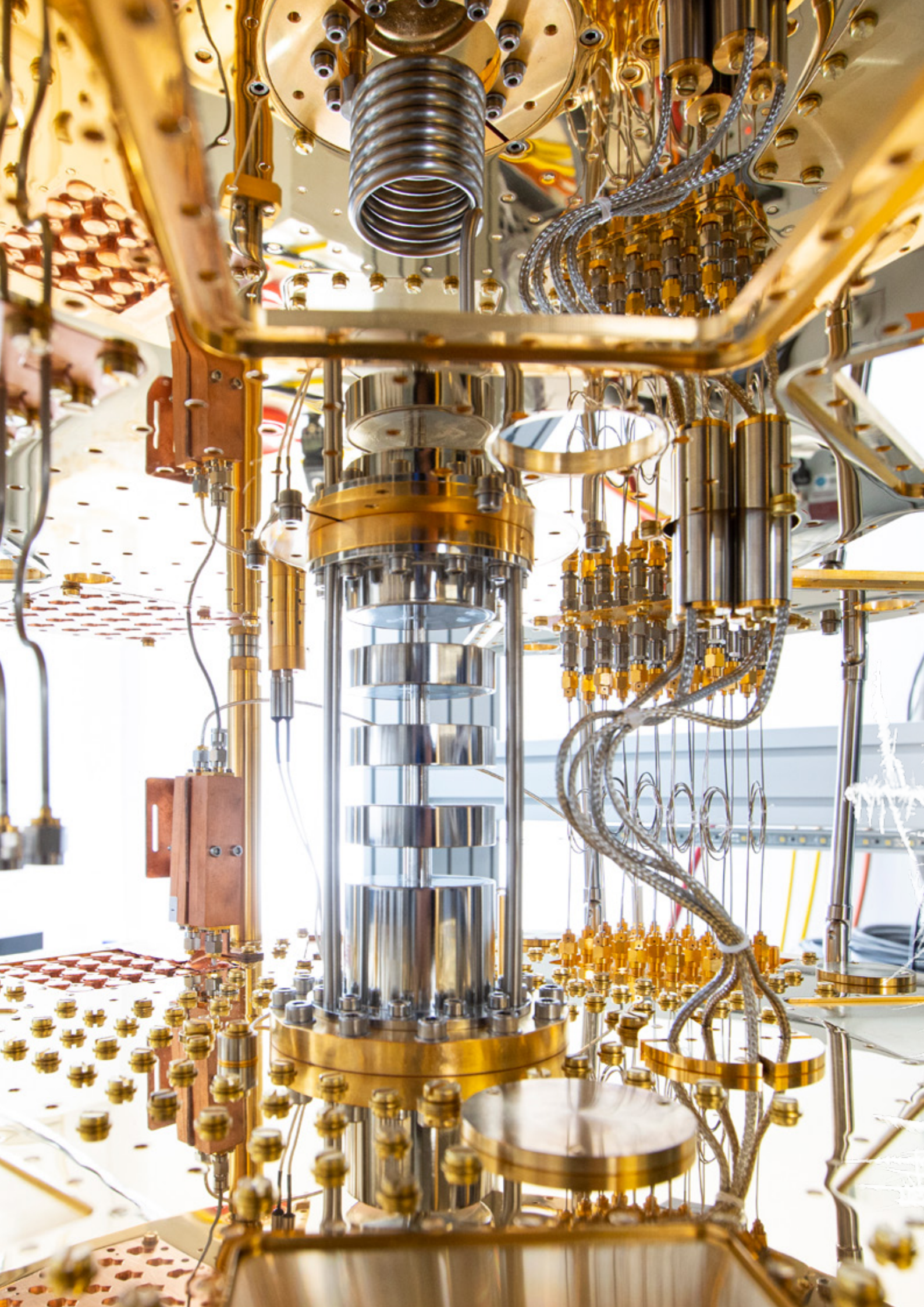
**Sparsam:** Kühlschranks mal anders

**Komfortabel:** Kühlkleidung im OP

#33

Nr. 2 | 2023







# RÄTSELHAFTE RECHENOPERATIONEN BEI EISESKÄLTE

*Quantencomputer gelten als revolutionär für die Informationstechnik. Auf dem Weg dorthin gibt es aber noch viele Forschungsfragen zu lösen.*

