DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

DIGITALE WELT

SCIENCE MEETS INDUSTRY

Ausgabe 4 ▪ Oktober ▪ November ▪ Dezember ▪ **2021**

Quantum Applications

Wie schon jetzt erste Anwendungsfelder entstehen

Finanzwirtschaft

Wie Qubits bei der Portfolieoptimierung helfen können

Kommunikation

Wie sich die Industrie auf das Zeitalter der Post-Quantum-Cryptography einstellt

Chemie

Wie die Pharmaforschung mit Quanten-computern Medikamente entwickeln will

QUANTENBITS

Die Grundlagen einfach erklärt

Der Healthcare Experte von Merck über das Potenzial des Quantencomputings

Dr. Thomas Ehmer

Quantum Applications

Dr. Sebastian Feld

Von Schaltkreisen zu Quantum Services

Vielleicht hat alles im Mai 1981 begonnen, als Richard Feynman in einem Plenarvortrag die Frage gestellt hat, ob Quantenphysik effizient von klassischen Computern simuliert werden kann. Die Antwort lautet schlichtweg: nein. Es musste also eine andere Lösung her. In kurzer Folge wurden entsprechende Formalisierungen vorgestellt, nämlich das quantenmechanische Modell einer Turingmaschine (Paul Benioff, 1982) als Analogon einer klassischen Rechenmaschine oder sogenannte Quantengatter (David Deutsch, 1985), das Pendant zur klassischen Binärlogik. Im Grunde war somit ein theoretischer Quantencomputer konzipiert. Es stellte sich nun jedoch eine weitere Frage: Mit welchen Anweisungen kann dieser theoretische Quantencomputer welche Aufgaben schneller oder besser als ein klassischer Computer lösen? Es dauerte einige Jahre, bis Algorithmen gefunden wurden, die bewiesenermaßen schneller als ihre entsprechenden klassischen Verfahren sind. So hat Lov Grover 1996 einen Weg gefunden, um eine unsortierte Datenbank schnell zu durchsuchen, und Peter Shor gelang es 1997 ein Verfahren zu beschreiben, mit welchem eine zusammengesetzte Zahl effizient in ihre Teiler zerlegt werden kann. Von diesen theoretischen Errungenschaften getrieben kam auch der experimentelle Drang auf zu überprüfen, ob solch eine Maschine tatsächlich gebaut und besagte Algorithmen praktisch ausgeführt werden können. Und es war tatsächlich möglich: 2001 haben experimentelle Physiker, Ingenieure und viele weitere kluge Köpfe eine Maschine gebaut, die in der Lage war, Shors Algorithmus auszuführen. Die Wissenschaftler haben die Zahl 15 in ihre Primfaktoren 3 und 5 zerlegt.

Diese scheinbar einfache Rechnung (3x5=15) war wissenschaftlich gesehen jedoch ein unbeschreiblich großer Schritt. Hiermit wurde bewiesen, dass Shors theoretische Versprechung auch praktisch umgesetzt werden kann. Denn mal ehrlich: Was nutzt einem ein theoretischer Bauplan einer Zeitmaschine, wenn diese nicht praktisch gebaut werden kann. Es folgten zahlreiche Durchbrüche in Sachen Ingenieurskunst, die der allgemeinen Öffentlichkeit eher verborgen geblieben sind. Der Bau eines funktionierenden Quantencomputers verlangt enormes theoretisches und praktisches Können aus vielen unterschiedlichen Disziplinen. Und genau dieses Wissen und diese Erfahrungen wurden in den darauffolgenden Jahren angehäuft und erprobt, sodass wir in den letzten etwa 5 Jahren zahlreiche Erfolge im Bereich der Hardware-Entwicklung beobachten konnten. Anscheinend haben die Ergebnisse die Labore der Universitäten verlassen und Einzug in die F&E-Abteilungen der globalen Unternehmen genommen. Verschiedene Akteure aus Wirtschaft und Wissenschaft forschen nun an sehr unterschiedlichen technischen Kandidaten zur Realisierung von Qubits, dem essentiellen Grundbaustein eines jeden Quantencomputers. Und all diese Kandidaten besitzen ihre eigenen Vorteile, Unzulänglichkeiten und entsprechend auch „Technology Readiness Levels“.

Nachdem nun erfolgreich daran gearbeitet wird, die Hardware (d.h. den Quantencomputer) aus der Theorie in die Praxis zu bringen, muss dies ebenso auch für die Software (d.h. die Algorithmen) geschehen. Oder anders ausgedrückt: Wir besitzen eine ausgereifte Idee von Quantencomputing, bewiesene theoretische Formalisierungen und erste praktische Realisierungen der Technik, und nun gilt es, die „PS auf die Straße zu bringen“ und Quantencomputer tatsächlich praktisch einzusetzen. Dies fühlt sich allerdings wie eine Art Zeitreise an. Es existiert Erfahrung aus Jahrzehnten professioneller Softwareentwicklung mit Design Patterns, Best Practices und dergleichen. Es offenbart sich jedoch, dass wir vieles des bereits Bekannten erneut erlernen müssen. Mit Sicherheit werden wir einige Techniken und Ideen der klassischen Softwareentwicklung auch im Quantencomputing verwenden können (bspw. Code-Reusability), anderes scheint jedoch viel schwerer zu sein (bspw. Fehlerkorrektur) oder gar nicht möglich (Inspektion von Variablen). Sprich: Wir müssen lernen, neu zu denken.

Wenn wir nun eine Zeitreise getan haben, wo befinden wir uns dann? Aktuell scheinen wir das Ende der Phase „Kernel-Entwicklung“ zu erreichen. Bislang haben wir uns mit einer 1-zu-1-Beziehung von Lösung zu Problem befasst, es wurden starre Schaltkreise entwickelt, die genau ein spezifiziertes Problem lösen. Diese Vorgehensweise ist vergleichbar mit der Programmierung mittels Lochkarten bis in die 1960er-Jahre hinein. Die nächste Phase, die nun zaghaft beschritten wird, ist wohl die „Algorithmus-Entwicklung“. Im Fokus stehen also nicht mehr kleine Mengen von Quantengattern, die als Einheit (Kernel) angesehen werden, sondern vielmehr Module. Es geht vorrangig um eine Wiederverwendbarkeit von Code, welche jedoch immer noch stark an der zugrunde liegenden Technik angelehnt ist und entsprechendes Wissen um die Quantenphysik erfordert. Aus Sicht der Software ist schließlich das Ziel, die Phase der „Modell-Entwicklung“ zu erreichen. Diese ähnelt der vorherigen Phase, ist jedoch weiter abstrahiert: Der Fokus entfernt sich gänzlich von Details der Quantenphysik und beinhaltet nun weitaus stärker notwendiges domänenspezifischen Wissen (bspw. aus den Bereichen Chemie, Finanzen oder Logistik) mit dem Ziel, mächtige Bibliotheken anzubieten.

Auf die eben beschriebenen Phasen aufbauend wird nun die Software- und Informatik-Sicht etwas verlassen und eine eher wirtschaftliche Betonung gesetzt. So werden zukünftig die Phasen der „Quantum Applications“ und „Quantum Services“ folgen. Es sollen Anwendungen erschaffen werden, die einen messbaren Wert schöpfen und darüber hinaus mit den Begebenheiten der Unternehmen skalieren. Die Wertschöpfung kann einerseits innerhalb des Unternehmens stattfinden (Quantum Applications im Sinne einer Prozessoptimierung) und andererseits außerhalb des Unternehmens (Quantum Service als Dienstleistung und Wirtschaftsgut). Je weiter wir uns allerdings von den technischen Details entfernen, desto öfter scheint Verwirrung in der Diskussion des Für und Wider von Quantencomputing aufzutauchen. Es gilt wie so oft: Nicht jedes Werkzeug passt zu jeder Fragestellung. Grundsätzlich existieren leichte und schwere Problemstellungen, und zwar sowohl für klassische Computer als auch für Quantencomputer. Es ist jedoch nicht der Fall, dass ein Problem, das für klassische Computer schwer ist, automatisch einfach für einen Quantencomputer ist. Domänenexperten aus Wirtschaft und Wissenschaft sollten also frühzeitig mit einer sorgfältigen Analyse der „Kosten und Nutzen“ beginnen. Damit ist folgende Frage gemeint: Gegeben ist die ganz spezielle Problemdomäne eines Unternehmens. Welchen Business Value würde die Problemlösung bieten (Nutzen) und wo liegt der erwartete Zeitpunkt eines entsprechenden Quantenvorteils (Kosten)? Sie erinnern sich: Ein vorteilhafter Algorithmus, der zwar in der Theorie existiert (siehe Primfaktorzerlegung), muss erst noch praktisch realisiert werden können (15=3x5). Leider ist die Beantwortung der soeben gestellten Frage, nämlich welches Problem wann mit welchem Vorteil gelöst werden kann, schwierig. Aber: Sie lohnt sich!

Lassen Sie uns in diesem Heft also eben dieser Frage nachgehen und schauen, wie wir vorteilbringende Quantum Applications entwickeln können und vielleicht auch wann wir diese nutzen können. Ich wünsche Ihnen viel Spaß bei der Lektüre!

Dr. Sebastian Feld lehrt und forscht als Assistant Professor im Bereich Quantum Machine Learning an der TU Delft und ist außerdem Mitgründer des Quantum Applications and Research Laboratory (QAR-Lab) der LMU München.

8
DR. THOMAS EHMER
„Der Scheidepunkt zwischen klassischem und Quantencomputing ist schon da."

14
QUANTUM APPLICATIONS
Wie schon jetzt neue Anwendungsfelder entstehen

12 DR. NORBERT GAUS
Quantencomputer auch in Deutschland – Nicht der Rechner zählt, sondern die Anwendungen

Cover: BAIVECTOR/Shutterstock, Merck Fotos: BAIVECTOR/Shutterstock, Merck, Enno Kapitza

LESEN SIE ONLINE MEHR

Fachbeiträge
Kolumnen
Blogs

Die nächste DIGITALE WELT erscheint am 01.12.2021

QAR LAB

QUANTUM APPLICATIONS & RESEARCH LABORATORY

Das QAR-Lab

Das Quantum Applications and Research Laboratory (kurz QAR-Lab) – im Jahr 2016 von der Informatik-Professorin Dr. Claudia Linnhoff-Popien der LMU München gegründet – hat die Mission, die Technologie des Quantencomputings (QC) einem breiten Nutzerkreis in Forschung und Wirtschaft zugänglich zu machen. Bereits 2019 wurde das QAR-Lab im Ranking als eine der „World's Top 12" Forschungseinrichtungen auf dem Gebiet des Quantencomputings durch „The Quantum Daily" international bekannt.

Unsere Schwerpunkte

Als Gründungsmitglied des europaweit einzigartigen Leuchtturmprojekts PlanQK („Plattform und Ökosystem für quantenunterstützte KI") leistet das Lab Pionierarbeit dabei, die Quantencomputing-Technologie auf dem Gebiet der Künstlichen Intelligenz zu nutzen.

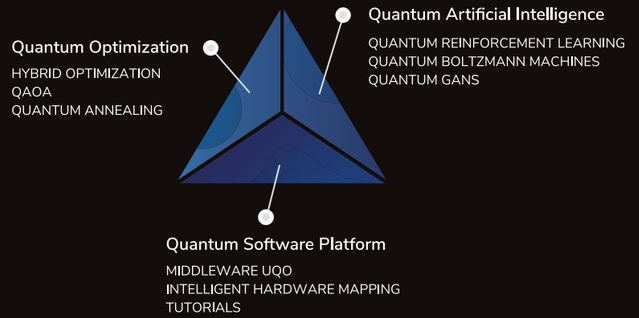
Das QAR-Lab hat – in Deutschland einzigartig – Zugang zu vier unterschiedlichen Quantencomputern und kann daher vergleichende Bewertung geeigneter Algorithmen durchführen.

Die Experten des QAR-Labs beschäftigen sich neben der Grundlagenforschung mit der Nutzung der Technologie für praxisnahe Anwendungen. Sie setzen auf Pilotprojekte für neue Technologien im Bereich QC und arbeiten an der Umsetzung von quantenunterstützten KI-Algorithmen für industrielle Use Cases im Rahmen von Forschungskooperationen mit großen Industriepartnern, die die Technologie erproben wollen.

Das QAR-Lab der LMU baut ein bayerisches Ökosystem für Anwenderkompetenz auf und stärkt den Standort München auf der deutschen Quantencomputing-Landkarte.

Finanziell gefördert wird das Lab seit 2019 vom Bundesministerium für Wirtschaft und Energie (BMWi) und seit 2020 vom Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi).

Unsere Forschungsschwerpunkte



BECOME QUANTUM READY!

Kooperationsmöglichkeit mit dem QAR-Lab

Nutzen Sie die Expertise des QAR-Labs, um sich im internationalen Wettbewerb rechtzeitig Wissen über Quantencomputing anzueignen. In einer Kooperation mit dem QAR-Lab werden Sie von Anfang an kompetent unterstützt. Wir gehen mit Ihnen die ersten Schritte oder begleiten Sie den ganzen Weg.
Unsere Experten wissen, welche Quantenhardware für welche Herausforderungen in einem Betrieb am geeignetsten sind.

Unser Ziel

Schwere Anwendungsfälle
Die Lösung mit heutigen Techniken braucht viel Rechenzeit oder geht gar nicht.

Wichtige Anwendungsfälle
Eine bessere/ schnellere Lösung hat einen großen Effekt, bspw. bei der Einsparung von Kosten oder der Verbesserung der Organisation.

Passende Anwendungsfälle
Es gibt ein (prospektives) Lösungsverfahren incl. QC-HW, das einen Vorteil bringt.

Frühe Anwendungsfälle
Eine QC-basierte Lösung ist relativ bald (schon mit NISQ?) umsetzbar.

Kontaktieren Sie uns: www.qar-lab.de

Prof. Dr. Claudia Linnhoff-Popien
Leitung QAR-Lab
Ludwig-Maximilians-Universität München
Oettingenstraße 67
80538 München
Telefon: +49 89 2180-9153
E-Mail: qar-lab@mobile.ifi.lmu.de

ALLES AGIL UND GLEICHZEITIG ENTSPANNT UND GESUND?

Wie Botschafter und Lotsen den Weg zur mentalen Stärke weisen.

Unsere Teammeetings beginnen seit einigen Wochen mit kurzen mentalen Übungen. Mal ist es ein mentales Entspannungsbild, mal eine Koordinationsübung, mal eine Atem-Technik, je nachdem ob wir Gelassenheit, Kreativität oder Stress-Abbau fördern möchten. Anschließend geht es ritualisiert immer erst um Erledigtes und dann um offene To-dos oder Themen." So der Bericht eines Teamleiters eines High-Tech-Unternehmens. „Diese Rituale wurden anfangs mit Skepsis betrachtet. ‚Zeitverschwendung' oder ‚Esotherik-Quatsch' waren häufige Reaktionen zu Beginn. Letztlich war es wohl eine meiner Kolleginnen, die sich zum Mental Health Ambassador qualifizierte. Sie hat das Thema mentale Gesundheit aufgenommen. Sie stellte sich mit ihrer neuen zusätzlichen Funktion im Team vor, informierte kurz und knapp über verschiedene nützliche Rituale zur psychischen Stabilität und lud zum Ausprobieren ein. Die Skepsis der Kolleg*innen schwand und inzwischen ist dieser Ablauf gut etabliert." Ein Beispiel, wie Unternehmen von Mental Health Ambassadors profitieren können.

In Unternehmen gibt es „Ersthelfer" bei körperlichen Beschwerden und Verletzungen, aber wie sieht es bei der psychischen Gesundheit aus? Psychische Gesundheit wird durch kleine Rituale im Alltag erhalten. Fallen diese weg, weil „keine Zeit ist" oder weil sie als nicht wichtig angesehen werden, ist das Risiko der Überlastung groß. Aufwand und Mühe, um von einer Überlastung wieder in eine positive Balance zu kommen, sind im Vergleich zu den präventiven Maßnahmen riesig.

Kolleg*innen, die als Botschafter für mentale Stärke im Unternehmen fungieren, haben die große Chance, immer wieder die Fahne für die Integration dieser präventiven Techniken zu schwenken. Mit deren Hilfe ist eine Veränderung der Unternehmenskultur leichter möglich. Wenn jetzt immerzu über agiles Arbeiten gesprochen wird und man auch versucht, dieses im Alltag zu leben, brauchen wir gleichzeitig eine persönliche Basis von Wohlbefinden und dem Wissen darum, wie wir es für uns immer wieder herstellen können. Deshalb erfahren Mental Health Ambassadors u.a.:

- Wie kann ich Achtsamkeitsrituale in meinen Tagesablauf integrieren und diese als Ambassador in den Unternehmensalltag effektiv einführen?
- Welche persönlichen Rituale für mehr Selbstwirksamkeit kann ich für mich nutzen? Welche Rituale und Techniken gibt es und wie kann ich diese in den Alltag von Teams integrieren?
- Wie kann ich für mich in besonderen Situationen sicherer werden und wie kann ich diese mentalen Techniken auch für meine Kolleg*innen bereitstellen?
- Sie kennen hilfreiche Angebote für mentale Stärke und wissen welche Expert*innen in schwierigen Situationen unterstützen können?

Wer Lust hat, kann diese Qualifizierung ausbauen zum Mental Health Navigator. Sie übernehmen folgende Aufgaben:

Präventiv mentale Stärke fördern: Mental Health Navigators gehen aktiv auf Führungskräfte zu, unterstützen eine Kultur, in der mentale Stärke thematisiert und Tabus nach und nach abgebaut werden. Sie bieten informelle Treffen an, in denen Kolleg*innen die Chance zum Austausch in kritischen Situationen haben oder Anforderungen an mentale Stärke diskutiert werden.

Kolleg*innen vor Überbelastung schützen: Mögliche Signale von Überbelastung zu erkennen und dann zu wissen, was zu tun ist, liegt auch in der Verantwortung von Mental Health Navigators. Sie wissen, wie sie betroffene Kolleg*innen angemessen ansprechen, und können in Abstimmung mit der Personalbetreuung ggf. an Expert*innen weitervermitteln.

Systeme des Unternehmens nutzen: Mental Health Navigators kennen hilfreiche Angebote für mentale Stärke, verstehen, wie eine Gefährdungsbeurteilung psychischer Belastung genutzt werden kann, bringen mentale Stärke immer wieder ins Gespräch z.B. mit Tipps in internen News.

Außerhalb der Verantwortung der Ersthelfer für psychische Gesundheit liegt das Stellen von Diagnosen, therapeutische Tätigkeiten sowie das Geben von Tipps und Ratschlägen. Sie sind Ansprechpartner, Botschafter und Lotsen in einer sich veränderten Kultur, in der körperliche und psychische Gesundheit systemrelevant ist. Ein Wandel, den unsere Arbeitswelt dringend braucht.

Habe ich Sie neugierig gemacht? Wenn Sie Lust haben, schreiben Sie mir. Herzlichst Ihre
**Dr. Petra Bernatzeder,
Diplom-Psychologin, Coach,
Expertin für mentale Intelligenz,
www.upgrade-hr.com**

Foto Privat

„Der Scheidepunkt zwischen klassischem und Quantencomputing ist schon da.“

Ein Gespräch mit Dr. Thomas Ehmer

Die Forschungsergebnisse und erste praktische Anwendungsmodelle haben gezeigt, dass Quantencomputing vielversprechende Ansätze liefert und zum Gamechanger in Industrie und Wirtschaft werden kann. Der Vorteil der neuen Technologie liegt in ihrer enormen Leistungsfähigkeit, die klassisches Computing auf kurz oder lang übertrumpfen wird. Für Dr. Thomas Ehmer, Innovation Incubator im IT Healthcare R&D Informatics Team der Merck KGaA, ist der Scheidepunkt schon eingetreten. Den optimalen Zeitpunkt, um auf Quantencomputing zu setzen, gäbe es eh nie, dennoch müsse man sich jetzt offen der neuen Technologie gegenüberstellen, um den Sprung nicht zu verpassen.

Quantencomputing ist längst in aller Munde. Durch die enorme Leistungsfähigkeit von Quantenrechnern verspricht man sich den viel zitierten Begriff der „Quantum Supremacy“. Was halten Sie von dieser proklamierten Quantenüberlegenheit? Welche Vorteile verbergen sich hinter diesem Ausruf?

Der Begriff „supremacy“ bzw. „Überlegenheit“ ist etwas unglücklich gewählt, hat aber allerdings auch für Aufsehen gesorgt. Die Community benutzt lieber den etwas weniger radikalen Begriff „advantage“ – also etwa Quantenvorteil. Die Hoffnung hinter diesem Ausdruck liegt darin, dass ein Quantencomputer Dinge tun kann, die ein konventioneller Rechner entweder prinzipiell nicht – oder nur in nicht wirtschaftlichem Maße – tun kann. Prominente Beispiele sind z.B. das Random circuit sampling von Google oder das Boson-Sampling aus dem Experiment der University of Science and Technology in Hefei/China. Dazu muss man wissen, dass diese Experimente sehr wertvoll für die Grundlagenforschung sind und für das grundlegende Verständnis, woher eine „quantum supremacy“ überhaupt kommen könnte. Diese Art Experimente helfen zu verstehen, was denn die Besonderheiten der Quantenmechanik sind, die eine Rolle spielen bei der Berechnung von Aufgaben, und wie diese genutzt werden könnten. Allerdings sind diese Experimente auch genau so konstruiert, eine „supremacy“ zu zeigen, d.h. sie bearbeiten spezielle Fragen, die besonders gut „mit Quantum“ und besonders schlecht „ohne Quantum“ zu lösen sind. Man tut sich dann teilweise doch schwer, tatsächlich praktische Relevanz für solche Fälle zu finden. In der Tat ist es so, dass es nur eine Handvoll Problemstellungen gibt, bei denen spezielle Algorithmen ganz spezielle Problemklassen besser lösen als klassische Computer. Das wohl meistzitierte Anwendungsgebiet ist die Primzahl-Faktorisierung mit dem Shor-Algorithmus, der allerdings selbst auch nur mit einem Teilstück des gesamten Algorithmus einen Quantenvorteil nutzt, indem er nämlich sehr clever Interferenzen ausnutzt, um bei der Fouriertransformation eine spezielle Frequenz zu finden, die dann später auf ein Ergebnis hinweist.

„Der Vorteil hinter dem Ausruf des ‚Quantum Advantage‘ ist in der Tat der, dass wir jetzt anfangen, über Benchmarks zu sprechen, und in der Lage sein werden, Probleme zu klassifizieren.“

Der Vorteil hinter dem Ausruf des „Quantum Advantage“ ist in der Tat der, dass wir jetzt anfangen, über Benchmarks zu sprechen, und in der Lage sein werden, Probleme zu klassifizieren, bei denen wir uns überhaupt Hoffnung machen können, dass deren Lösung von einem Quantum-speedup profitieren kann. Und dann so stark, dass tatsächlich ein „advantage“ vorliegt, der ja zusätzlich noch die Nachteile wie z.B. langsame Dateneingabe und Datenausgabe, mehrfache Berechnung und so weiter beim Quantencomputer kompensiert. Man darf ja nicht vergessen, dass wir hier beim Quantencomputing von einem speziellen Co-Prozessor sprechen, der eben einige Aufgaben besonders gut kann. Inwieweit das dann besser ist als alle anderen Rechenmethoden und Konzepte (sei es klassisch digital, neuromorphisch, sonst unkonventionell oder analog über z.B. Nutzung von Pilzwachstum oder Oberflächenspannung …), ist das Spannende an der ganzen Sache – Diversität ist auch hier absolut unabdingbar.

Stehen wir aktuell also am Scheidepunkt zwischen klassischem Computer und Quantencomputing? Ist eine vollständige Ablösung des herkömmlichen Computers ein realistisches Szenario für die nächsten Jahre?

Ein Scheidepunkt ist schon da, ja, und zwar insofern, dass es bestimmte Problemklassen gibt, die sich für Quantencomputer oder zumindest Computer mit Quanten Co-Prozessoren anbieten. Es gibt einige Hinweise, dass auch die Art des Quantencomputing teilweise bestimmt, welche Probleme auf welchem Typ besser laufen. Es gibt ja (mindestens) zwei fundamental unterschiedliche Ansätze: einmal das Gate Computing, wo vereinfacht gesprochen einzelne Qubits gezielt schrittweise manipuliert werden, und dann das sogenannte Adiabatische Quantum Computing (oder Annealing), bei dem alle Qubits eine zeitliche Änderung durchlaufen, um dann gemeinsam einen optimalen Endzustand zu erreichen. Die Methoden sind beide universell, nutzen aber komplett unterschiedliche Herangehensweisen und Quantenphänomene aus. Gerade bei Letzterem (adiabatisch) zeigt sich zum Beispiel, dass es nicht so sehr auf eine Verdrängung, sondern eher auf eine Synergie – sogenannte hybride Systeme – hinauslaufen wird.

Eine vollständige Ablösung des herkömmlichen Computers wird definitiv nicht allein durch Quantum Computing und nicht in den nächsten Jahren kommen. – Es gibt viele Dinge, die ein klassischer Computer aus Prinzip besser kann als ein Quantencomputer, z.B. die Grundrechenarten und das Speichern digitaler Daten.

Quantencomputing allein ist ein Rohdiamant, der erst geschliffen werden muss. Um den Nutzen dieser neuen Technologie besser einzuordnen, kommt es stark auf die möglichen Anwendungen an. In welchen Bereichen sehen Sie Anwendungsmöglichkeiten von Quantencomputing?

Im Rahmen von QUTAC, dem deutschen Industrie Quantum Computing Anwender Konsortium, untersuchen wir die drei folgenden Problem-Klassen: Simulation, Machine Learning und Optimierungsprobleme. Bevor es allerdings zur Anwendung kommen kann, kommt ein Punkt ins Spiel, der mir auch persönlich sehr am Herzen liegt. Man benötigt nämlich nicht nur Mut und Neugier, bekannte Themen überhaupt neu zu betrachten, sondern auch das notwendige Grundverständnis von Quantenmechanik und ein Gefühl für deren Besonderheiten bzw. „features“. Das ist deswegen notwendig, weil die Quantenmechanik der klassischen Alltagslogik widerspricht. Um also überhaupt in der Lage zu sein, ein Problem komplett neu „Quantum-kompatibel“ zu betrachten, braucht man „Quantum Intuition“. Wir haben seit etwa einem Jahr den Begriff „Quantum Literacy“, der die Fähigkeit beschreibt zu verstehen, was denn die Eigenart von Quantenmechanik ist und wie diese – idealerweise spielerisch – genutzt werden kann, um komplett neue Herangehensweisen an „alte harte Nüsse“ zu finden und auszuprobieren. Das ist ein wesentlicher Grundstein, und je früher man damit anfängt, die Phänomene der Quantenmechanik aufzuzeigen bzw. zu erklären, desto spielerischer und leichter tut man sich dann später, damit unkonventionelle Algorithmen zu finden. Es spricht nichts dagegen, die Fundamente der Quantenmechanik bereits in der Grundschule zu lehren, wenn man die Methode richtig wählt und sich nicht hinter der Mathematik versteckt, sondern die Faszination der „Eigenarten“ wie Verschränkung, Interferenz und Nichtlokalität als gegeben hinnimmt und sie benutzt, anstelle zu versuchen, sie bis zum Studium wegzudiskutieren und dann wieder mühsam einzuführen. Dort könnte man dann auch jeweils die Stärken und Schwächen der über fünfzehn verschiedenen philosophischen Interpretationen der Quantenmechanik behandeln. – Man darf die Kreativität und Neugier von niemandem jemals unterfordern.

„Das Ganze ist also ein Tanz der Methoden und Werkzeuge, der choreografiert werden will.“

Quantenchemie dient in verschiedenen Bereichen dazu, Eigenschaften von Molekülen und Materialien präzise vorherzusagen. Für den konkreten Nutzen davon ist ein Paradigmenwechsel vonnöten. Was heißt das genau?

Computer-Quantenchemie wird ja schon seit längerer Zeit erfolgreich auf „klassischer“ Architektur gemacht. Wir haben im Unternehmen mehrere Projekte, die z.B. in einer Einheit rund um Dr. Philipp Harbach bearbeitet werden. Er hat auch eine sehr schöne Erklärung veröffentlicht, die das besser beschreibt, als ich es könnte.

Ich versuche es hier in meinen Worten zusammenzufassen: Die relevanten Probleme sind sehr komplex, und man muss dann bei der Berechnung vereinfachte Modelle nutzen und Kompromisse finden zwischen Präzision z.B. des energetischen Grundzustands eines Moleküls und der Dauer, die benötigt wird, diesen zu berechnen.

Wie schon angedeutet gibt es bestimmte Eigenarten in der Quantenmechanik, die man generell versucht auszunutzen, entweder direkt oder indirekt. Derzeit sprechen wir viel vom indirekten Weg, nämlich ein Quantensystem mit zwei Zuständen als Qubit zu benutzen und dann mit den Qubits zu rechnen – in der Hoffnung, mathematisch sehr aufwendige Fragestellungen viel eleganter zu lösen. Im Prinzip geht es beim Quantencomputing immer darum, einen Algorithmus zu finden, der dann Interferenzen der Zustände ausnutzt. Je mehr verschränkte Qubits man hat, desto mächtiger der Erfolg. Andererseits kann man das Quantensystem natürlich auch direkt nutzen, um Quantenprobleme direkt zu „berechnen“ und dann zu messen – also mit einem Quantensystem ein anderes Quantensystem zu simulieren. Das wäre dann z.B. „measurement based“ und ist derzeit ein heißes Thema in der Grundlagenforschung.

Im Prinzip geht es in der Quantenchemie darum, sowohl die Eigenschaften von Materialien auf atomarer Ebene zu berechnen als auch die Wechselwirkung untereinander und mit anderen Materialien. Dort spielen dann aber wieder weitere – auch nicht quantenmechanische – Effekte eine Rolle, die sich klassisch besser lösen lassen als mit Quantencomputern. Das Ganze ist also ein Tanz der Methoden und Werkzeuge, der choreografiert werden will.

Welche Optimierungslösungen erwarten Sie sich vom Quantencomputing?

Gerade in letzter Zeit gab es mehrere Berichte auf Konferenzen über Fortschritte im Adiabatischen Quantum Computing (oder Annealing), die es auch in die Presse geschafft haben, wie z.B. das Taxi-routing in Barcelona von VW, oder auch Fachartikel wie etwa spezifische Rechnungen zur mRNA-Codon-Optimierung von unseren Kollegen von GSK. Viele der Optimierungslösungen fallen daher in die Klasse der sogenannten QUBO (quadratic binary optimization), also Fragestellungen, die sich so formulieren lassen, dass man Probleme mit vielen Variablen und mehreren gleichzeitig zu erfüllenden Randbedingungen so formulieren kann, dass man eine Reihe von quadratischen Gleichungen aufstellen kann, die das Problem beschreiben, worauf man dann ein Minimum des Gleichungssystems sucht. Das hört sich meist trivial an, ist aber aufgrund der hohen Kombinatorik in der Tat klassisch nur sehr schwer und aufwendig lösbar. Meist sind das Probleme aus der Logistik, wo irgendwo ein oder mehrere Engpässe bestehen, z.B. optimale Auslastung von Maschinen bei minimaler Umrüstzeit oder Versorgung mit kritischen Ressourcen. Derzeit herrscht immer noch eine Diskussion der unterschiedlichen Quantum-Computing-Paradigma-Lager in der Interpretati-

on, ob das Annealing jetzt „echtes“ Quantencomputing ist oder nicht, und ob es tatsächlich „speed-up“ gibt oder nicht. Eine interessante vergleichende Studie zwischen „Gate“ und Annealing für unterschiedliche Problem-Klassen wird derzeit übrigens gerade an der LMU unter Leitung von Frau Prof. Linnhoff-Popien und diverser Industriepartner durchgeführt.

Welche Rolle spielt die Verbesserung von Halbleitern für Quantencomputing?

Quantencomputer sind eine Glanzleistung an Ingenieurskunst und höchst sensible Maschinen und erfordern natürlich absolute Präzision. Hier muss man zwei Dinge wissen: erstens, dass Qubits per se erst mal analog sind und daher momentan nicht nur die Materialien selbst, sondern vor allem die Fertigungsprozesse aus der Halbleiterindustrie wesentlich sind. Zweitens gibt es sehr unterschiedliche physikalische Implementierungen der Quantencomputer und Qubits, und je nach physikalischem Prinzip des Qubits spielen dann auch Halbleiter selbst oder andere Materialien die entscheidende Rolle. Ein häufig benutzter Typ der Qubits sind sogenannte künstliche Atome (Transmons), die auf supraleitenden Schwingkreisen und einer sogenannten Josephson-Junction basieren, bei der – vereinfacht gesagt – die Elektronen durch die isolierende Schicht des Widerstands tunneln. Dort ist z.B. die gleichmäßige Dicke und Güte der Oxid-Schicht relevant, und da das Ganze mit Mikrowellen gesteuert wird, ist natürlich auch die Materialeigenschaft der Leitungselektronik entscheidend, um Störungen zu vermeiden. Eine weitere Klasse sind Ionenfallen. Dort kommt es darauf an, geladene Ionen physikalisch auf einem Chip zu transportieren, optisch anzuregen und die Anregung zu detektieren. Da spielt ein Fortschritt in der Halbleiter-Technologie natürlich auch eine Rolle ebenso wie in Elektron-Spin-basierten Architekturen, bei denen möglichst reine Quantenpunkte präzise angesteuert werden, was hochreine Materialien und Herstellungsprozesse voraussetzt.

Wenn man ein weiteres Paradigma, nämlich photonisches Quantencomputing, betrachtet, wird dort mit Lichtleitern gearbeitet, und sowohl die Erzeugung als auch die Detektion der Photonen ist hier wesentlich, und auch die Güte der Leiter bestimmt die Streuverluste und damit Ausbeute – und ist am Ende entscheidend für die Machbarkeit und Zuverlässigkeit dieses Ansatzes, bei dem einzelne Photonen gezählt werden.

Ferner gibt es noch eine andere Klasse an Qubit-Technologie, die wir auch sehr vielversprechend finden, die sogenannten Stickstoff-Fehlstellen-Diamanten (NV-diamonds), die auch als Quantensensoren in der magnetischen Bildgebung eingesetzt werden. Auch hier kommt es sehr auf die Reinheit der verwendeten Materialien an, z.B. spezielle stabile Kohlenstoff-Isotope, die bei der Herstellung benötigt werden, um dem Diamanten spezielle Eigenschaften, die man für die Informationsspeicherung im Diamanten benötigt, zu geben. Ein Fortschritt in der Materialforschung führt also nicht nur im Halbleiterbereich zu Erfolgen. Die letzte, kontrovers diskutierte, Technologie – das topologische Qubit – benötigt eine spezielle Klasse an Halbleitern; daran wird derzeit weltweit mit Hochdruck geforscht – denn ohne dieses Material X funktioniert der Ansatz nicht. Man kann also zusammenfassend sagen, je nach benutztem Ansatz ist Halbleiterforschung fundamental.

„Ferner gibt es noch eine andere Klasse an Qubit-Technologie, die wir auch sehr vielversprechend finden, die sogenannten Stickstoff-Fehlstellen-Diamanten (NV-diamonds), die auch als Quantensensoren in der magnetischen Bildgebung eingesetzt werden.“

In welchem der drei Segmente, die Merck verfolgt, sehen Sie die größten Anwendungsmöglichkeiten von Quantencomputing: Healthcare – Life Science – Electronics? Warum?

In jedem Bereich gibt es Potenzial. Wenn man in den Kategorien Simulation, Optimierung und Machine Learning denkt, sind hier natürlich Material- und Pharmaforschung/Quantenchemie relevant, aber auch Optimierungsprobleme, die für alle Bereiche Anwendungsmöglichkeiten versprechen, sofern sich denn die Probleme „quantenprofitabel“ formulieren lassen und die Infrastruktur (Hardware und Software) ausgereift genug ist, um auch relevante Probleme ökonomisch sinnvoll anzugehen. Wir experimentieren auch gerade mit neueren Ansätzen des Machine Learning – erwarten dazu erste Ergebnisse allerdings erst nach Redaktionsschluss.

Wo arbeiten Sie aktuell in der Chemie- und Pharmaindustrie mit Quantencomputing-Technologie und möglichen Anwendungen? Warum profitiert gerade dieser Industriezweig besonders vom Quantencomputing?