Nicht nur große Firmen arbeiten an der Entwicklung von Quantencomputern, auch Forschungseinrichtungen haben entsprechende Rechner in Betrieb genommen. Hier ist der Kryostat eines Quantencomputers zu sehen, der im Rahmen des europäischen Projekts „OpenSuperQ“ am Forschungszentrum Jülich aufgebaut wurde. Die Ruhr-Universität Bochum kooperiert mit dem Jülicher Team im neuen Quantum-computing-Netzwerk „EIN Quantum NRW“. (Foto: FZ Jülich / Sascha Kreklau)

**Q**uantencomputer – den Begriff liest man inzwischen häufiger. Und dazu sieht man Bilder von exotisch anmutenden hängenden Gebilden, in denen zahlreiche Leitungen mehrere goldene Etagen miteinander verbinden. Mit dem Aussehen klassischer Computer, die in jedem Haushalt stehen, haben sie nichts gemein. Und sie sind auch weit davon entfernt, in jedem Haushalt stehen zu können. Denn viele von ihnen benötigen spezielle Umgebungsbedingungen für den Betrieb: beispielsweise möglichst tiefe Temperaturen – nahe dem absoluten Nullpunkt.

„Das liegt daran, dass Quantenbits, die Speichereinheiten der Quantencomputer, sehr klein und deshalb auch sehr empfindlich sind“, erklärt Prof. Dr. Michael Walter, Leiter des Lehrstuhls für Quanteninformatik an der Ruhr-Universität Bochum. Je höher die Temperatur, desto mehr bewegen sich die Teilchen in einem Quantencomputer. Dieses mikroskopische Rauschen stört die Quantenbits.

Das Besondere: Anders als in klassischen Computern ist es sehr viel schwieriger, Information in Quantencomputern redundant zu speichern. Wird also ein einziges Quantenbit gestört, kann schnell Information verloren gehen. „Aktuelle Quantencomputer sind deshalb noch auf wenige tausend Rechenoperationen begrenzt“, weiß Michael Walter. Um die ▶

## **i FÜR DIE QUANTENINFORMATIKER\*INNEN VON MORGEN**

Quantencomputer – klingt interessant? Aber irgendwie auch rätselhaft? Dann ist Quantum Quest genau das Richtige: Auf der Onlineplattform [www.quantum-quest.de](http://www.quantum-quest.de) bietet der Lehrstuhl von Michael Walter zusammen mit Partnern von der Universität Amsterdam regelmäßig einen mehrwöchigen Onlinekurs an, bei dem sich Schülerinnen und Schüler auf die Suche nach den Geheimnissen des Quantumcomputings begeben können. Für das Programm im November 2023 haben sich 400 Interessierte angemeldet. Auch 2024 soll der Kurs wieder stattfinden. Das Kursmaterial ist ganzjährig online zu finden.



Systeme in die Anwendung zu bekommen, müssen sie also zunächst robuster werden. „Das Zauberwort lautet Fehlerkorrektur“, so Walter. Theoretisch ist das gut verstanden. Es wird aber noch einige Jahre Entwicklungsarbeit benötigen, das in die Realität umzusetzen.

Unabhängig vom aktuellen Hardware-Entwicklungsstand zielt Michael Walters Forschung darauf ab, zu ergründen, was die Existenz von stabil laufenden Quantencomputern bedeuten würde. Quantencomputer werden gängige Verschlüsselungsverfahren mühelos brechen können. Wie lässt sich sicherstellen, dass das nicht auch mit neuartigen Verschlüsselungsverfahren passiert? Wie können Quantencomputer helfen, für mehr Sicherheit zu sorgen? Wie lassen sich Quantendaten verschlüsseln? Walters Arbeit rund um IT-Sicherheitsfragen ist eingebettet in das Exzellenzcluster CASA – Cybersicherheit im Zeitalter großskaliger Angreifer.