Wir haben international einige Kollaborationen mit Start-ups z.B. mit SeeQC, die an digitalen Steuereinheiten für Quantencomputer arbeiten, oder mit HQS Quantum Systems aus Karlsruhe, mit denen wir Methoden zur Beschreibung von molekularen Systemen auf Quantencomputern entwickeln, und mit weiteren, die wir noch nicht nennen können. Konkrete Projekte, welche die derzeitig verfügbaren Quantencomputer nutzen, haben wir derzeit als Grundlagenforschung der Machbarkeit und um das Werkzeug kennenzulernen. Das Problem auf dem Weg zur Profitabilität liegt im Moment noch daran, dass es unklar ist, wie ein Quantencomputer tatsächlich skaliert. – D.h. der Weg vom derzeitigen NISQ-Laborprototyp zu einer Maschine, die es erlaubt, echte Probleme profitabel zu lösen, ist zwar in den Portfolios der Hersteller aufgezeigt, ob das aber wirklich funktioniert, ist aus unserer Sicht unklar. Die Hoffnung liegt darin, dass es in absehbarer Zeit sowohl bedienbare Software gibt als auch funktionierende Hardware, die dann Materialforschung in industriellem Maßstab erlaubt. Wichtig hierbei ist allerdings immer wieder zu betonen, dass Quantum Chemistry und generell Computer-Simulationen immer nur ein kleiner Anteil an der Produktentwicklung sind. Wir haben im Rahmen des Pharma Industrie Konsortiums QuPharm, an dem ziemlich alle Pharmafirmen und Hersteller, Berater und Entwickler aus dem Quantencomputing-Ökosystem beteiligt sind, über zweihundert „use cases“ identifiziert, die alle „irgendwie“ mit Quantencomputern untersucht werden könnten. Das Problem sind auch hier wieder eher die Fragen: a) Wie formuliere ich meine Probleme so, dass ein Quantencomputer wirklich helfen kann?, b) Ist der Aufwand den Nutzen wert? und c) Welche alternativen Methoden gibt es, die besser etabliert sind und damit eine höhere Akzeptanz im Unternehmen haben?

Greifen wir ein paar Teilaspekte aus Medizin/Healthcare heraus: Welche Rolle spielt Quantencomputing in der Diagnostik? Spielt die Zusammenarbeit mit Künstlicher Intelligenz eine Rolle für Ihre Forschungen?

Hier sind wieder zwei Aspekte relevant. Quantentechnologie selbst ist fundamental z.B. für die Bildgebung oder sonstige Sensoren für Diagnostik. Je besser die Bildgebung und Sensorik, desto höher der Nutzen – das hat mit Computing eher am Rande zu tun. Das Computing kommt dann bei der Auswertung der Sensoren und der Interpretation der Diagnostik ins Spiel. Es gibt jetzt in der Industrie Bestrebungen, gerade in der Analyse von Bildern auch auf Quantencomputer-gestütztes Machine Learning zu setzen. Inwieweit das Ganze funktioniert, muss sich aber im Benchmark noch herausstellen. Die Hoffnung dabei liegt wieder darin, dass eine spezielle Klasse von Algorithmen spezielle algorithmische Aufgaben besser löst, sei es schneller oder mit weniger Daten. Ein weiteres Anwendungsfeld wäre die Analyse von astronomisch vielen und gleichzeitig hochkomplexen Daten, wie sie zum Beispiel beim Mikrobiom anfallen – wie gesagt, ob man dafür später Quantencomputer profitabel einsetzen kann, ist offen. – Dort findet Grundlagenforschung statt, meist in Kollaborationen.

Das 21. Jahrhundert steht vor der vielleicht größten ökologischen Herausforderung. Die Rede ist vom Klimawandel. Wie schätzen Sie hier die Funktionen von Quantencomputing ein? Gibt es Möglichkeiten, die Leistungsfähigkeit des Quantencomputers auch für das große Thema der Nachhaltigkeit nutzbar zu machen?

Die Hoffnung liegt hier bei der Quantentechnologie sowohl im Computing wie auch in neuartigen Quantenmaterialien, die auch direkt durch bessere Materialeigenschaften zur Lösung des Problems beitragen könnten: Sei es ein Katalysator für die energieeffiziente Herstellung von Dünger (der Heilige Gral) oder, wie oben bereits erwähnt, durch bessere Sensoren, um überhaupt eine Datenbasis zu schaffen, die dann modelliert und analysiert werden kann.

Beim Computing denke ich wieder in den drei Kategorien Machine Learning, Simulation und Optimierung – und definitiv könnte z.B. eine verbesserte, Industrie-übergreifende Optimierung der Materialflüsse zur Vermeidung von unnötigen Transporten beitragen. Wir selbst schauen uns im Rahmen unserer Nachhaltigkeitsstrategie immer wieder an, ob bzw. wo Quantencomputing beitragen kann. Das muss dann von Fall zu Fall geprüft werden und steht und fällt auch sowohl mit den mathematischen Modellen, um komplexe System zu beschreiben, als auch der Verfügbarkeit von Daten.

Seit 2019 kooperiert Merck mit HQS Quantum Simulations. Was erwarten Sie sich von der Partnerschaft und was sind bereits konkrete Erfolge, die daraus entstanden sind?

Wir haben, wie oben erwähnt, unterschiedliche Entwicklungs-Kooperationen sowohl auf Hardware- als auch auf Software-Seite. Für alle unsere Kollaborationen gilt:

- Ziel ist immer die Kommerzialisierung von Quantencomputing-Technologie und damit die Frage: Was fehlt, um eine neue Technologie marktreif zu machen?
- Ziel ist nicht unbedingt eine direkte Anwendung bei Merck, sondern die Entwicklung quantenchemischer Methoden auf NISQ, um ein Gefühl für Quantum Advantage, Zeithorizont, Skalierbarkeit und Kosten zu bekommen.

Speziell bei der Kollaboration mit HQS haben wir jeweils auf beiden Seiten schon viel gelernt und erarbeitet (wir beginnen jetzt das dritte Jahr der Kollaboration). Konkret wissen wir jetzt z.B., wie wir größere chemische Quantensysteme auf NISQ-Hardware der nächsten drei bis fünf Jahre abbilden können (unter Bezugnahme von error/noise), sodass sie aus industrieller Sicht Sinn machen.

Das Konjunkturpaket der Bundesregierung vom Sommer 2020 hat erstmalig dem Quantencomputing eine breite Unterstützung in Höhe einer Milliardensumme zugesichert. Kommt dieser Schritt zum richtigen Zeitpunkt? Wie steht Deutschland, wie Europa im internationalen Vergleich da?

Es gibt ja nie „den richtigen“ Zeitpunkt. Das Paket ist sehr willkommen und war ja schon länger angekündigt. Die Ausschreibungen haben sich dann etwas verzögert – aber jetzt läuft das ganz gut an. Es kommt dabei auch darauf an, ob die Empfänger so vorbereitet sind, dass das Geld zügig sinnvoll eingesetzt werden kann. Bei den Projekten und Anträgen, die ich kenne, ist das der Fall. Flankierend zum Konjunkturpaket gab es die Gründung von QUTAC, in dessen Rahmen wir als spätere Industrie-Anwender unsere konkreten use cases und Bedarfe aus Anwendersicht mit den Forschern und Entwicklern teilen. – Das kenne ich selbst jetzt in dieser Form nicht so prominent im internationalen Vergleich.

Andere Nationen waren dafür vielleicht bei der Förderung etwas schneller oder mutiger. International liegen die USA, China, Japan und auch Kanada und Australien schon leicht vorne, und innerhalb Europas finde ich persönlich Großbritannien vorbildlich, man sieht dort den Vorsprung der Reife der Start-ups.

Deutschland ist als Wissenschaftsstandort und in der Quantenforschung sehr gut aufgestellt. Wir haben einige großartige Start-ups und sehen gerade die Gründung diverser Quantum Valleys. D.h. wir sind mit der Förderung aus öffentlicher Hand vielleicht etwas später gestartet, dann aber doch breit genug aufgestellt, um Konsortien zu bilden, die international ganz vorne mitmischen können. Ganz wichtig hierbei ist auch, dass wir jenseits der nationalen Grenzen denken müssen. Dialog findet überall statt, und als globales Unternehmen im Austausch mit anderen globalen Unternehmen nutzen wir die Vielfalt der jeweils regionalen Stärken.

Interview: Hannes Mittermaier

Dr. Thomas Ehmer

Dr. Thomas Ehmer promovierte in Medizinischer Biophysik in Heidelberg und ist seit September 2000 bei der Merck KGaA in unterschiedlichen Bereichen auf der Suche nach neuen Technologien und deren Anwendungsmöglichkeiten. Derzeit ist er Innovation Incubator im IT Healthcare R&D Informatics Team und untersucht dabei neue Technologien wie neuromorphes Computing und Quantentechnologie (Sensoren und Computing) auf ihren möglichen Wertbeitrag. Er ist Mit-Gründer der Quantum Computing Task Force bei Merck und überzeugt, dass spielerische Neugier der Schlüssel zu wissenschaftlichen und technologischen Durchbrüchen ist, und engagiert sich, die Besonderheiten der Quantenmechanik auch Laien barrierefrei zugänglich zu machen. Dadurch – so die Hoffnung - könnte es möglich werden, „harte Nüsse“ aus neuen Blickwinkeln zu betrachten und mit „unkonventioneller Kreativität“ zu knacken.

Foto: Merck

Ein Quantencomputer auch in Deutschland Nicht der Rechner zählt, sondern die Anwendungen

Ein Gespräch mit Dr. Norbert Gaus

Die technologischen Fortschritte, welche die neue Ära des Quantencomputings verspricht, hängen stark von den Anwendungen für Industrie und Wirtschaft ab. Deutschland will sich in einer eigenen „Quanten-Allianz“, die aus führenden Unternehmen bestehen soll, zusammentun, um sich international besser aufzustellen. Auch die Siemens AG steht schon seit längerer Zeit mit dem Bundeskanzleramt in Kontakt, um eine Quantencomputing-Agenda gemeinsam auszuarbeiten. Dr. Norbert Gaus ist Head of Research in Digitalization and Automation der Siemens AG und blickt auf die Herausforderungen des Quantencomputing-Zeitalters.

Jüngst hieß es, dass führende deutsche Technologie-Konzerne eine sog. „Quanten-Allianz“ bilden würden. Die Idee sei angeblich von der Bundeskanzlerin selbst gekommen. Was verbirgt sich hinter dieser Kooperation und was verspricht sie?

In der Tat ist Siemens seit mehr als einem Jahr in Kontakt mit dem Bundeskanzleramt, das eine nationale Vernetzung der High-Tech-Industrie zur Festlegung einer Agenda für Quantencomputing angeregt hat.

Die Ankündigung großer Förderprogramme durch BMBF und BMWi folgt dem Wunsch nach Zusammenarbeit der großen Industrieplayer. Aber auch die Industrie selbst war nicht untätig und hat mit QUTAC (Quantum Technology and Application Consortium) eine nationale Plattform geschaffen, zu dem Siemens als ein Gründungsmitglied strategische und inhaltliche Impulse liefert – zusammen mit neun weiteren in Deutschland verankerten Weltmarktführern.

Eine Use-Case-übergreifende Zusammenarbeit von Firmen, um nationale und europäische Souveränität zu QC zu stärken und zu sichern, erfordert natürlich eine konstruktive Begleitung der Förderstrategie der Bundesregierung.

Wie sieht Ihre persönliche Zusammenarbeit mit anderen Unternehmen, die Teil dieses Konsortiums sind, aus?

Wir sind Gründungsmitglied des Konsortiums und haben dessen Struktur und Themenfelder mit festgelegt.

In welchen Branchen wird Quantencomputing zuerst einen technologischen Mehrwert darstellen? Warum?

Der technologische Mehrwert wird sich nicht an der Branche, sondern am Anwendungsfall entscheiden! Ab wann fehlerkorrigierte, universelle Quantencomputer zur Verfügung stehen werden, ist eine offene Frage – daher setzt Siemens auf problemspezifische Lösungen, die auf Noisy Intermediate-Scale (NISQ)-Rechnern und maßgeschneiderten, hybriden quanten-klassischen Verfahren und Hardware basieren. Konkrete Anwendungsfälle werden wir innerhalb der nächsten drei Jahren an realen Szenarien erproben. Wir gehen davon aus, dass ein erster kommerzieller Einsatz in sogenannten Verbundleitwerken – beispielsweise bei der Siemens-Elektronikfertigung in Karlsruhe – innerhalb der nächsten Jahre erfolgen wird.

Konkret fokussieren wir uns auf komplexe Optimierungsprobleme, die klassische Computer schnell überfordern, und maschinelles Lernen, wo wir uns Quantenvorteile versprechen, beispielsweise hinsichtlich der Lerngeschwindigkeit.

„Wir gehen davon aus, dass ein erster kommerzieller Einsatz in sogenannten Verbundleitwerken – beispielsweise bei der Siemens-Elektronikfertigung in Karlsruhe – innerhalb der nächsten Jahre erfolgen wird.“

Zusammen mit Partnern haben wir dem BMBF, basierend auf umfangreichen internen Vorarbeiten, ein spannendes Proposal mit Herausforderungen aus dem Bereich „Planning and Control of Assembly and Manufacturing“ vorgelegt, das drängende Probleme von Produktion und Logistik mit Chancen auf direkte industrielle Umsetzung adressiert, sobald passende, problemspezifisch maßgeschneiderte Quanten-Hardware zur Verfügung steht. Wir denken vor allem von der Anwendung her, berücksichtigen aber auch die grundlegenden Herausforderungen des Hardware-Software-CoDesigns.

Ein weiterer Projektvorschlag beim BMWi adressiert Lieferketten und digitale Zwillinge – mit dem Ziel, optimierte Supply-Chains über Herstellergrenzen zu realisieren. Auch künstliche Intelligenz ist ein wesentlicher Bestandteil unserer Strategie, beispielsweise im QLindA-Förderprojekt (Quantum Reinforcement Learning für industrielle Anwendungen).

Quantencomputing wird eine enorme Leistungsfähigkeit attestiert, die im Vergleich zu herkömmlichen Rechnern gerade damit trumpft, deutlich schnellere Berechnungsergebnisse zu liefern. Das wird gerne als „Optimierungslösung“ beschrieben. Können Sie ein Optimierungsbeispiel, das mittels eines Quantencomputers generiert wird, erläutern?

Zwei Aspekte sind bei Optimierungsproblemen von Bedeutung: Die exponentielle Komplexitätssteigerung bei wachsender Problemgröße und die Qualität der erzielten Lösung. Für viele industrielle Probleme ist eine perfekte Lösung aber oftmals gar nicht erforderlich. Praktisch ist es beispielsweise häufig irrelevant, ob die Auslastung einer Maschine 99,5% oder 100% beträgt. Gerade Quanten-Annealer können Näherungslösungen finden, die zwar nicht dem Optimum entsprechen, dafür aber in sehr kurzer Zeit gefunden werden. Dies macht die Technologie für echtzeitrelevante Optimierungsaufgaben wie bei der Steuerung industrieller Prozesse interessant.

Die Meldung verbreitete sich wie ein Lauffeuer, als Mitte Juni 2021 der erste Quantencomputer auf europäischem Boden in der Nähe von Stuttgart in Betrieb ging. Warum ist das ein Meilenstein im Quantencomputing? Ist damit eine neue Ära eingeleitet, weil das traditionelle Computing an ein Ende kommen wird?

Die Aktion hat natürlich ein großes Medienecho ausgelöst, und die Installation ist ein Zeichen für den Technologiestandort Deutschland. Wichtig ist aber, dass selbst eine breite Verfügbarkeit von Quantenchips nicht zum Ende des klassischen Rechners führen wird: Quantenprozessoren werden, ähnlich wie GPUs oder TPUs, als Beschleuniger in integrierten Systemen eingesetzt werden. Die industrielle Anwendung braucht integrierte Quanten-Klassische Systeme, die hybride Algorithmen nutzen. Diese wichtigen Aspekte hat Siemens im Rahmen der Projektvorschläge für die Hightech-Strategie der Bundesregierung berücksichtigt.

„Gewinner der Quantentechnologie ist nicht, wer den ersten Rechner baut –, sondern wer als Erster gewinnbringende Anwendungen der Technologie findet.“

Dieser Quantencomputer, der kommerziell genutzt werden soll, wird von dem amerikanischen Unternehmen IBM betrieben. Die Bundesregierung kündigte an, innerhalb von fünf Jahren einen Quantencomputer „made in Germany“ präsentieren zu können. Warum ist das wichtig und wie realistisch ist das?

Siemens arbeitet mit innovativen Start-ups in Europa und weltweit zusammen, die Quantenbits mit Technologien von NV-Zentren bis hin zu Tieftemperatur-Silizium-Technik implementieren – ein klarer technologischer Gewinner zeichnet sich noch nicht ab. Die akademische Grundlagenforschung wird auch weiterhin neue Wege eröffnen.

Wichtig ist die Balance zwischen Grundlagenforschung, der industriellen Umsetzung und der Optimierung etablierter Quantentechnologien. Essenziell ist nicht die Frage des Produktionsstandorts, sondern die souveräne Verfügbarkeit der Technologie in Europa.

Befürchten Sie eine auseinanderdriftende Schere zwischen Groß- und Kleinunternehmen, da die Großunternehmen die finanziellen Ressourcen besitzen, früher auf Quantencomputing zu setzen? Was würden Sie einem Klein- oder Mittelstandsunternehmen raten, um den Quantencomputing-Zug nicht zu verpassen?

Unternehmen aller Größen arbeiten heute bei anspruchsvollen Themen eng zusammen. Das muss uns auch beim Quantencomputing gelingen. Daher kollaborieren wir eng mit KMUs, die in den beantragten Förderprojekten wichtige Spezialkenntnisse beitragen, dabei aber auch Quantenkompetenzen aufbauen. Wichtig ist auch die Unterstützung der Hochschulen beispielsweise durch frühzeitige Einbindung von QC-Vorlesungen in die Curricula. Transferanstrengungen aus der Forschung in die Praxis, wie sie an Hochschulen für angewandte Wissenschaften gepflegt werden, sind ebenfalls sehr geeignet, um die Bedürfnisse der Wirtschaft zielgerichtet zu adressieren.

Der Klimawandel ist in aller Munde. Die Menschheit steht vor der vielleicht größten Herausforderung ihrer Geschichte: vor der Erhaltung ihres eigenen Lebensraumes. Vielversprechende Ansätze frohlocken zum Beispiel bei einer energieeffizienten Herstellung von Dünger. Was halten Sie davon?

Siemens ist ein Vorreiter beim Klimaschutz. Mit innovativen Technologien trägt unser Unternehmen bereits seit Jahren weltweit zur Eliminierung von Treibhausgasemissionen bei. Mit Erfolg: Der CO_2-Fußabdruck unserer eigenen Wertschöpfungskette konnte seit 2014 um 1,2 Mio. Tonnen, d.h. mehr als die Hälfte (54%), reduziert werden. Bis 2030 soll unser Unternehmen komplett klimaneutral sein. Bis 2050 streben wir zudem eine emissionsfreie Lieferkette an.

Es gibt wahrscheinlich nie den einen „richtigen“ Zeitpunkt, um mit Quantencomputing anzufangen. Aktuell liegt Europa, international gesehen, vielleicht leicht im Hintertreffen. Wie schätzen Sie die derzeitigen Bemühungen Europas und insbesondere Deutschlands ein? Erwarten Sie in den kommenden Jahren einen Technologiesprung mittels Quantencomputing?

Der richtige Zeitpunkt ist jetzt! Dabei geht es für uns alle darum zu verstehen, wie Quantencomputing unsere Produkte und Lösungen besser und wettbewerbsfähiger machen wird. Die von der Bundesregierung angestoßenen Programme verfolgen das Ziel, dieses Potenzial zu heben und dazu technologische Rückstände aufzuholen. Insbesondere in den Bereichen, in denen die deutsche Industrie stark ist. Gewinner der Quantentechnologie ist nicht, wer den ersten Rechner baut –, sondern wer als Erster gewinnbringende Anwendungen der Technologie findet. Dazu ist es notwendig, sich in die Technologieentwicklung einzubringen, um sicherzustellen, dass die domänenspezifischen Anforderungen passend adressiert werden. Siemens beteiligt sich an aktuellen Förderprogrammen vor allem mit Projektvorschlägen, die auf Anwendungen aus unseren Segmenten fokussiert sind.

Interview: Hannes Mittermaier

Dr. Norbert Gaus

Als Executive Vice President der Siemens AG leitet Dr. Norbert Gaus seit 1. Mai 2015 die Hauptabteilung „Research in Digitalization and Automation“. Nach seinem Studium der Elektrotechnik an der Technischen Universität München war er als Wissenschaftlicher Mitarbeiter im Deutschen Forschungszentrum für Luft- und Raumfahrt tätig und wurde an der Ruhr-Universität Bochum zum Dr.-Ing. promoviert. Im Jahr 1991 trat er in die Siemens AG bei Corporate Technology ein und wechselte 1994 in den Bereich „Information and Communication Networks Group“. Von 2001 bis 2005 war Gaus CEO bei Siemens Corporate Research Inc., USA. Von 2005 bis zu seiner heutigen Aufgabe verantwortete er Geschäftsgebiete bei Siemens Healthcare und war dort zuletzt CEO der Division Customer Solutions. Seit März 2018 ist Dr. Norbert Gaus stellvertretender Vorsitzender des Aufsichtsrates der Siemens Healthineers AG.

Foto: Enno Kapitza

1. QUANTUM APPLICATIONS

Quantencomputing bietet eine völlig neuartige Möglichkeit, komplexe Berechnungen sehr viel schneller und oftmals überhaupt erst auf praktische Weise durchzuführen.

Diese bahnbrechende Entwicklung, die in den letzten Jahren große Sprünge in der Praxis erlebt hat, geht auf zwei wissenschaftliche Revolutionen des frühen 20. Jahrhunderts zurück. Die erste Revolution wurde um 1930 durch die radikal neuartige Theorie der Quantenmechanik ausgelöst, die unsere Auffassung von Realität drastisch verändert hat. Die zweite wissenschaftliche Revolution erfolgte in den 1940er-Jahren, indem die Grundlagen für den Bau erster programmierbarer Computer gelegt wurden, welche die Basis aller Rechentechnik sind, wie wir sie heute von Smartphones bis Großrechner kennen. In den letzten beiden Jahrzehnten wurden diese beiden Wissenschaften zusammengeführt und es entstand der interdisziplinäre Zweig des Quantencomputings.

Quantencomputer sind Rechenmaschinen, welche die Effekte der Quantenmechanik verwenden. Dies beinhaltet die Fähigkeit, mehrere Zustände gleichzeitig zu besitzen (Superposition), mit einer Operation viele Zustände gleichzeitig zu verändern (Verschränkung) sowie unwahrscheinliche Lösungen zielstrebig zu erreichen (Tunneling). Neben universellen Quantencomputern spielen sogenannte Quantenannealer eine immens wichtige Rolle, da sie besonders dafür konzipiert sind, Optimierungsprobleme zu lösen.

In dieser Ausgabe erwarten Sie Artikel rund um das Thema Quantencomputing. Die Themen fokussieren technische Hintergründe, mögliche Anwendungsfälle sowie visionäre Gedanken.

MEIST GEKLICKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt über **2.500.000 Mal** geklickt*

Beiträge zum Thema **QUANTUM COMPUTING** erhielten **380.000** Klicks.

	Autor	Thema
#1	**Matthias Ziegler**	Starting the Quantum Incubation Journey with Business Experiments **Seite 56**
#2	**Alexander Eser**	Ist durch Quantum Computing eine „Artificial general intelligence“ in absehbarer Zeit realistisch? **Seite 75**
#3	**Carsten Meurer**	Digital Annealing – a bridge technology for quantum computing **Seite 82**
#4	**Dominik Friedel**	Revolutioniert Quantencomputing die Finanzwelt nachhaltig? **Seite 60**
#5	**Christine Schönig**	Post-Quantum-Kryptographie: Sichere Verschlüsselung trotz Quantencomputer **Seite 73**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 11. August 2021.**

INHALT

Warum Moleküle Quantencomputer brauchen

Michael Streif, Matthias Degroote, Elica Kyoseva, Nikolaj Moll, Raffaele Santagati, Christofer Tautermann, Clemens Utschig-Utschig
Boehringer Ingelheim

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy"

— Richard Feynman

In diesem Artikel erklären wir, warum Quantencomputer hilfreich sind, um komplexe Moleküle zu beschreiben. Aus Gründen der Lesbarkeit und um den Artikel für eine breite Leserschaft zu öffnen, verzichten wir auf genaue mathematische Beschreibungen und auf die Erklärung wichtiger Techniken wie beispielsweise der Jordan-Wigner-Transformation oder der Beschreibung fermionischer Hamiltonians. Hingegen setzen wir ein Grundverständnis der Eigenschaften von Qubits voraus. Für eine mathematische und vollständige Einführung empfehlen wir die Review-Artikel [1, 2].

1 Quantenchemie und Pharmaforschung

Medikamente sind chemische Stoffe, die im menschlichen oder tierischen Körper eine gewünschte Wirkung, zum Beispiel die Hemmung eines Proteins, auslösen. Dazu muss das Medikament in der Lage sein, an körpereigene Moleküle wie Proteine oder DNA mittels Atom- und Molekül-Wechselwirkungen spezifisch zu binden.

Um herauszufinden, ob potenzielle Medikamente dazu in der Lage sind, werden nach der aufwendigen Synthese des Moleküls zur genaueren Untersuchung viele Experimente (in vitro – im Reagenzglas) durchgeführt. Diese Experimente sowie die Synthesen sind sowohl zeitaufwendig als auch kostenintensiv. Wäre man in der Lage, solche Experimente durch andere Methoden zu ergänzen oder sogar vollständig zu ersetzen, wäre es möglich, Medikamente deutlich schneller und effizienter zu entwickeln.

Durch die immer leistungsstärker werdenden Computer war es in den letzten Jahrzehnten möglich, Experimente mit Simulationen auf Computern zu ergänzen. Um vorherzusagen, ob z.B. ein Molekül an ein Protein bindet, muss man allerdings in der Lage sein, beide Systeme sehr genau zu beschreiben, was viel Rechenleistung benötigt.

Um beispielsweise einen Computer dazu zu benutzen, die Frage, ob zwei Atome eine Bindung eingehen, zu beantworten, kann man den Computer eine Potentialkurve berechnen lassen. Die Potentialkurve kann man sich analog dem Verlauf der potentiellen Energie eines Balls in einem Gebirge vorstellen. Auf einem hohen Berg hat der Ball eine höhere potentielle Energie als im tiefsten Tal. Bei zwei Atomen entsteht diese Kurve durch die verschiedenen Abstoßungs- und Anziehungskräfte der verschiedenen Teilchen. In Abbildung 1 zeigen wir den Verlauf der Potentialkurve für zwei Wasserstoffatome. Für kurze Entfernungen von beiden Atomen wird das Geschehen von der Abstoßung der beiden positiv geladenen Kerne und quantenmechanischen Kräften dominiert. Für große Kernabstände überwiegen die anziehenden Kräfte zwischen den negativ geladenen Elektronen und positiv geladenen Kernen. Die Potentialkurve in Abbildung 1 zeigt für verschiedene Abstände der beiden Atome die Energie des Gesamtsystems. Wir finden bei einem Abstand von r = 0.0741 nm = 0.741 Å das Minimum der Potentialkurve, an diesem Punkt gleichen sich abstoßende und anziehende Kräfte aus! Wir haben also herausgefunden, dass zwei Wasserstoffatome sich gerne nah beieinander aufhalten, also eine Bindung eingehen und ein Wasserstoffmolekül bilden. Für solch ein relativ einfaches Molekül stellt die Berechnung der Potentialkurve auf einem klassischen Computer noch kein zu großes Problem dar. Je größer die Systeme sind, desto unzuverlässiger werden die Simulationen auf Computern. So kann es auch zu völlig falschen Vorhersagen kommen, ob Moleküle tatsächlich aneinander binden.

2 Warum Quantencomputer?

In den letzten Jahrzehnten wurde bei der quantenchemischen Simulation auf klassischen Computern viel Fortschritt gemacht. Trotz der vielen Näherungsmethoden, die eingeführt wurden, bleibt die Komplexität der Quantenmechanik schwer zu bewältigen. Zudem führen die vielen eingeführten Näherungen dazu, dass berechnete Vorhersagen nicht immer zuverlässig sind. Das Aufkommen der Quantencomputer und die Verwendung ihrer einzigartigen Eigenschaften wird die Simulation von Quantenchemie in den kommenden Jahrzehnten revolutionieren. Quantencomputer werden bei vielen wichtigen Problemen in der Quantenchemie, wie zum Beispiel der Berechnung der elektronischen Struktur von Molekülen, effizient genaue Ergebnisse liefern. In den letzten zwei Jahrzehnten wurden bei der Entwicklung von Algorithmen und physikalischer Hardware für Quantencomputer bedeutende Fortschritte erzielt.

Wir erwarten, dass die Simulation von Molekülen die erste wirkliche Anwendung sein wird, bei der Quantencomputer ihre beispiellose Rechenleistung zeigen können.

In Abbildung 2 zeigen wir eine Darstellung des Empagliflozin-Moleküls inklusive seiner Elektronenverteilung, ein Wirkstoff zur Behandlung des Diabetes Typ 2. Dieses Molekül besteht aus 58 Atomen und 235 Elektronen. Die Elektronen wechselwirken elektrostatisch und quantenmechanisch miteinander, was Auswirkungen auf die Struktur und Eigenschaften des Moleküls hat. Wenn sich ein Elektron bewegt, spüren alle anderen Elektronen diese Bewegung und reagieren darauf.

Die benötigten Ressourcen auf einem Computer, die für die Simulation eines Moleküls benötigt werden, steigen exponentiell mit der Anzahl der quantenmechanischen Teilchen, der Elektronen, an. Aufgrund dieser exponentiell wachsenden Komplexität sind Moleküle auf klassischen Computern nur mit Näherungen zu beschreiben. Um ein Molekül wie in Abbildung 2 exakt zu berechnen, würde es Computerressourcen benötigen, welche weder heute verfügbar sind noch in absehbarer Zukunft verfügbar sein werden.

Der Nobelpreisträger Richard Feynman hat deshalb schon 1982 vorgeschlagen, anstatt klassischer Computer quantenmechanische Systeme zu benutzen, um andere quantenmechanischen Systeme, wie beispielsweise Moleküle, effizient zu simulieren [4]. Ein solches quantenmechanisches System ist der Quantencomputer.

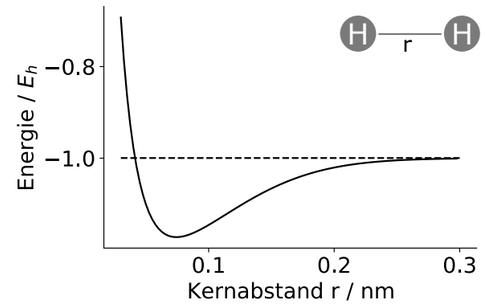


Abbildung 1: Die Potentialkurve eines Wasserstoffmoleküls erzeugt mit dem Computerprogramm PySCF [3]. Wir finden das Minimum der Potentialkurve bei einem Kernabstand von 0.0741nm.

3 Wie kommt das Molekül auf den Quantencomputer?

Auch wenn sich Quantencomputer und klassische Computer grundlegend unterscheiden, sind beides technische Systeme, die dafür genutzt werden sollen, Lösungen von komplexen Problemen zu finden. Die Aufgabe als Benutzer dieser Systeme ist es, das gewünschte Problem mathematisch so zu formulieren, dass es auf einem Computer effizient berechnet werden kann. Hier erklären wir, wie das Problem der Beschreibung eines Moleküls – des Wasserstoffmoleküls – aussieht, zeigen, wie es auf einem Computer beschrieben werden kann und warum die Darstellung auf einem Quantencomputer effizienter ist als die Darstellung auf einem klassischen Computer.

3.1 Moleküle und Quantenphysik

In der Realitat bestehen Moleküle aus Elektronen und Kernen, welche aus Neutronen und Protonen bestehen. Als zu Beginn des 20. Jahrhunderts versucht wurde, die Bewegung der Elektronen und der Kerne zu beschreiben, wurde festgestellt, dass die klassische Physik nicht in der Lage ist, theoretische Vorhersagen zu liefern, die den experimentellen Ergebnissen entsprechen. Man entwickelte eine neue Theorie zur Beschreibung solcher System: die Quantenphysik.

In der klassischen Physik beschreibt man Objekte mit einem Ort und einer Geschwindigkeit – während in der Quantenphysik Teilchen an keinem bestimmten Ort, sondern über den Raum verteilt sind, was durch sogenannte Wellenfunktionen $\Psi(r)$ beschrieben wird. Das Quadrat einer solchen Wellenfunktion $|\Psi(r)|^2$ beschreibt die Wahrscheinlichkeit, das Teilchen an einem bestimmten Ort r im Raum zu finden. In Experimenten wurden außerdem festgestellt, dass, anders als in der klassischen Welt, quantenmechanische Systeme nicht beliebige kontinuierliche Energien besitzen können. Die Energien sind gequantelt – es existieren nur bestimmte, diskrete Energiestufen.

Um solche diskreten Messergebnisse zu beschreiben, verwenden wir in der Quantenphysik Operatoren. Operatoren sind nicht nur einfache Zahlen, sondern beschreiben mathematische Operationen auf Funktionen, wie beispielsweise eine Ableitung. Wendet man Operatoren auf eine Wellenfunktion an, wird diese sich verändern. Zum Beispiel kann ein Operator die Wellenfunktion im Raum verschieben oder ihre Form ändern. Dadurch ändert sich auch die Wahrscheinlichkeit $|\Psi(r)|^2$, das Teilchen an einem bestimmten Ort r zu finden. Der wichtigste aller Operatoren ist der Energieoperator oder Hamiltonian, welcher die Information über die Energiebeiträge im System wie zum Beispiel die Bewegungsenergie und die potentiellen Energien enthält. Der Hamiltonian beschreibt, welche diskreten Energiewerte wir im Experiment messen können. Um die möglichen Messergebnisse zu finden, müssen wir ein mathematisches Problem lösen: Wir müssen die Wellenfunktionen finden, welche unter der Anwendung des Hamiltonians ihre äußere Form nicht ändern. Diese spezielle Klasse von Wellenfunktionen nennen wir Eigenfunktionen des Hamiltonians, und jeder Eigenfunktion können wir eine diskrete Energie zuweisen.

Das mathematische Problem, das wir gerade beschrieben haben, wird in der Schrödinger-Gleichung

$$\hat{H}\Psi(r) = E\Psi(r)$$

abgebildet. Auf der linken Seite, $\hat{H}\Psi(r)$, wirkt der Hamiltonian auf eine Wellenfunktion, auf der rechten Seite, $E\Psi(r)$, steht dieselbe Wellenfunktion multipliziert mit der dazugehörigen Energie E. Die Schrödinger-Gleichung gilt also, wenn die Aktion des Hamiltonians die Wellenfunktion bis auf einen Faktor, nämlich der Energie E, unverändert lässt. Anstatt Eigenfunktionen werden diese Wellenfunktionen dementsprechend auch Lösungen der Schrödinger-Gleichung genannt.

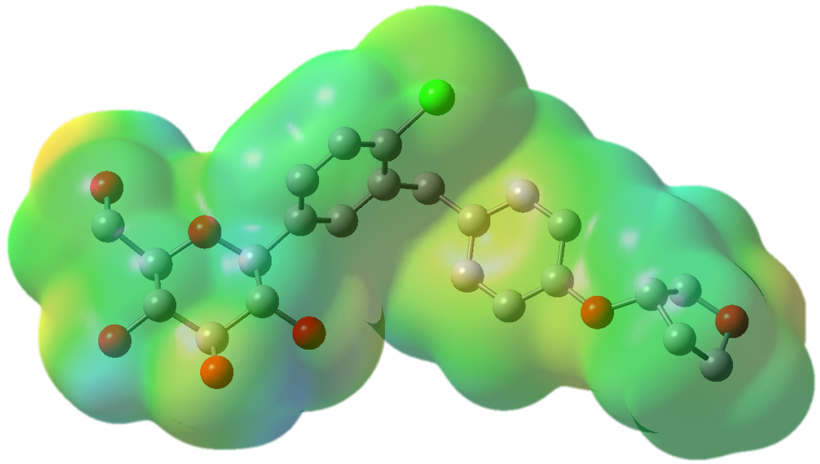


Abbildung 2: Die Struktur des Empagliflozin-Moleküls mit der Strukturformel $C_{23}H_{27}ClO_7$. Die grauen Bälle sind Kohlenstoffatome, die roten Bälle Sauerstoffatome und der grüne Ball Chlor. Die 27 Wasserstoffatome sind in dieser Darstellung nicht gezeigt. Die Wolke gibt die Verteilung der 235 Elektronen des Moleküls an.

3.2 Das Wasserstoffatom

Für jedes System, sei es ein großes Molekül, ein kleines Atom oder gar ein einzelnes Elektron, können wir eine Schrödinger-Gleichung aufstellen. Für jede Schrödinger-Gleichung beschreibt der Hamiltonian $\hat{H}$ die verschiedenen Energiebeiträge des Systems. Als Beispiel schauen wir uns das Wasserstoffatom, H, an, welches aus einem Proton und einem Elektron besteht. In diesem Fall enthält der Hamiltonian $\hat{H}$ die Information über die Bewegungsenergie der Teilchen sowie die Wechselwirkung des Elektrons mit dem Kern. Wir müssen nun herausfinden, welche Wellenfunktionen die Schrödinger-Gleichung für dieses System lösen. Für ein einzelnes Wasserstoffatom können wir die Lösungen nach einer mathematischen Rechnung ohne Hilfe eines Computers finden [6]. Aus allen Lösungen können wir dann die Wellenfunktion mit niedrigster Energie bestimmen – und finden so den energetischen Grundzustand des Atoms. Für das Wasserstoffatom nennen wir diese Lösungen auch Atomorbitale. Da jede Wellenfunktion einen Zustand des Elektrons im drei-dimensionalen Raum beschreibt, können wir die Lösungen auch bildlich darstellen, siehe Abbildung 3 für eine Auswahl der Wahrscheinlichkeitsverteilungen $|\Psi(r)|^2$.