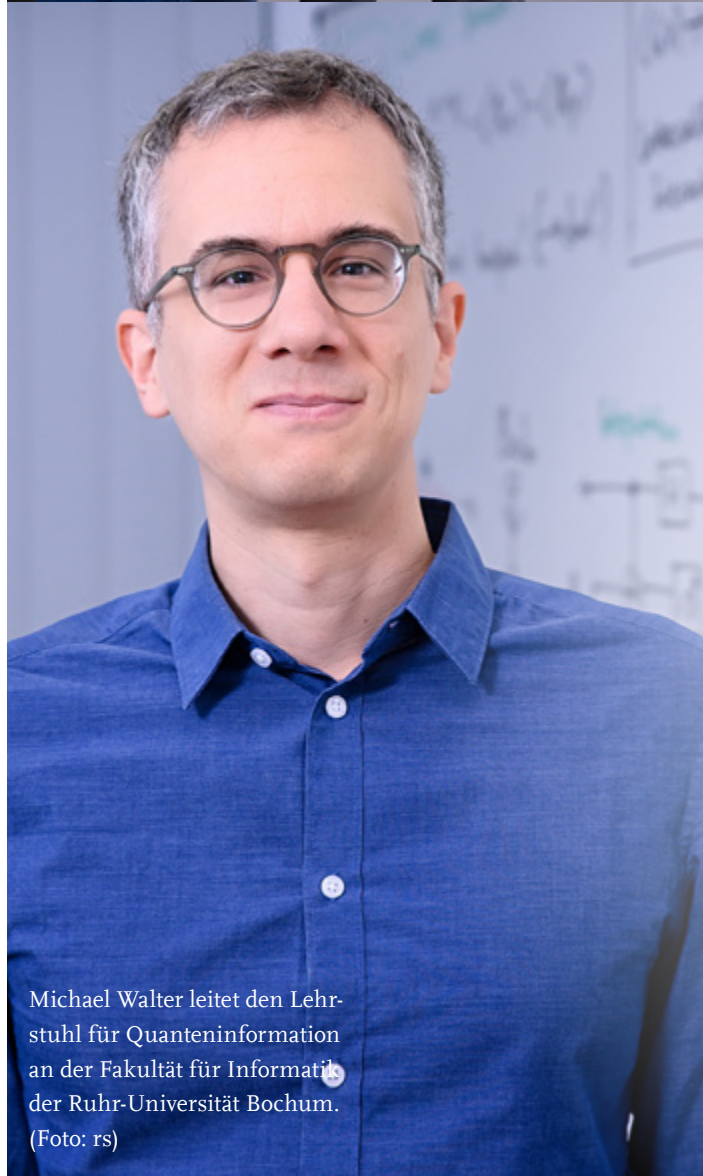
Eine Herausforderung, die den Informatiker besonders umtreibt, ist der Wunsch, mit Quantencomputern für mehr Sicherheit zu sorgen. Ein Problem heutiger Verschlüsselungstechniken ist, dass verschlüsselte Nachrichten prinzipiell abgefangen, gespeichert und in vielen Jahren mithilfe von Quantencomputern entschlüsselt werden könnten. Eine Verschlüsselung mit everlasting security hingegen würde sicherstellen, dass eine Information, die im Moment des Abfangens nicht geknackt werden kann, auch später nicht mehr entschlüsselt werden kann. Mit Quantenbits ist das möglich. Die Forschenden gehen dabei von folgendem Szenario aus: Alice will Bob eine geheime Information schicken. Das passiert in Form eines Quantenbits, kurz auch Qubit genannt. Eve versucht, dieses Qubit abzufangen, zu speichern und unbemerkt durch ein anderes Qubit auszutauschen – ein sogenannter Person-in-the-middle-Angriff.