Damit haben wir das Elektron allerdings noch nicht vollständig beschrieben. Elektronen, anders als makroskopische Objekte, besitzen neben ihrer Beschreibung im drei-dimensionalen Raum noch einen weiteren Freiheitsgrad: den Spin. Der Spin ist ein rein quantenmechanisches Konzept und hat keinerlei klassische Interpretation – jedoch kann man ihn als intrinsische Eigenrotation des Teilchens sehen. Diese Eigenrotation kann nur zwei Werte annehmen, entweder der Spin zeigt nach oben (spin up: ↑) oder nach unten (spin down: ↓). Zusammen mit der räumlichen Komponente beschreibt die Spin-Komponente das Atom vollständig.

3.3 Die Elektron-Elektron-Wechselwirkung und das Pauli-Prinzip

Im Vergleich zu allen anderen Atomen des Periodensystems besitzt das Wasserstoffatom ein Alleinstellungsmerkmal: Es ist das einzige Atom mit nur einem Elektron. Andere Atome besitzen viele Elektronen, beispielsweise besitzt Lithium, Li, 3 Elektronen oder Cäsium, Cs, 55 Elektronen. In solchen Systemen gibt es natürlicherweise Wechselwirkungen zwischen Elektronen, welche im Hamiltonian und damit in der Schrödinger-Gleichung beschrieben werden müssen. Des Weiteren gilt für Systeme mit mehreren Elektronen ein weiteres quantenmechanisches Gesetz: das Pauli-Prinzip. Dieses Gesetz besagt, dass zwei Elektronen niemals von der exakt gleichen Wellenfunktion und selber Spin-Ausrichtung beschrieben werden können. Die Wellenfunktion von zwei Elektronen muss sich also entweder in ihrer räumlichen oder ihrer Spin-Komponente unterscheiden. Zum Beispiel dürfen zwei Elektronen mit derselben Spin-Ausrichtung nicht von der selben räumlichen Wellenfunktion beschrieben werden. Die komplizierten Elektron-Elektron-Wechselwirkungen sowie das Pauli-Prinzip machen die Lösung der Schrödinger-Gleichung für Systeme mit mehr als einem Elektron viel aufwendiger als für ein einzelnes Wasserstoffatom mit nur einem Elektron. Bereits das Wasserstoffmolekül, H_2, kann nicht mehr exakt beschrieben werden, sondern muss vereinfacht werden und benötigt die Hilfe von Computerprogrammen.

3.3.1 Näherungen

Eine erste wichtige Näherung ist die Born-Oppenheimer-Näherung. Da ein Proton etwa 2000 mal schwerer ist als ein Elektron, beeinflussen die Elektronen die Bewegung der Kerne kaum. Wir können die Kerne also als ruhend annehmen und unser Problem vereinfacht sich auf das Problem der Beschreibung von Elektronen im Einfluss der ruhenden Kerne. Die komplizierte Elektron-Elektron-Wechselwirkung bleibt allerdings weiter Teil des Problems.

Eine offensichtliche, aber drastische Vereinfachung ist es, diese Wechselwirkung vollständig zu ignorieren. Die Wellenfunktionen, welche wir unter dieser drastischen Vereinfachung finden, sind keine exakten Lösungen der Schrödinger-Gleichung und auch die berechneten Energien weichen stark von experimentellen Werten ab.

Anstatt die Elektron-Elektron-Wechselwirkung vollständig zu ignorieren, ist es besser, sie näherungsweise zu beschreiben. Hierfür gibt es verschiedene Ideen und Ansätze. Die wohl bekannteste Methode ist die Hartree-Fock-Methode, siehe [7]. Das Resultat der Hartree-Fock-Methode sind, analog zu den gefundenen Atomorbitalen des Wasserstoffatoms, Molekülorbitale, welche benutzt werden können, um eine näherungsweise Lösung der Schrödinger-Gleichung zu finden. Für komplexere Systeme wie beispielsweise dem Empagliflozin-Molekül können die Molekülorbitale sehr komplexe Strukturen und Formen annehmen, siehe Abbildung 4 für die grafische Darstellung eines einzelnen Molekülorbitals von Empagliflozin. Die Hartree-Fock-Methode liefert für schwach wechselwirkende Moleküle eine gute Annäherung an den Grundzustand der Schrödinger-Gleichung. Ein weiterer Vorteil ist, dass die benötigte Rechenleistung für die Hartree-Fock-Methode auf klassischen Computern moderat ist, was es ermöglicht, Berechnungen auch für große Moleküle mit vielen Elektronen auszuführen. Für manche Moleküle ist die exakte Wechselwirkung der Elektronen allerdings von entscheidender Bedeutung für die Beschreibung des Moleküls. In solchen Fällen liefert die Hartree-Fock-Methode keine zufriedenstellende Ergebnisse mehr.

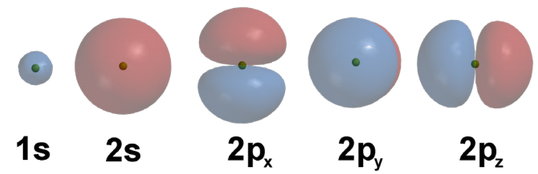


Abbildung 3: Die fünf energetisch niedrigsten Atomorbitale eines Wasserstoffatoms. Bild von [5].

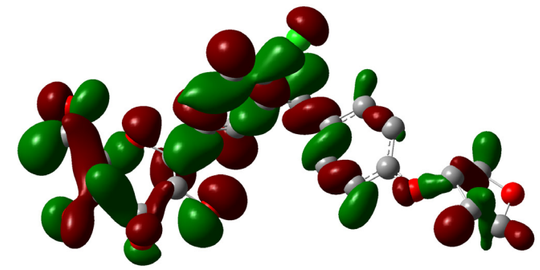


Abbildung 4: Ein Molekülorbital des Empagliflozin-Moleküls, erhalten durch eine Hartree-Fock-Rechnung. Das Molekülorbital ist nicht lokal auf einzelne Atome beschränkt, sondern erstreckt sich über das gesamte Molekül.

3.3.2 Auf dem Weg zur exakten Lösung

Es existieren viele Methoden, welche ausgehend von den Molekülorbitalen versuchen, bessere Lösungen zu finden. Solche Post-Hartree-Fock-Methoden liefern häufig bessere Resultate, sind aber auch deutlich rechenintensiver und deshalb meist nur für kleine Systeme möglich. Ein Beispiel für solche Methoden ist die Full Configuration Interaction (FCI)-Methode, siehe [7].

Die FCI-Methode benötigt auf einem Computer viele Ressourcen. Für ein Molekül mit n Elektronen und N Molekülorbitalen benötigen wir exponentiell viele Koeffizienten, um die FCI-Methode zu implementieren. Diese Koeffizienten müssen wir auf einem klassischen Computer speichern. Nehmen wir an, dass jeder Koeffizient mit einer Präzision von 128 Bits gespeichert wird, benötigten wir für n = 20 Elektronen und N = 40 Molekülorbitale 4 Terabyte an Arbeitsspeicher. Für n = 50 Elektronen und N = 100 Molekülorbitale sind es bereits 10^{18} Terabyte, ein Wert, welcher viele Größenordnungen über dem verfügbaren Arbeitsspeicher des größten Superrechners liegt.

Im Gegensatz ist dieselbe Darstellung auf einem Quantencomputer dank Superposition deutlich effizienter. Für Moleküle mit n Elektronen in N Molekülorbitalen benötigen wir nur N Qubits – eine deutliche Ersparnis gegenüber der Darstellung auf einem klassischen Computer!

Die Darstellung eines Moleküls auf dem Quantencomputer ist allerdings nur der erste Schritt. Als nächstes muss man auf dem Quantencomputer den Grundzustand suchen. Dazu benutzt man Quantenalgorithmen, beispielsweise den Variational Quantum Eigensolver (VQE) [8], einen Quantenalgorithmus für Quantencomputer mit wenigen Qubits und ohne Fehlerkorrektur, oder

Die Hartree-Fock-Methode

Die Hartree-Fock-Methode erlaubt den energetischen Grundzustand der Schrödinger-Gleichung näherungsweise zu bestimmen. Hierfür werden die Elektron-Elektron-Wechselwirkungen nicht explizit beschrieben. Elektronen wechselwirken nicht mehr direkt miteinander, sondern spüren die Wechselwirkung durch ein elektrostatisches Feld, welches von allen anderen Elektronen erzeugt wurde (mean-field approach). Jedes Elektron kann also wieder durch eine eigene Schrödinger-Gleichung beschrieben werden. Löst man diese Schrödinger-Gleichung, erhält man einen neuen Zustand – und eine neues Feld. Man wiederholt dieses Verfahren iterativ, bis sich die Felder nicht mehr ändern. Am Ende der Berechnung erhalten wir Molekülorbitale. Besetzen wir die Molekülorbitale mit niedrigster Energie unter Beachtung des Pauli-Prinzips, erhalten wir eine Wellenfunktion, welche (näherungsweise) den Grundzustand der Schrödinger-Gleichung darstellt. Die mögliche Besetzung der Molekülorbitale kann mithilfe der Dirac-Schreibweise anschaulich dargestellt werden. Das Pauli-Prinzip erlaubt, dass ein Molekülorbital mit einem Elektron mit spin down (↓) und einem Elektron mit spin up (↑) besetzt werden kann: In jedem Molekülorbital ist also Platz für zwei Elektronen. Für zwei Molekülorbitale haben wir also vier freie Plätze um ein Elektron zu platzieren. Der Grundzustand in der Dirac-Schreibweise kann also als $|\downarrow\uparrow, \square\square\rangle$ dargestellt werden – wir haben das erste Molekülorbital mit einem Elektron mit spin down und einem Elektron mit spin up besetzt. Die beiden Plätze, um zweiten Molekülorbital bleiben unbesetzt (□).

Full Configuration Interaction und die Superposition von Qubits

Die Full Configuration Interaction (FCI) ist eine Post-Hartree-Fock-Methode und versucht, den Grundzustand der Schrödinger-Gleichung aus der Überlagerung aller möglichen validen (dem Pauli-Prinzip entsprechenden) Konfigurationen der in der Hartree-Fock berechneten Molekülorbitale zu konstruieren. Für das Beispiel von zwei Molekülorbitalen kann dies in der Dirac-Schreibweise mathematisch als eine lineare Kombination, oder Superposition, dargestellt werden,

$$c_0\,|\downarrow\uparrow,\square\square\rangle + c_1\,|\downarrow\square,\downarrow\square\rangle + c_2\,|\downarrow\square,\square\uparrow\rangle + c_3\,|\square\uparrow,\downarrow\square\rangle + c_4\,|\square\uparrow,\square\uparrow\rangle + c_5\,|\square\square,\downarrow\uparrow\rangle\ .$$

Die Koeffizienten c_i beschreiben den Anteil der verschiedenen Konfigurationen zum Gesamtzustand. Zur Erinnerung: Im Hartree-Fock-Grundzustand war Zustand durch die erste Konfiguration, $|\downarrow\uparrow,\square\square\rangle$, gegeben. In der FCI-Methode optimiert man die Koeffizienten, sodass eine Lösung mit niedrigster Energie gefunden wird.

Mithilfe der Dirac-Schreibweise geben wir an, ob ein Molekülorbital inklusive Spin-Freiheitsgrad besetzt oder unbesetzt ist. Dies können wir auch binär, also mit 0 (unbesetzt) und 1 (besetzt), darstellen. Für den Hartree-Fock-Grundzustand $|\downarrow\uparrow,\square\square\rangle$ können wir also $|1100\rangle$ schreiben und die obige Superposition der verschiedenen Konfigurationen können wir als

$$c_0\,|1100\rangle + c_1\,|1010\rangle + c_2\,|1001\rangle + c_3\,|0110\rangle + c_4\,|0101\rangle + c_5\,|0011\rangle$$

abbilden. Auf einem Quantencomputer können wir diesen Zustand mithilfe von vier Qubits darstellen, bei dem jedes Qubit anzeigt, ob ein bestimmtes Molekülorbital inklusive Spin besetzt oder unbesetzt ist. Die Superposition der verschiedenen Konfigurationen kann dann also durch eine Superposition von Qubits dargestellt werden – der Paradedisziplin eines Quantencomputers!

Quantum Phase Estimation (QPE) [9, 10], einen Quantenalgorithmus für fehlerkorrigierte Quantencomputer. Mit solchen Algorithmen ist man dann in der Lage, den Grundzustand eines komplexen Moleküls für verschiedene Kernabstände zu finden, kann damit exakte Potentialkurven berechnen und genau vorhersagen, ob zwei Moleküle binden. Bis dies Realität wird, wird es allerdings noch einige Jahre dauern. Die bisherigen Quantenchemie-Berechnungen auf Quantencomputern wurden aufgrund der geringen Anzahl von verfügbaren Qubits und den hohen Fehlerraten nur für kleine Moleküle wie beispielsweise BeH_2 [11] oder Wasserstoffketten [12] durchgeführt. All diese ersten Berechnungen könnte man auch problemlos auf heutigen klassischen Computern ausführen. In den nächsten Jahren wird die Anzahl der Qubits weiter steigen, die Fehlerrate sinken und es wird möglich sein, Berechnungen auszuführen, welche auf klassischen Computern undenkbar wären.

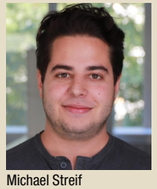
In Zukunft könnte man Quantencomputer dann beispielsweise dazu nutzen, um das in Abbildung 2 gezeigte Empagliflozin-Molekül akkurat zu beschreiben. Dies wäre der erste Schritt in Richtung einer neuen – von Quantencomputern unterstützten – Art der Medikamentenentwicklung. Für echte bahnbrechende Innovationen müssten im Anschluss allerdings viele weitere Forschungsfragen beantworten werden, zum Beispiel wie man das Molekül mithilfe eines Quantencomputers nicht nur im Vakuum, sondern auch im Umfeld des menschlichen Körpers beschreiben könnte. Hierzu müssten dann nicht nur leistungsstärkere Quantencomputer gebaut, sondern auch bessere Quantenalgorithmen entwickelt werden.

Zusammenfassend war das Ziel dieses Artikels, einen ersten Einblick in die Welt der Moleküle zu geben und zu erklären, wie diese auf einem Quantencomputer dargestellt werden können. Die hier gewählte Darstellung mittels Molekülorbitalen ist allerdings nur eine vieler Möglichkeiten, ein Molekül darzustellen.

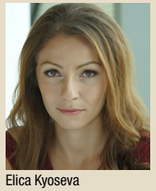
Ebenso gibt es viele weitere Methoden für klassische Computer, welche gute Näherungen erzeugen können. Wichtige Beispiele solcher Methoden sind die Dichtefunktionaltheorie (DFT), Coupled Cluster-Methoden (CC) oder das Møller-Plesset-Verfahren, siehe [7]. In den nächsten Jahren, wo die Rechenleistung der Quantencomputer aufgrund der geringen Anzahl von Qubits beschränkt sein wird, ist es dementsprechend wichtig, Probleme zu identifizieren, welche mit diesen klassischen Methoden nicht mehr akkurat genug dargestellt werden können, um so Raum für einen möglichen Quantenvorteil zu schaffen.

Literatur: **[1]** Bela Bauer, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Chan. Quantum algorithms for quantum chemistry and quantum materials science. Chemical Reviews, 120(22):12685– 12717, 2020. **[2]** Yudong Cao, Jonathan Romero, Jonathan P Olson, Matthias Degroote, Peter D Johnson, M´aria Kieferov´a, Ian D Kivlichan, Tim Menke, Borja Peropadre, Nicolas PD Sawaya, et al. Quantum chemistry in the age of quantum computing. Chemical reviews, 119(19):10856– 10915, 2019. **[3]** Qiming Sun, Timothy C Berkelbach, Nick S Blunt, George H Booth, Sheng Guo, Zhendong Li, Junzi Liu, James D McClain, Elvira R Sayfutyarova, Sandeep Sharma, et al. PySCF: the python-based simulations of chemistry framework. Wiley Interdisciplinary Reviews: Computational Molecular Science, 8(1):e1340, 2018. **[4]** Richard P Feynman. Simulating physics with computers. International Journal of Theoretical Physics, 21:467–488, 1982. **[5]** Wikimedia Commons. Different p-orbitals and s-orbitals. https://commons.wikimedia.org/wiki/File:AOs-1s-2pz.png, 2006. [Online; accessed 21-July-2012]. **[6]** David J Griffiths and Darrell F Schroeter. Introduction to quantum mechanics. Cambridge University Press, 2018. **[7]** Attila Szabo and Neil S Ostlund. Modern quantum chemistry: introduction to advanced electronic structure theory. Courier Corporation, 2012. **[8]** Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Al´an Aspuru-Guzik, and Jeremy L O'brien. A variational eigenvalue solver on a photonic quantum processor. Nature communications, 5(1):1–7, 2014. **[9]** A Yu Kitaev. Quantum measurements and the abelian stabilizer problem. arXiv preprint quant-ph/9511026, 1995. **[10]** Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002. **[11]** Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. Nature, 549(7671):242–246, 2017. **[12]** Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Sergio Boixo, Michael Broughton, Bob B Buckley, David A Buell, et al. Hartree-fock on a superconducting qubit quantum computer. Science, 369(6507):1084–1089, 2020.

Alle Autoren sind Teil des Quantum Computing Teams von Boehringer Ingelheim


Michael Streif

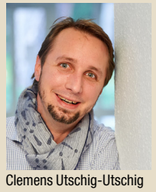

Matthias Degroote


Elica Kyoseva


Nikolaj Moll


Raffaele Santagati


Christofer Tautermann


Clemens Utschig-Utschig

Fotos: Privat

Quantum computing comfort zones

Clemens Schäfermeier
attocube systems

Quantum computing has made its way into "everyday" media, from television to newspaper. Due to the unavoidable effect of information loss over various communication channels, quantum computers are already facing a similar fate as the popular metaphor of a "quantum leap": a portray of a can-do-it-all machine is quickly drawn in the most vivid colours. Or its threat to nowadays data security is used to forecast the potential darker side of coming technology, notoriously exploited by pseudo-scientists. It is not surprising that a new technology, whose intricacies astonish even the experts and which is yet not applied in actual real-world problems, has gained a reputation that falls short in describing the actuality. It is also not surprising that, when multiple solutions are at hand for a challenge, the one that shows the first results receives the greatest attention. Willingly or unwillingly, this can lead to building on technologies that are fast to realise, but not efficient in the long run. It is, so to speak, the time-to-market rule for technology.

Yet quantum computers are different in many aspects, but there appears to be no exception to that time-to-market rule. Not only since Google and IBM have shown their technological advancements towards real-world applications, the time-to-market race in quantum computing technology shows a clear winner: so-called gate-based models with realisations in cryogenic environments. The reasons why this approach has achieved the most attention? First, gatebased quantum computing adopts well-developed concepts from classical computing. It is a sequential set of operations, realised by a (finite) set of basis gates. Second, cryogenic environments have been the establishing grounds for solid-state quantum experiments. A solid-state quantum computer is thus inevitably connected to cryogenics. As a result, today's newspapers show photos of cryogenic equipment to visualise quantum computers.

Let us review why there are other solutions towards quantum computers, and what benefits they might offer in the end. To review other solutions, let us motivate why there can be other solutions in the first place. To anticipate the overall answer: because the underlying concept is easily overlooked when a particular solution is at hand. In the following, we will discuss the mentioned solutions of "gate-basedness" and cryogenic hardware.

The particular solution of gate-based computing originates from the earliest theoretical discussions of quantum computers, starting in the 1980s [1–3]. First experimental realisations were published less than 2 decades later [4, 5] – compared to many theoretical ideas in quantum mechanics a "fast lane" development. So what is the underlying concept of this solution of gate-basedness? Quantum computing, that is: the quantum

part of it, builds upon superposition and entanglement [6]. These ingredients make room for the characteristic weirdness of quantum mechanics, and are the differentiating factor between classical and quantum bits (technical parenthesis: when focussing on pure states). The spirit of gate-based quantum computing is to establish these features by starting with the most fundamental qubits and forcing them along a sequence of logic gates. Over this course, entanglement is built-up by gates, connecting the lanes. As the input states are following those lanes, one creates “quantum truth tables”. On paper, this is extendable to any desired complexity. In reality, the hurdle to overcome is: the more complex the algorithm, the more gates are required. Which in turn generates the need for longer and longer storage times – coherence is the keyword for the overall scheme – and more efficient gate implementations. Plus each gate needs to be controlled, demanding for more wiring and eventually a better space management. So if we assume that for most quantum-computational benefits, one requires entanglement and superposition, we might ask - is there another path to it? One that shifts the demand to something more, say, scalable? To repeat in simplified terms: in orthodox gate-based quantum computation, we start with unentangled states. Then by means of gates, an algorithm is implemented. The difficult part is thereby the “channel” between input and result, not the input. What if we could move the difficulty from the channel to the generation of input states? It can turn out that creating large entangled states is increasingly easier, the more demanding the tasks becomes. If that means a decreased amount of operations on the input, it comes as a benefit. In fact, from quantum metrology, we learned the tenet that the same measurement sensitivity is achievable with a “simple” input state and a challenging measurement operation – or vice versa [7]. This tenet is an exploitable consequence of time reversibility in quantum mechanics. While this is not waterproof and while it sweeps many critical concepts under the rug, we draw this analogy for reasons of clarity. As is now suggested to the reader, such an approach also exists for quantum computing. Most commonly it is referred to as measurement-based quantum computing and was introduced in the 2000ths [8–10]. While we find variations of measurement-based quantum computing, the underlying approach is to create an entangled input state which is sufficiently large to support the amount if information required for the task. Next, only a few basic measurements need to be performed on that state. These measurements are essentially the “gates” in a gate-based approach; however, there is no need for coherence between the gates. Though difficult in their generation, experimental proof of several thousand entangled modes, so-called cluster states, was published 2019 [11, 12]. The resulting number of qubits was still less than 10 for the implementations, and error correction is lacking for this demonstration, as well. Since this field of quantum computing is rather young, its potential is yet to be unravelled. To draw one major technical advantage: the demonstrated generation of cluster-states was performed with photons of the telecom wavelength. A need for transduction between “stationary” and “flying” qubits like in IBM’s quantum computer does not exist. Amongst very few, Xanadu is a company that early on capitalises on measurement-based concepts [13, 14].

To mention as well is PsiQuantum; while their exact approach remains secret to the public, they gathered $ 215 million of funding on what is speculated to be a measurement-based quantum computer [15]. We should note that there is no free lunch also for measurement-based concepts. This motivated theoretical proposals to combine gate- and measurement-based approaches into a “hybrid” concept [16].

Now that we covered the first paradigm of circuit implementation, let us turn to the apparent need for cryogenic hardware. Whenever qubits are realised, key is to preserve their coherence over the computation time. Interactions with “the environment”, which is usually depicted as an abstract medium that scrambles information, destroy that important feature. While theoretically no information ever is lost, this idea of the environment is a practical concept. Shielding the qubit from its environment is commonly achieved by cutting off unwanted paths to the system of interest. A viable way is to lower the energy of the environment to a point where it is negligible compared to the qubit’s “activation” energy. One “freezes out” the paths to the qubit. Why special cooling equipment (cryostats) is required in solid state systems is seen when equating energy to frequency

$E = hf$ and energy to temperature $E \propto k_B T$. For an operation between 1 – 10 GHz, the temperature T is on the order of 50 – 500 mK (-273.10 to -272.65 °C). To shield a qubit of that frequency from its surrounding, the environment should be cooled to temperatures of at least one order of magnitude lower. Thus cryogenics are found in almost any solid state quantum computer. Surely, with the aim to build bigger systems, more heat is potentially introduced to the processing unit, in turn increasing the demand for more cooling power. There are a few other ways to overcome the need for cryogenics, alas. One is: rather than on damping the environment, the coupling between the environment and the qubit is cut. This is achievable by resonators. Another way, seized by startups as Xanadu, is to increase the frequency of the qubit. A drastic increase is achieved by moving from stationary qubits, for instance realised by Josephson junctions, to flying qubits, that is: photons. A photon at telecom wavelength has an energy of 800 meV, which is about 9000 K. Contributions to a 1550 nm photon from photons at room temperature are rather unlikely. Hence, photonic quantum computers are often operated outside of cryostats. Sometimes cooling is required to enable efficient detection or creation of photons, but that is not a general rule. Why so are cryostats representing quantum computers? Because current cleanroom technology can be adopted to the production of solid-state systems. Making compact optical quantum computers will involve the implementation of optical setups, stretching over square-meter sized tables, to photonic chips. Their maturity is not yet as solid as the one of solid state, and mass production is yet to come – potentially to be on par with semiconductor technology.

To conclude, we have discussed the current paradigms of quantum computing and offered a brief overview and approach outside of the apparent comfort zone, namely gate-based quantum computers working at very low temperatures. As a simple bottom line, the way towards quantum computing should be kept open for exploration. Since investors, public and private, are not necessarily experts on the very technology and are furthermore not always motivated by decadelong success, this is a plea rather towards scientists. By offering alternative approaches, we cannot only decrease the risk of ending up in dead-ends. We can also make room for public participation, we can decrease the risk of fraudulent usage; we can at least provide some ground for the right use of a technology that holds high promises in solving pressing problems across the world. The more investors embarked on quantum technology, specifically computing, the more vital it is to stress the importance of alternative routes towards a technology yet outside of our comfort zone.

Figure 1: Typical depiction of a quantum computer: a cryostat. It cools the quantum processor down to a few milli Kelvin.

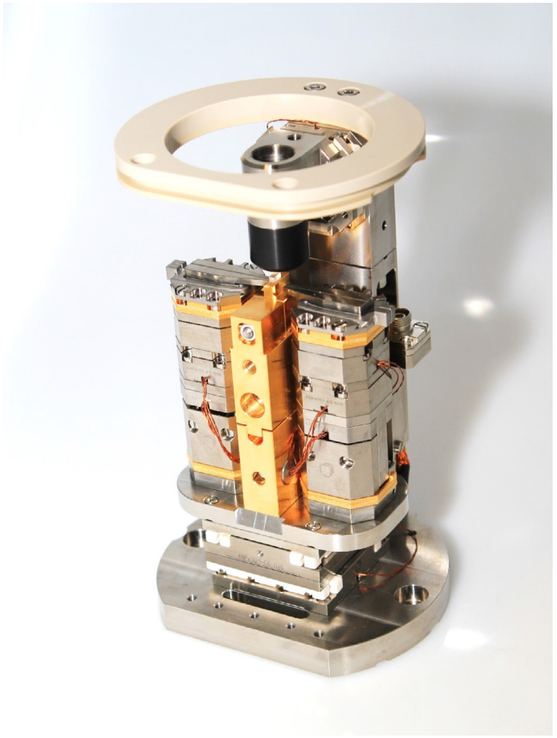
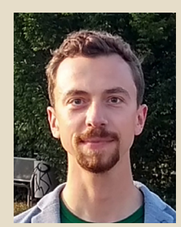


Figure 2: Setup to implement a photonic quantum computer. Measurementbased concepts at room temperature can be realised on such a platform. The central piece below the objective (2 cm in diameter) carries a photonic chip, the holders to the left and right hold optical fibres.

References: **[1]** P. Benioff. “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines”. In: J. Stat. Phys. 22.5 (May 1980), pp. 563–591. doi: 10. 1007/BF01011339. **[2]** R. P. Feynman. “Simulating physics with computers”. In: Int. J. Theor. Phys. 21.6 (June 1982), pp. 467–488. doi: 10.1007/BF02650179. **[3]** P. Benioff. “Quantum mechanical hamiltonian models of turing machines”. In: J. Stat. Phys. 29.3 (Nov. 1982), pp. 515–546. doi: 10.1007/BF 01342185. **[4]** C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland. “Demonstration of a Fundamental Quantum Logic Gate”. In: Phys. Rev. Lett. 75.25 (Dec. 1995), pp. 4714–4717. doi: 10.1103/PhysRevLett.75. 4714. **[5]** MIT researchers create quantum computer that simulates quantum system. MIT news. June 1999. url: https://news.mit.edu/1999/quantum. **[6]** R. Jozsa and N. Linden. “On the role of entanglement in quantum-computational speed-up”. In: Proc. R. Soc. Lond. A. 459.2036 (2003), pp. 2011–2032. doi: 10.1098/rspa.2002.1097. **[7]** K. J. Resch et al. “Time-Reversal and Super-Resolving Phase Measurements”. In: Phys. Rev. Lett. 98.22 (May 2007), p. 223601. doi: 10.1103/ PhysRevLett.98.223601. **[8]** R. Raussendorf and H. J. Briegel. “A One-Way Quantum Computer”. In: Phys. Rev. Lett. 86.22 (May 2001), pp. 5188–5191. doi: 10.1103/ PhysRevLett.86.5188. **[9]** H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf and M. Van den Nest. “Measurement-based quantum computation”. In: Nat. Phys. 5.1 (Jan. 2009), pp. 19–26. doi: 10.1038/nphys1157. **[10]** R. Jozsa. “An introduction to measurement based quantum computation”. In: arXiv e-prints (Sept. 2005). arXiv: quant-ph/0508124. **[11]** W. Asavanant et al. “Generation of time-domain-multiplexed two-dimensional cluster state”. In: Science 366.6463 (2019), pp. 373–376. doi: 10.1126/ science.aay2645. **[12]** M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen and U. L. Andersen. “Deterministic generation of a two-dimensional cluster state”. In: Science 366.6463 (2019), pp. 369–372. doi: 10.1126/science.aay4354. **[13]** D. Su, K. K. Sabapathy, C. R. Myers, H. Qi, C. Weedbrook and K. Brádler. “Implementing quantum algorithms on temporal photonic cluster states”. In: Phys. Rev. A 98.3 (Aug. 2018), p. 032316. doi: 10.1103/ PhysRevA.98.032316. **[14]** Xanadu. 2021. url: https://www.xanadu.ai/. **[15]** PsiQuantum. 2020. url: https://psiquantum.com/news/. **[16]** M. Zwerger, H. J. Briegel and W. Dür. “Hybrid architecture for encoded measurement-based quantum computation”. In: Sci. Rep. 4.1 (June 2014). doi: 10.1038/srep05364.

Dr. Clemens Schäfermeier

Studium der Physikalischen Technik an der FH Münster, MPI Hannover und MPI Erlangen; Promotion an der DTU in Kopenhagen über die Quantenoptik in Kommunikation und Metrologie; Postdoc an der TU Delft. Seit 2018 bei attocube systems in der Forschungsabteilung innovision.



Fotos: attocube systems

Quantum Annealing und das Assignmentproblem

Ruben Pfeiffer, Lilly Palackal, Hans Ehm, Maximilian Hess
Infineon Technologies AG

Einleitung und Motivation

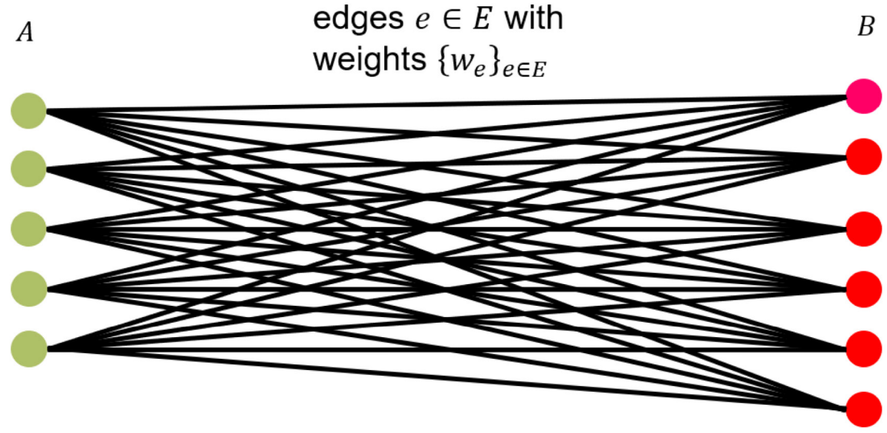
In vielen Bereichen der Forschung und der Industrie tun sich aktuell dank immer ausgereifteren und größeren Quantencomputern neue Möglichkeiten auf. Die Frage nach einer baldigen Quanten-Überlegenheit, also der Möglichkeit, mit einem Quantencomputer Probleme schneller oder genauer als mit einem klassischen System zu lösen, wird heiß diskutiert und durch neue Anwendungen, Technologien und Forschungsprojekte immer weiter befeuert.

Die Realität ist jedoch, dass die meisten, wenn nicht alle Quantentechnologien noch in den Kinderschuhen stecken. Mit Qubitzahlen im niedrigen zweistelligen Bereich, wie zum Beispiel bei IBM [1], lassen sich kaum Probleme nennenswerter Größe, gerade für die praktische Anwendung in der Industrie, angehen. Eine potenzielle Ausnahme bietet das Quantum Annealing, für das das Unternehmen D-Wave der Öffentlichkeit bereits Systeme mit mehreren Tausend Qubits zur Verfügung stellt. Diese Maschinen sind zwar keine universellen Computer, sondern arbeiten ausschließlich mit Optimierungsproblemen bestimmter Formate; die Firma selbst behauptet dafür allerdings, dass hiermit bereits einige industriell relevante Anwendungen besser gelöst werden können als mit klassischen Rechnern [2].

Eines der Probleme, die mit Quantum Annealing angegangen werden können, ist das Assignmentproblem. Dieses fundamentale Optimierungsproblem in einem gewichteten, bipartiten Graphen stellt die Frage nach einem Matching mit minimaler Summe der Kantengewichte im Matching. Das Assignmentproblem ist bereits gut erforscht und mit klassischen Methoden sowohl approximierbar als auch algorithmisch lösbar. Die bekannten Algorithmen, selbst für die Approximierung, haben allerdings erhebliche Laufzeiten für in der Industrie relevante große Probleminstanzen [3]. Zudem weicht die Qualität heuristischer Annäherungen von den Idealwerten oft in relevantem Maße ab. Sollten Lösungen, die Quantum Annealing nutzen, die Qualität der bekannten Heuristiken erreichen, könnten sie ein wichtiges Werkzeug für die praktische Anwendung werden und ein Schritt in Richtung der bereits erwähnten Quanten-Überlegenheit sein.

Wir befassen uns in diesem Beitrag genauer mit der Verwendung von Quantum Annealing zur Lösung des Assignmentproblems und einigen potenziellen Anwendungen, die sich in der Industrie daraus ergeben. Hierbei möchten wir die besprochenen Sachverhalte für den interessierten Leser ohne besondere Vorkenntnisse bezüglich Matchingproblemen oder Quantum Annealing verständlich machen.

Zunächst definieren wir das Assignmentproblem formal und gehen kurz auf bekannte klassische Algorithmen und insbesondere ihre Laufzeiten ein. Danach zeigen wir auf, dass dieses Problem nicht nur ein fundamentales Optimierungsproblem in der Wissenschaft ist, sondern auch wichtige Anwendungen in vielen Bereichen der Industrie hat. Als konkretes Beispiel betrachten wir die Planung einer global verteilten Supply Chain. Mithilfe einer Prognose der Nachfrage können wir einen Teil der Planung als Instanz des Assignmentproblems modellieren. Hierbei entspricht minimales Kantengewicht einer optimalen Einteilung der verfügbaren Produktionsmittel. Dieser Anwendung geben wir den Namen Demand-Supply-Matching. Anschließend führen wir das von D-Waves Quantum Annealern verwendete Format Quadratic Unconstrained Binary Optimization, kurz QUBO, ein und legen dar, wie man eine beliebige Instanz des Assignmentproblems in diese Form überführen kann, um es danach mit Quantum Annealing oder auch einer anderen Lösungsmethode für QUBO-Probleme behandeln zu können. Zuletzt versuchen wir uns an einem Ausblick auf weitere Anwendungsfälle und mögliche Methoden zur Verbesserung der Ergebnisse, die Quantum Annealing für das Assignmentproblem liefert.



Das Assignmentproblem

Das Assignmentproblem arbeitet auf einem gewichteten bipartiten Graphen G=(V,E). Das bedeutet, dass die Knotenmenge V in zwei disjunkte Teilmengen A und B partitioniert werden kann, sodass für jede Kante e=(a,b) gilt: a ∈ A und b ∈ B. Jeder Kante e ∈ E wird ein Kantengewicht $w_e \in R$ zugeordnet. In diesem Graphen soll nun ein Matching, also eine Teilmenge M ⊆ E, in der für jede zwei Kanten m,n ∈ M gilt, dass sie keinen Knoten teilen, gefunden werden. Dabei suchen wir dasjenige Matching, welches die Summe der Kantengewichte $\sum_{m \in M} w_m$ maximiert bzw. minimiert.