Verhindern lässt sich dieser Angriff mit folgendem Trick: Alice schickt Bob ein Qubit, das mit einem anderen Qubit verschränkt ist. Verschränkung bedeutet, dass die beiden Qubits zwar räumlich voneinander getrennt sind, aber dennoch miteinander verbunden. Dadurch kennt das eine Qubit den Zustand des anderen. Versucht Eve also das versendete Qubit zu manipulieren, so können Alice und Bob diesen Eingriff feststellen. Die Idee für eine sichere Kommunikation basierend auf verschränkten Qubits ist nicht neu. „Bislang war allerdings nicht bekannt, wie viel Interaktion dafür wirklich notwendig ist“, erklärt Michael Walter. Zusammen mit CASA-Partnern entwickelte seine Gruppe ein neues Protokoll, das diese grundlegende Frage beantwortet.

Unabhängig von den IT-Sicherheitsaspekten interessiert sich das Team von Michael Walter für viele andere Fragen in der Quanteninformatik. Dabei wird er auch von einem prestigeträchtigen ERC Grant des Europäischen Forschungsrats unterstützt. Ein Fokus liegt dabei auf Algorithmen, mit denen Quantencomputer bestimmte Aufgaben schneller lösen können. Beispielsweise das sogenannte Erreichbarkeitsproblem. Ziel dabei ist, in einem Graphen einen Weg von A nach B zu finden. „Man kann es sich vorstellen wie die Suche nach einem Weg von einer Stadt zur anderen in einem komplexen Netz aus Straßen und Orten“, beschreibt der Informatiker.

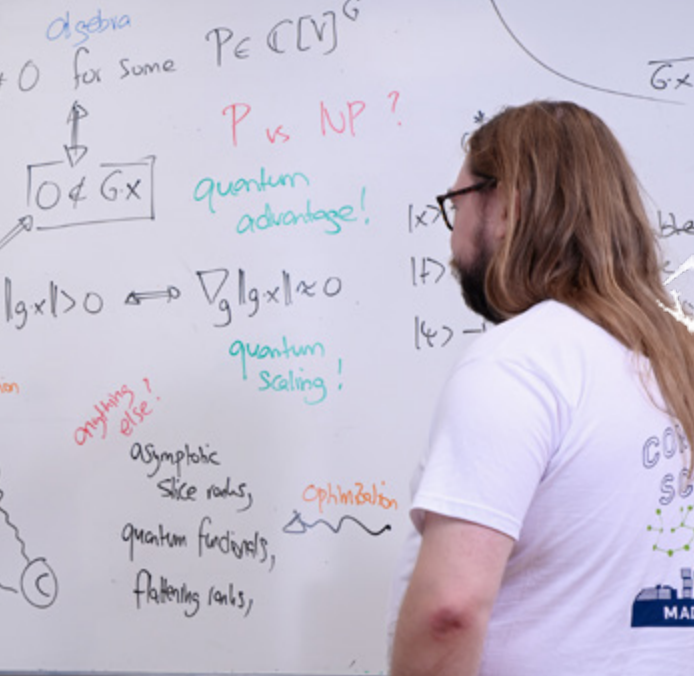


Was werden Quantencomputer alles leisten können? Einige Antworten auf diese Frage verbergen sich hinter Formeln wie diesen. Michael Walter entwickelt mit seinem Team Algorithmen, die später einmal auf Quantencomputern laufen könnten.  
(Foto: rs)



Michael Walter leitet den Lehrstuhl für Quanteninformation an der Fakultät für Informatik der Ruhr-Universität Bochum.  
(Foto: rs)





„Das Problem könnte man lösen, indem man versucht, sich einen Überblick über die Karte zu verschaffen. Dazu müsste man die gesamte Karte oder zumindest einen großen Teil speichern, sodass man den Weg von A nach B sehen kann.“