Duan und Pettie beschäftigten sich 2014 extensiv mit klassischen Methoden zur Lösung sowie zur Approximierung des Assignmentproblems und des allgemeineren Maximum Weight Matching-Problems. In ihrer Aufstellung finden sich Algorithmen, die das Assignmentproblem in $O(m\sqrt{n} + n^2 \log n)$ bzw. für ganzzahlige Kantengewichte in $O(m\sqrt{n} \log N)$ mit $m := |E|, n := |V|$ und $N := \max(\{w_e : e \in E\})$ lösen. Sie entwickelten außerdem einen Approximationsalgorithmus mit Laufzeit in $O(m\epsilon^{-1} \log \epsilon^{-1})$, wobei $\epsilon > 0$ als Betrag des maximalen Fehlers, den man in Kauf nimmt, definiert ist [3]. Alle diese Laufzeiten sind mindestens linear in m, also in der Anzahl der Kanten in G, was bei einer großen Probleminstanz zu erheblichem Zeit- und Rechenaufwand führt. Quantum Annealing bietet hier die Chance, maßgeblich an Aufwand zu sparen, sofern es ebenfalls gute Ergebnisse liefert.

Erstes Anwendungsbeispiel: Supply Chain-Planung via Demand-Supply-Matching

Die Planung einer großen Supply Chain mit vielen, weltweit verteilten Produktionsstätten und einer konstant fluktuierenden Nachfrage ist ein sehr komplexes Problem. Von dessen Optimierung hängen sowohl Gewinn als auch Kundenzufriedenheit maßgeblich ab. Im Folgenden wollen wir skizzieren, wie man durch die Lösung eines speziell konstruierten Assignmentproblems zumindest einen Teil dieser komplizierten Planung vereinfachen und dann auch optimieren kann.

Hierfür benötigen wir einen Überblick über die verfügbaren Produktionsstätten des betrachteten Unternehmens und ihre potenzielle Leistung für die betrachtete Zeitspanne (im Folgenden Angebot genannt) sowie eine Vorhersage der angefragten Produktmengen in derselben Zeitspanne (im Folgenden Nachfrage). Das verfügbare Angebot soll dann so genutzt werden, dass der erzielte Gewinn maximiert wird, indem die Nachfrage zu einem möglichst großen Teil abgedeckt wird. Wir treffen zwei vereinfachende Annahmen, die in der Praxis meistens gegeben sind oder durch eine Anpassung der Prognose der Nachfrage erfüllt werden können:

- Die Nachfrage lässt sich in einzelne Teilaufträge zerlegen, die nicht voneinander abhängen und ungefähr identische Ressourcen benötigen (z. B. die Fertigung einer bestimmten Stückzahl eines bestimmten Produkts).
- Das Angebot ist nie in der Lage, die Nachfrage komplett zu bedienen, ohne selbst voll ausgelastet zu sein.

Mit diesen Annahmen können wir nun zwei Mengen S und D definieren. S enthält ein Element für jeden Auftrag, den eine der Produktionsstätten in der betrachteten Zeitspanne ausführen kann. D enthält ein Element für jede auszuführende Tätigkeit in der Nachfrage. Diese beiden Mengen bilden unsere Knoten-

menge $V = S \cup D$ für das Assignmentproblem. Wir definieren dann die Kantenmenge E, indem wir eine Kante e_{sd} zwischen allen s ∈ S und d ∈ D einfügen, für die eine Zuweisung des Auftrags d zur Produktionsstätte, der s zugeordnet ist, theoretisch möglich wäre. Wie genau dabei die Kantengewichte zu wählen sind, ist noch eine offene Frage bei dieser Anwendung, jedoch sollten sie offensichtlich den erzielten Umsatz durch die jeweiligen Zuweisungen abbilden, wobei entstehende Kosten abgezogen werden.

Finden wir nun, entweder klassisch oder per Quantum Annealing, ein Matching mit maximaler Summe der Kantengewichte, erfüllt dieses Ergebnis folgende Eigenschaften:

- Da im Matching jeder Knoten aus V maximal einmal vorkommt, werden nach unserer Definition von S und D keine Produktionsstätten überlastet und keine Aufträge ausgeführt, die nicht zur Abdeckung der vorhergesagten Nachfrage dienen.
- Da das Matching die maximal mögliche Summe Kantengewichte hat, entspricht es auch der Zuteilung des Angebots zu Aufträgen aus der Nachfrage mit dem maximal möglichen erzielten Gewinn.

Eine Lösung unseres Assignmentproblems liefert uns also eine optimale Zuteilung der verfügbaren Ressourcen unseres betrachteten Unternehmens in der betrachteten Zeitspanne.

Vom Graphen zum QUBO-Problem

Wir haben uns ausführlich mit dem Assignmentproblem und einer industriellen Beispielanwendung befasst. Jedoch können die Quantum Annealer von D-Wave nicht direkt mit einem graphentheoretischen Optimierungsproblem umgehen, sondern benötigen sehr spezielle Problemformate, die in einer quadratischen Matrix kodiert werden können. Eines dieser Formate ist das Quadratic Unconstrained Binary Optimization-Problem, kurz QUBO.

Die formale Definition des allgemeinen QUBO-Problems lautet:

$$\underset{x\in\{0,1\}^k}{\text{minimize/maximize}}\, y = x^T Q x$$

mit einem Vektor von binären Entscheidungsvariablen x und einer problemspezifischen quadratischen Matrix Q mit k×k reellen Einträgen [4].

Zu erwähnen ist hier, dass die Maximierungs- und die Minimierungsvariante des Problems äquivalent zueinander sind und durch die Transformation Q ↦ -Q ineinander umgewandelt werden können. Im Folgenden betrachten wir stets das Minimierungsproblem.

Bevor wir damit anfangen, das Assignmentproblem in diese Form umzuwandeln, verdeutlichen wir zunächst, was die Einträge von Q im Einzelnen repräsentieren. Eine Ausmultiplizierung der oben eingeführten Definition des QUBO-Problems ergibt folgende Formel:

$$\underset{x\in\{0,1\}^k}{\text{minimize}}\, x^T Q x = \underset{x\in\{0,1\}^k}{\text{minimize}} \sum_{i=1}^{k} q_{ii} x_i + \sum_{i<j} q_{ij} x_i x_j$$

Hier kann man erkennen, dass die Einträge q_{ii} von Q, die auf der Diagonale liegen, jeweils nur mit einer Entscheidungsvariable aus x multipliziert werden, während alle anderen Einträge q_{ij} mit i≠j von Q mit zwei Entscheidungsvariablen multipliziert werden. Das QUBO-Problem lässt sich also in einen linearen und einen quadratischen Term aufteilen, um den potenziellen Nutzen von einzelnen Entscheidungen sowie die Zusammenhänge zwischen je zwei Entscheidungen getrennt voneinander betrachten zu können.

	x_1	x_2	x_3	⋯
x_1	q_1	$q_{1,2}$	$q_{1,3}$	⋯
x_2		q_2	$q_{2,3}$	⋯
x_3			q_3	⋱
⋮				⋱

Matrix Q

Nun können wir uns der tatsächlichen Umwandlung des Assignmentproblems in eine QUBO-Formulierung widmen. Wir erinnern uns an die allgemeine Definition des Assignmentproblems als Graph G=(V,E) mit |E|=m. Um von diesem Graphen zu einem QUBO-Problem zu gelangen, definieren wir zunächst unseren Entscheidungsvektor $x=(x_1,x_2,\ldots,x_m)$ mit jeweils einer Entscheidungsvariable $x_i \in \{0,1\}$ für jede Kante in E. Die zu treffenden Entscheidungen bestehen also darin, welche Kanten des Graphen wir ins resultierende Matching aufnehmen und welche nicht.

Im ursprünglichen Assignmentproblem ist der zu optimierende Wert die Summe aller Kantengewichte im Matching. Dies lässt sich intuitiv durch den linearen Anteil des QUBO-Problems repräsentieren; die Einträge q_ii auf der Diagonale von Q entsprechen also jeweils dem Gewicht der zur Entscheidungsvariable x_i gehörenden Kante $e_i \in E$. Zu beachten ist hier, dass wir am Ende ein Minimierungsproblem bekommen wollen; sollte unsere betrachtete Instanz des Assignmentproblems ein Maximierungsproblem sein, müssen wir hier also die negativen Kantengewichte $-w_e$ für die Diagonaleinträge verwenden.

Die verbleibenden Einträge der QUBO-Matrix Q, die zum quadratischen Anteil des QUBO-Problems gehören, werden genutzt, um Nebenbedingungen in unsere Zielfunktion zu integrieren. Wir erinnern uns, dass das Assignmentproblem noch die Bedingung enthält, dass die resultierende Kantenmenge ein Matching bildet, also keine zwei Kanten im Ergebnis einen Knoten teilen. Diese Bedingung lässt sich zwar nicht direkt an alle Ergebnisse des QUBO-Problems stellen; sie lässt sich aber so in den quadratischen Anteil des Problems übertragen, dass sie für alle optimalen und annähernd optimalen Lösungen des Problems gilt. Hierfür setzen wir einfach alle Einträge q_{ij} mit i≠j von Q, sodass die Kanten zu x_i und x_j einen Knoten teilen, auf einen hohen, positiven Wert. Die optimale Wahl dieses Strafwerts für die Nutzung von Quantum Annealing ist noch eine offene Frage; er sollte jedoch größer als alle vorkommenden Kantengewichte sein, damit Lösungen, die keinem Matching entsprechen, nicht nur suboptimal, sondern auch klar abgrenzbar von den zulässigen Lösungen sind.

Nun werden noch alle verbleibenden Einträge q_{ij} auf 0 gesetzt. Somit ist unsere Transformation des Assignmentproblems in eine QUBO-Formulierung abgeschlossen. Um diese QUBO-Formulierung tatsächlich auf einem Quantum Annealer von D-Wave nutzbar zu machen, müssen wir die QUBO-Matrix Q nun noch in eine Obere Dreiecksform bringen. Dies erfordert zwei einfache Schritte [4]:

1. Wir ersetzen alle Einträge q_{ij} von Q mit i<j durch $q_{ij}+q_{ji}$.
2. Wir ersetzen alle Einträge q_{ji} von Q mit i>j durch 0.

Somit haben wir eine vollständige Methode, ein beliebiges Assignmentproblem so umzuformen, dass eine Lösung mit Quantum Annealing oder einer anderen Lösungsmethode für QUBO-Probleme möglich ist.

Weitere Anwendungsmöglichkeiten und Ausblick

Zu Beginn dieses Beitrags haben wir mit dem Demand-Supply-Matching bereits eine in der industriellen Praxis relevante Anwendung des Assignmentproblems kennengelernt. Dies ist jedoch bei Weitem nicht das einzige praktisch vorkommende Problem, das als Instanz des Assignmentproblems verstanden werden kann. In der Industrie und außerhalb sind noch viele weitere Anwendungen denkbar, beispielsweise die Zuteilung von (in mittlerer Zukunft potenziell autonomen) Taxis auf Passagiere, die effiziente Aufteilung von Arbeitsschritten auf Arbeitskräfte oder auch die optimale Aufteilung von Büroarbeitsplätzen auf Mitarbeiter.

Es ist außerdem zu betonen, dass die Ergebnisse, die in diesem Beitrag vorgestellt wurden, bisher nahezu ausschließlich theoretischer Natur sind. Die Frage, wie performant die verfügbaren Quantum Annealer mit tatsächlichen Anwendungen sind, bleibt aktuell offen. Erste Tests mit einer verhältnismäßig kleinen (40 Kanten im Graphen ≙ 40 Qubits) Modellinstanz des oben zuletzt genannten Anwendungsfalls der Sitzplatzverteilung in einem Bürogebäude ergaben eher enttäuschende Ergebnisse bei einer reinen Nutzung eines Quantum Annealers, allerdings deutlich bessere Ergebnisse bei einer Nutzung des ebenfalls von D-Wave bereitgestellten Hybrid Solver Service, der Quantum Annealing mit klassischen Rechenmethoden kombiniert. Da die genaue Funktionsweise der Hybridmethode leider nicht öffentlich zugänglich ist, ist ein nächster Schritt der Versuch, eine eigene Implementierung für eine ähnlich performante hybride Methode zu entwickeln; ein möglicher Ansatz hierfür ist beispielsweise ein „Iterative Heuristic Solver", beschrieben von Rosenberg et al. [5].

Zuletzt bleibt noch zu erwähnen, dass, während sich dieser Beitrag ausschließlich mit Quantum Annealing beschäftigt, auch andere Quantentechnologien zur Lösung des Assignmentproblems eingesetzt werden könnten. Eine Implementierung mithilfe des Quantum Approximate Optimization Algorithm, kurz QAOA, ist zum Beispiel auch möglich und könnte ebenfalls erhebliche Vorteile gegenüber klassischen Lösungsmethoden liefern, sobald geeignete Quantencomputer mit ausreichend Qubits zur Verfügung stehen.

Referenzen: **[1]** IBM, „IBM Quantum," [Online]. Available: https://quantum-computing.ibm.com/services?services=systems. [Accessed 12 07 2021]. **[2]** D-Wave Systems, „Advantage | D-Wave Systems," [Online]. Available: https://dwavesys.com/d-wave-two%E2%84%A2-system. [Accessed 12 07 2021]. **[3]** R. Duan und S. Pettie, „Linear-Time Approximation for Maximum Weight Matching," Journal of the ACM, Bd. 61, Nr. 1, pp. 1-23, 2014. **[4]** F. Glover, G. Kochenberger und Y. Du, A Tutorial on Formulating and Using QUBO Models, arXiv:1811.11538 [cs.Ds], 2019. **[5]** G. Rosenberg, M. Vazifeh, B. Woods und E. Haber, „Building an Iterative Heuristic Solver for a Quantum Annealer," Computational Optimization and Applications, Bd. 65, Nr. 3, pp. 845-869, 2016.

Ruben Pfeiffer

Ruben Pfeiffer is studying Computer Science: Games Engineering at Technical University Munich (TUM). He is currently writing his Bachelor's thesis about „Solving Matching Problems with Quantum Annealing" at TUM and Infineon Technologies AG, in the team of Hans Ehm in Supply Chain Innovation.

Lilly Palackal

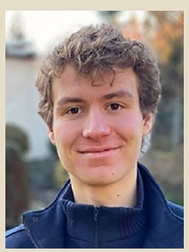
Lilly Palackal is an upcoming PhD student at Infineon Technologies AG in the team of Hans Ehm in Supply Chain Innovation working on Quantum Algorithms. She studied Mathematics at Technical University of Munich.

Hans Ehm

Hans Ehm studied Physics, Computer Science and Mechanical Engineering at HS Munich, Fernuni Hagen and Oregon State University. After various management and consulting positions in the semiconductor industry he is today responsible for Supply Chain Innovation at Infineon Technologies AG.

Maximilian Hess

Maximilian Hess is studying mathematics at Technical University Munich (TUM). He is currently writing his Master's thesis in the field of algebraic topology at TUM. He is working on quantum algorithms in the team of Hans Ehm in Supply Chain Innovation.



Fotos: Privat

Getting Civil Aviation Ready for the Post Quantum Age with LDACS

Daniel M. Mielke, Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganell
Deutsches Luft- und Raumfahrtzentrum e. V.

Digitisation has finally arrived in civil aviation: A new, feature rich communication, navigation, and surveillance system called LDACS is going to be deployed. An important aspect of LDACS is its cyber-security features. Since aeronautical equipment is used for long times, possibly decades, it is important to take future risks into account – including quantum computer driven cyberattacks. This article describes the first in-flight demonstration of Post-Quantum Cryptography in aviation on the basis of LDACS.

1 Introduction

Digital communications became a part of people's everyday life during the last years. However, in aviation, many communication tasks are still performed using analog voice radio – with all the disadvantages analog systems have. This includes comparatively low bandwidth efficiency, low sound quality (leading to potentially dangerous misunderstandings), and the lack of encryption and authenticity checks based on cryptography.

Although the intense growth of the aviation sector has been interrupted by the worldwide measures against the coronavirus, the trend to more modern aircraft collecting and exchanging more and more data is not stopped.

The L-band Digital Aeronautical Communications System (LDACS) is a digital system designed to bring aeronautical Communication, Navigation and Surveillance (CNS) into the 21st century. Especially on the physical layer, it makes use of modern communication techniques as they are used in established wireless communication systems like IEEE 802.11 ("Wifi") and the 4G phone network. LDACS will only be used for "operational" aeronautical communication i.e. it will be used for digital flight guidance, but not for passenger entertainment.

One critical aspect in operational aeronautical communications is security: How can it be ensured that confidential information is only received by authorised parties? How can the origin of a received message be verified? How is it guaranteed that a message has not been modified during transmission? While the first question addresses the cryptographic task of encryption, the second question addresses authentication, and the last question addresses integrity. These three properties are of high importance in a communication system whose messages directly affect flight guidance – especially in an environment where an increasing number of tasks is automated. This increasing level of automation is not the only ongoing development that motivates research on security in aeronautical communications: The broad availability of powerful computers and Software Defined Radios (SDRs) extends the circle of potential attackers on wireless systems in general and on the communication infrastructure of civil aviation in particular. This makes state-of-the-art cyber-security a must for digital aviation.

However, it has been shown that many widely used crypto-systems cannot be considered save anymore, once quantum computers with a sufficient amount of qubits become available. Hence, there is ongoing research on the topic of post-quantum security, i.e. cryptographic algorithms that are "immune" against quantum computer driven attacks.

Luckily, the breakthrough in quantum computation enabling massive attacks on current encryption schemes is not expected to happen tomorrow. Nevertheless, the development of post-quantum secure crypto-systems is already of high relevance – especially for systems used in environments with long technology life spans like civil aviation. Since LDACS is expected to be used for decades, there is a high chance, that sophisticated quantum computers may become available during its life time. Thus, before deploying a

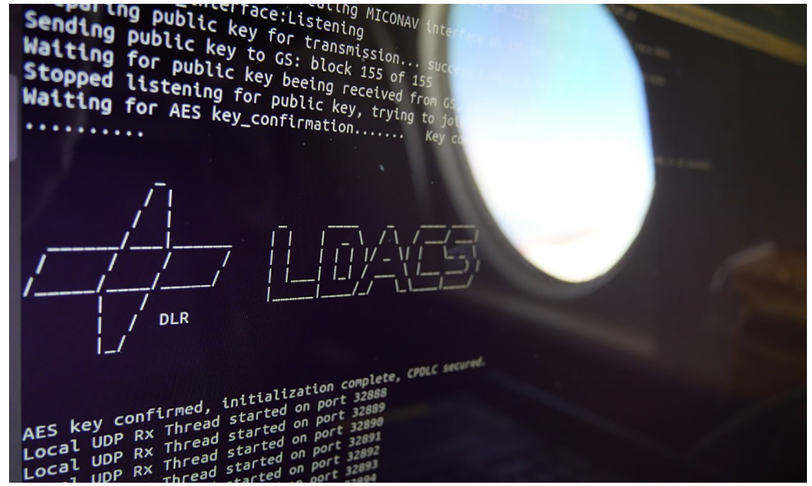


Figure 1: The result of a successful inflight McEliece encapsulated AES-256 key exchange shown on the terminal of the control computer aboard DLR's Falcon 20E research aircraft.

communication system that is used for critical infrastructure, it must be ensured that it can be operated securely for this duration.