Ein alternativer Ansatz wäre, einen zufälligen Weg zu gehen. „Das wäre so, wie wenn eine betrunkene Person aus einer Bar kommt und versucht, nach Hause zu finden, indem sie an jeder Straßenecke eine zufällige Entscheidung trifft“, veranschaulicht Walter. „Das ist wenig zielgerichtet, funktioniert aber genauso, wenn auch langsamer. Der Vorteil: Der Algorithmus muss sich keinerlei Information merken, außer den Ort, an dem man sich gerade befindet.“ Diese Methode – auch random walk oder Zufallssuche genannt – klingt nicht intuitiv, aber: „Wir haben einen Random-Walk-Algorithmus für Quantencomputer gefunden, der das Problem viel schneller löst als die klassische Zufallssuche“, schildert Walter.

Während es bei klassischen Computern einen Wettstreit zwischen Speicherplatz und Geschwindigkeit gibt – wenig Speicher bedeutet zugleich langsam –, zeigt Walters Forschung, dass diese Einschränkung für Quantencomputer nicht gelten würde. Die Quanten-Zufallssuche braucht minimalen Speicherplatz und findet trotzdem schnell eine Lösung für das Erreichbarkeitsproblem. Aber: „Aufgrund der Natur der Quantencomputer würde der Algorithmus nur die Information ausgeben, dass es einen Weg von A nach B gibt, nicht aber den Weg selbst“, so Michael Walter. Denn in dem Moment, in dem man den Zustand der Qubits misst, um herauszufinden, welchen Weg der Algorithmus gerade nimmt, würde man den Quantenzustand zerstören und die Rechnung unterbrechen.

„Gerade wenn man einen neuen Algorithmus entwickelt, wäre es praktisch, in seine Arbeitsweise hineinschauen zu können“, bedauert Walter. „Andererseits ist es auch faszinierend, dass wir das Problem lösen können, ohne zu wissen, wie wir nun eigentlich ans Ziel gekommen sind“, sagt er.

Häufig liest man, dass Quantencomputer viel leistungsfähiger sein werden als klassische Computer, weil in ihnen vieles parallel geschieht. „So einfach ist das zum Glück nicht“, erklärt der Forscher. „In Quantencomputern passiert so einiges, aber sie rechnen nicht einfach parallel, sondern folgen völlig anderen Spielregeln als gewöhnliche Rechner.“ Die eigentliche Herausforderung sei es, aus den vielen Dingen, die gleichzeitig passieren, am Ende ein einziges Ergebnis zu erzeugen. „Man kann sich das wie ein Orchester vorstellen“ vergleicht Michael Walter. „Nur wenn alle Instrumente auf die richtige Weise zusammenwirken, entsteht wohlklingende Musik. Genauso es ist mit den Qubits in einem Quantenalgorithmus.“

Bis es Entwicklerinnen und Entwicklern gelingt, das Orchester richtig zu trainieren und die exotisch anmutenden goldenen Gebilde in Routinearbeiten einsteigen können, werden noch ein paar Jahre vergehen. Aber wenn es so weit ist und Quantencomputer etabliert sind, werden Michael Walter und sein Team schon einige Algorithmen bereithaben, die dem Orchester zu neuen Klängen verhelfen.

## SO FUNKTIONIERT EIN QUANTENCOMPUTER

Während klassische Computer auf Bits basieren, die die Zustände „0“ und „1“ annehmen können, basieren Quantencomputer auf Quantenbits. Diese können sich in Zuständen befinden, die eine Überlagerung von „0“ und „1“ sind, also mehrere Zustände gleichzeitig annehmen. Diese Überlagerung bricht jedoch zusammen, wenn man misst, in welchem Zustand sich ein Quantenbit befindet. Im Moment der Messung nimmt es entweder den Wert „0“ oder den Wert „1“ an, womit die Quantennatur zerstört wird.

„ES IST FASZINIEREND, DASS WIR DAS PROBLEM LÖSEN KÖNNEN, OHNE ZU WISSEN, WIE WIR NUN EIGENTLICH ANS ZIEL GEKOMMEN SIND.“

Michael Walter

# REDAKTIONSSCHLUSS



Fotos: RUB, Marquard

Festkörperphysik – das mag zunächst abstrakt klingen. Aber einige Phänomene, mit denen diese Disziplin arbeitet, lassen sich leicht erfahren, zum Beispiel der kalorische Effekt. Manche Materialien können durch eine bestimmte Behandlung Wärme oder Kälte erzeugen, etwa indem man sie in ein Magnetfeld einbringt oder indem man sie dehnt. Das lässt sich leicht mit einem Luftballon ausprobieren, der für das Experiment nicht aufgepustet sein sollte: 1) Den Ballon ruckartig auseinanderziehen. 2) Das gedehnte Gummi an die Lippen halten. Das Material hat sich erwärmt. 3) Den Ballon anschließend von den Lippen entfernen und – weiterhin gedehnt – ein paar Sekunden in die Luft halten, sodass das Gummi auf Umgebungstemperatur abkühlen kann. 4) Dann den Ballon zusammenschnappen lassen. 5) Jetzt schnell wieder an die Lippen halten. Der entspannte Ballon ist nun kälter als die Umgebungsluft. Wie man den kalorischen Effekt eines Tages für den Bau von Kühlschränken nutzen könnte, lesen Sie auf Seite 20.

## IMPRESSUM

**HERAUSGEBER:** Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

**WISSENSCHAFTLICHER BEIRAT:** Prof. Dr. Christian Albert (Geowissenschaft), Prof. Dr. Birgit Apitzsch (Sozialwissenschaft), Prof. Dr. Thomas Bauer (Fakultät für Wirtschaftswissenschaft), Prof. Dr. Gabriele Bellenberg (Philosophie und Erziehungswissenschaften), Prof. Dr. Maren Lorenz (Geschichtswissenschaften), Prof. Dr. Markus Kaltenborn (Jura), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Günther Meschke (Prorektor für Forschung und Transfer), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Nils Pohl (Elektro- und Informationstechnik), Prof. Dr. Markus Reichert (Sportwissenschaft), Prof. Dr. Tatjana Scheffler (Philologie), Prof. Dr. Gregor Schöner (Informatik), Prof. Dr. Sabine Seehagen (Psychologie), Prof. Dr. Roland Span (Maschinenbau), Prof. Dr. Martin Tegenthoff (Medizin), Prof. Dr. Marc Wichern (Bau- und Umweltingenieurwissenschaft), Prof. Dr. Peter Wick (Evangelische Theologie)

**REDAKTIONSANSCHRIFT:** Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

**REDAKTION:** Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Lisa Bischoff (lb); Raffaella Römer (rr)

**FOTOGRAFIE:** Damian Gorczany (dg), Schiefersburger Weg 105, 50739 Köln, Tel.: 0176 / 29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpfe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de

**COVER:** Roberto Schirdewahn

**BILDNACHWEISE INHALTSVERZEICHNIS:** Teaserfoto für Seite 16: Andreas Pflitsch, Seite 20: Damian Gorczany, Seite 32: Jennifer Herzog-Niescery, Seite 40: Roberto Schirdewahn, Seite 50: Katja Marquard

**GRAFIK, ILLUSTRATION, LAYOUT UND SATZ:** Agentur für Markenkommunikation, Ruhr-Universität Bochum, www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

**DRUCK:** LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, info@ld-medienhaus.de, www.ld-medienhaus.de

**ANZEIGEN:** Dr. Julia Weiler, Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de

**AUFLAGE:** 3.900

**BEZUG:** Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin/abo. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden.

**ISSN:** 0942-6639

Nachdruck bei Quellenangabe und Zusenden von Belegexemplaren

Die nächste Ausgabe von RUBIN erscheint am 3. Juni 2024.