2 Digital Flight Guidance with LDACS

LDACS is one of the radio access technologies realising the future aeronautical communications infrastructure that will allow aircraft to be digitally connected to the aeronautical telecommunications network (ATN) during all phases of flight [1]. Specifically, LDACS shall connect aircraft operating in the continental airspace by deploying a network of ground stations, each one of them covering a part of the airspace. An aircraft carrying an LDACS radio will then be able to connect to the ATN by communicating with the LDACS ground station covering its current location. In this way, it is similar to cellular mobile communication networks.

Technically, LDACS is a cellular broadband system based on Orthogonal Frequency-Division Multiplexing (OFDM) technology and supports quality-of-service while taking the requirements of aeronautical services into account [2]. It shares many technical features with 4G wireless communications systems. In addition to communication, LDACS supports navigation with its built-in ranging functionality.

Safety and security are deeply interrelated in aviation and flight guidance [3, 4]. For this reason, LDACS has been designed with a security architecture relying on state-of-the-art cryptography [5, 6, 7]. However, as we alluded to, this might not be good enough, if recent developments in Post-Quantum Cryptography (PQC) are not taken into account.

3 Post Quantum Cryptography

In general cryptography is "the mathematical science that deals with transforming data to render its meaning unintelligible, prevent its undetected alteration, or prevent its unauthorized use" [8], or in simpler terms: "Cryptography is loosely the science of encrypting and decrypting secret codes" [9]. Before we go into depth about "Post-Quantum Cryptography (PQC)", we would like to introduce some basic cryptographic operations and terms: First we want to introduce our two communication partners, Alice and Bob[1]. If Alice and Bob want to communicate securely with each other, Alice and Bob can encrypt a message and Bob can decrypt that message. If they want to use a symmetric crypto-system (e.g. Advanced Encryption Standard (AES) [10]), they first have to agree on such a shared secret. A symmetric crypto-system means, Alice and Bob use the same secret as the key to encrypt and decrypt messages. Agreeing on a shared secret over an insecure communication channel is hard and for that purpose key exchange protocols exist, e.g. Diffie-Hellman Key Exchange (DHKE) [11].

In asymmetric crypto-systems, like Rivest–Shamir–Adleman (RSA) [12], both Alice and Bob have each a public key and a private key. Thus Alice knows Bob's public key and Bob knows Alice' public key. If Alice wants to encrypt a message for Bob, she encrypts that message with Bob's public key and sends that message to Bob. Since Bob is the only person, that knows his private key, only he can decrypt that message.

Another important use of asymmetric crypto-systems are signatures, which can be used to digitally sign messages (e.g. via Digital Signature Algorithm (DSA) [12]) by one of the communication partners. If Alice wants to make sure, that Bob really believes, that she sent a message, she signs that message with her private key. Bob, and everyone else in possession of Alice's public key, can now verify that this message was actually sent by Alice.

The term "Post-Quantum Cryptography (PQC)" is used in the context of cryptography to describe the idea that an attacker has access to a quantum-computer, which can calculate the underlying mathematical problems much more efficiently than a classical computer [13]. Thus cryptographers divide cryptographic security levels in pre-quantum (no practical quantum-computer exists) and post-quantum (a practical quantum-computer does exist). The implication being, that some of today's most relevant cryptographic systems, that are secure in a pre-quantum world,

[1] Alice and Bob are generic names traditionally used to designate cryptographic communication partners.

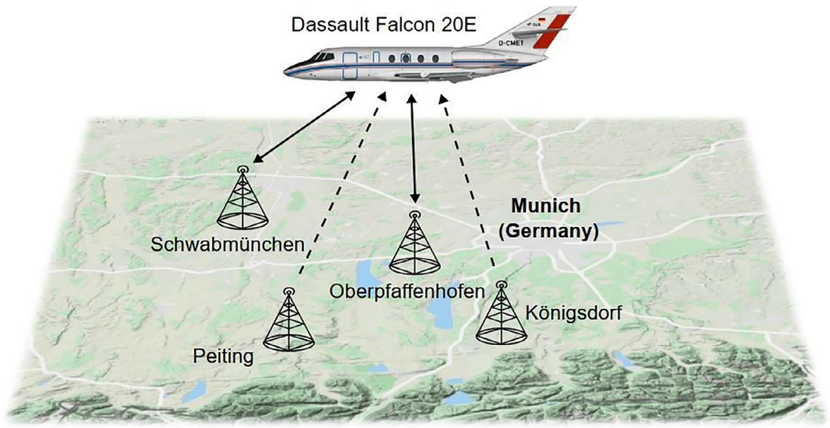


Figure 2: LDACS flight trials using four LDACS ground stations deployed in southern Germany and one LDACS airborne station carried by a Dassault Falcon 20E aircraft. Copyright of background map: Map data ©2020 GeoBasis-DE/BKG (©2009), Google. [22]

are no longer secure in a post-quantum world. The reason is, that these cryptographic systems' security is based on mathematical problems, that cannot be solved within in a reasonable amount of time using a classical computer. One famous example is the factorization of large integers that cannot be solved by non-quantum computers in any practical way. Thus, cryptographic systems making use of this property, like the RSA public-key system, are considered save (assuming a sufficient key length) while no quantum computers are available.

However, in 1994, Shor [14] introduced Shor's algorithm, which is a fast quantum algorithm to find the prime factorization of any positive integer [15]. Shor's algorithm applied to RSA and combined with a large enough quantum-computer would break RSA. Other cryptographic operations, such as the DHKE key exchange or the DSA signature scheme, or the elliptic curve variations of these schemes would be broken, as well [15].

In 1996, Grover introduced Grover's algorithm [16], which speeds up searching in unordered data-structures of size N from N operations to $\sqrt{N}$. Again applied with a large enough quantum computer, Grover's algorithm reduces the security level of the symmetric crypto-system AES with a key length of 128bit to 64bit in a post quantum world, thus effectively halving security levels.

Both attacks would require thousands logical and, due to faulty-behavior of qubits, millions of physical qubits [17]. To put his into perspective: In 2021 the IBM Quantum Eagle processor will launch with 127-qubits and IBM plans for a 1121-qubit IBM Quantum Condor processor in 2023 [18]. Both machines would be the most powerful public quantum-computers to date. With that, a million qubit machine could well be decades away [18].

In order to begin defending against the possible threat that quantum-computers pose to the world's most used crypto-systems, post-quantum robust crypto-systems are, however, currently being developed and standardised. Post-quantum crypto-systems are based on mathematical problems that are equally impractical to be solved by quantum computers and classical computers. The National Institute of Standards and Technology (NIST) started its standardisation work in

2017, in search for the most promising post-quantum crypto-systems in a series of three rounds [19]. One of the most promising candidates and finalist for public-key crypto-systems and key establishment algorithms is the McEliece crypto-system, that has been invented in 1978 [20].

Every computer and practically all digital communication systems use error correction codes to provide highly reliable services. A straightforward example is a repetition code, where every bit is sent three times to allow the correction of a single bit-flip during transmission (e.g. 0 1 → 000 111). There exist many other (and way more efficient) error correction codes like Reed-Solomon Codes, Convolutional Codes or Goppa Codes. The latter code class is an example for a code that is not only used for error correction, but that can also be used for encryption. This is called code-based cryptography. The security of the McEliece crypto-system is based on the NP-hard problem of decoding a general linear code like the Goppa Code. Currently, the major drawback of McEliece is its very large key size. For example, to reach a similar security level as AES-128, McEliece requires a key size of roughly 1MB. Encryption and decryption, however, are faster than with RSA [19].

In our flight trials, we used McEliece keys, that strongly benefited from advancements in key size reduction in recent years [21]. The key size could be reduced to 200kB. A successful key exchange is shown in Figure 1.

4 Flight Trials

After years of development and tests in the laboratory and through computer simulations, LDACS was ready to be demonstrated in flight trials in 2019. Within the German national project MICONAV[2], the German Aerospace Center (DLR), together with its project partners[3], conducted the first in-flight LDACS demonstration in March and April 2019 in Germany [22]. We employed four experimental LDACS ground stations and one experimental LDACS airborne station. In order to recreate the expected cellular deployment of LDACS, the four LDACS ground stations were distributed in the south-west of Germany, as it can be seen in Figure 2.

[2] Migration towards Integrated COM/NAV Avionics
[3] Rohde & Schwarz GmbH & Co. KG, Bo¨gl & Partner Systemtechnik GmbH, iAd – Gesellschaft fu¨r Informatik, Automatisierung und Datenverarbeitung GmbH, Technical University of Munich

(a)LDACSGroundStation (b)LDACSGroundAntenna (c)LDACSAircraftStation

Figure 3: Overview of ground and airborne LDACS equipment. [23]

Figures 3a to 3c show the LDACS ground station located in the DLR premises in Oberpfaffenhofen and the LDACS airborne station, respectively. The airborne station was installed into the Dassault Falcon 20E DLR research aircraft shown in Figure 4.

The flight trials, which consisted of six flights over two consecutive weeks, allowed us to conduct numerous experiments addressing the communication, navigation, and surveillance capabilities of LDACS. Through these experiments, we were able to demonstrate that LDACS can support applications relevant to air traffic management, such as Controller–Pilot Data Link Communications

(CPDLC) communications, audio streaming, as well as general-purpose data transmission and broadcast. Basically, data were generated by the different applications running on laptops connected to either the ground station or the airborne station. The generated data were transmitted over LDACS to its counterpart station, therefore enabling the applications to communicate with each other and to recreate future ATM procedures.

5 Post-Quantum Aeronautical Communication

The cryptographic protocol used in the MICONAV project follows the common approach of using a combination of an asymmetric and a symmetric crypto-system. The applied proof-of-concept consists of three parts:

- The exchange of public keys between Ground Station (GS) and Aircraft Station (AS), denoted by PubKeyGS and PubKeyAS, respectively.
- The (asymmetrically encrypted) sharing of a secret session key KAES.
- The confirmation of this session key.

The first two parts of the protocol are visualized in Figure 5 in more detail. The mutual exchange of the public keys is performed in step 1) and 2): Both communication partners, i.e. GS and AS, generate their respective McEliece key pair (one private key and one public key) before they send their public key to the other partner. In step 3), the AS generates a random key of length 256bit called session key KAES. This key is then encrypted with the public key of the GS using the McEliece scheme as shown in step 4). Then, the encrypted session key is sent to the GS. Step 5) shows how the GS receives the encrypted key and decrypts it using its private key PrivKeyGS. Finally, the GS stores the decrypted session key KAES. Both communication partners share a secret KAES although this secret has never been transmit in clear-text.

Additionally, we have also implemented a confirmation protocol which guarantees that both parties use the same key [24]. The protocol is based on using a randomly generated number-usedonce "nonce" and a timestamp that are encrypted using the KAES. By mutually exchanging this information, both communication partners can verify that the same session key is used. From now on, all data exchanged between AS and GS can be symmetrically encrypted using the session key KAES. In MICONAV, the AES crypto-system was used for this purpose using a key length of 256bit.

The described implementation is a first proof-of-concept and not ready for deployment yet. The key exchange as shown in Figure 5 is vulnerable to Man-in-the-Middle (MITM) attacks: Imagine, an attacker would infiltrate all communication between GS and AS starting from the very first step by acting as the AS with respect to the actual GS while acting as the GS with respect

Figure 4: DLR's research aircraft Dassault Falcon 20E (D-CMET) used in the experiments. [23]

to the actual AS. In the current setup, neither the actual AS nor the actual GS have a chance to realize this MITM attack and the attacker has access to the symmetric keys – and consequently to all messages encrypted using these keys. This vulnerability can be addressed by performing a signed key exchange; however this requires at least some pre-shared information like certificates. Another option would be to perform the exchange of the public keys in advance via a secure side channel, e.g. smart cards. This would also simplify the protocol in Figure 5, since the first two steps could be skipped.

6 Summary

Critical communication systems like the L-band Digital Aeronautical Communications System (LDACS) discussed in this article are potentially used for decades. It is important to take foreseeable cyber-security threats into account that may arise in this time. A particular threat that is expected to materialise within the next decade, is the threat of quantum computers rendering many state-of-the-art cryptography systems vulnerable. We strive therefore to introduce post-quantum secure cryptography into aviation.

In a first step of getting civil aviation ready for the post-quantum age, we demonstrated McEliece cryptography for aeronautical communications in flight. The flights performed in the MICONAV project were the first time that an LDACS demonstrator was flown aboard an aircraft, confirming the expected performance of LDACS, and demonstrating post-quantum cryptography in aviation for the first time.

Clearly, the results presented in this article are just the first step in realising our vision of postquantum secure aviation, and much work remains to be done. However, our results demonstrate that if recent advances in cryptography and aeronautical communication systems are combined, the goal is already within reach.

Abbreviations

AES	Advanced Encryption Standard
AS	Aircraft Station
CNS	Communication, Navigation and Surveillance
CPDLC	Controller–Pilot Data Link Communications
DHKE	Diffie-Hellman Key Exchange
DSA	Digital Signature Algorithm
GS	Ground Station
LDACS	L-band Digital Aeronautical Communications System
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
RSA	Rivest–Shamir–Adleman
SDR	Software Defined Radio

References: **[1]** M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger. LDACS: Future Aeronautical Communications for Air-Traffic Management. Communication Magazine, 52(5):104–110, May 2014. **[2]** T. Gräupl, C. Rihacek, and B. Haindl. LDACS A/G Specification. SESAR2020 PJ14-02-01 D3.3.030, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, August 2019. **[3]** M. Slim, B. Mahmoud, A. Pirovano, and N. Larrieu. Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey. Computer Science Review, 1112:1–29, May 2014. **[4]** Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. On perception and reality in wireless air traffic communication security. IEEE transactions on intelligent transportation systems, 18(6):1338–1357, 2016. **[5]** Mäurer, N. and Bilzhause, A. A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS). In 37th Digital Avionics Systems Conference (DASC), pages 1–10, New York, NY, USA, Sept. 2018. IEEE. **[6]** N. Mäurer and C. Schmitt. Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis. In 19th Integrated Communications, Navigation and Surveillance Conference (ICNS), pages 1A2/1–1A2–13, New York, NY, USA, Apr. 2019. IEEE. **[7]** Mäurer, N., Gräupl, T. and Schmitt, C. Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS. In 39th Digital Avionics Systems Conference (DASC), pages 1–10, New York, NY, USA, Oct. 2020. IEEE. **[8]** Robert Shirey. RFC 4949 - Internet security glossary, version 2. Technical report, IETF, August 2007. **[9]** Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, and Gerhard Rosenberger. A course in mathematical cryptography. Walter de Gruyter GmbH & Co KG, 2015. **[10]** Daemen Joan and Rijmen Vincent. The design of rijndael: Aes-the advanced encryption standard. In Information Security and Cryptography. springer, 2002. **[11]** Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE transactions on Information Theory, 22(6):644–654, 1976. **[12]** Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978. **[13]** Daniel J Bernstein. Introduction to post-quantum cryptography. In Post-quantum cryptography, pages 1–14. Springer, 2009. **[14]** Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science, pages 124–134. Ieee, 1994. **[15]** Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. Nature, 549(7671):188– 194, 2017. **[16]** Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219, 1996. **[17]** Earl T Campbell, Barbara M Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. Nature, 549(7671):172–179, 2017. **[18]** Jay Gambetta. Ibm's roadmap for scaling quantum technology, 2021. [Online]. Available: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/ [Accessed: January 15, 2021]. **[19]** Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. US Department of Commerce, NIST, 2020. **[20]** Robert J McEliece. A public-key cryptosystem based on algebraic. Coding Thv, 4244:114–116, 1978. **[21]** Hannes Bartz and Gianluigi Liva. On decoding schemes for the mdpc-mceliece cryptosystem. In SCC 2019; 12th International ITG Conference on Systems, Communications and Coding, pages 1–6. VDE, 2019. **[22]** Miguel A. Bellido-Manganell, Thomas Gräupl, Oliver Heirich, Nils Mäurer, Alexandra FilipDhaubhadel, Daniel M. Mielke, Lukas Marcel Schalk, Dennis Becker, Nicolas Schneckenburger, and Michael Schnell. LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System. submitted to IEEE Transactions on Aerospace and Electronic Systems, 2021. **[23]** Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganell, Daniel M. Mielke, Alexandra Filip-Dhaubhadel, Oliver Heirich, Daniel Gerbeth, Michael Felux, Lukas Marcel Schalk, Dennis Becker, Nicolas Schneckenburger, and Michael Schnell. Flight Trial Demonstration of Secure GBAS via theL-band Digital Aeronautical CommunicationSystem (LDACS). IEEE Aerospace and Electronic Systems Magazine, pages 1–19, 2021. **[24]** M. Fischlin, F. Gu¨nther, B. Schmidt, and B. Warinschi. Key confirmation in key exchange: A formal treatment and implications for tls 1.3. In 2016 IEEE Symposium on Security and Privacy (SP), pages 452–469, 2016.

Ground Station (GS)		Aircraft Station (AS)
1 :		Generate McEliece AS Key Pair: $PrivKey_{\mathrm{AS}}$ and $PubKey_{\mathrm{AS}}$
		Store $PrivKey_{\mathrm{AS}}$ and transmit $PubKey_{\mathrm{AS}}$
	$PubKey_{\mathrm{AS}}$ ←	
Receive and store $PubKey_{\mathrm{AS}}$		
..... GS knows public key of AS		
2 : Generate McEliece GS Key Pair: $PrivKey_{\mathrm{GS}}$ and $PubKey_{\mathrm{GS}}$		
Store $PrivKey_{\mathrm{GS}}$ and transmit $PubKey_{\mathrm{GS}}$		
	$PubKey_{\mathrm{GS}}$ →	
		Receive and store $PubKey_{\mathrm{GS}}$
..... AS knows public key of GS		
3 :		Generate and store session key K_{AES} of length 256 bit
4 :		Encrypt K_{AES} using $PubKey_{\mathrm{GS}}$
	encrypted K_{AES} ←	
5 : Receive encrypted K_{AES}		
Decrypt encrypted K_{AES} using $PrivKey_{\mathrm{GS}}$		
Store session key K_{AES}		
..... AS and GS share session key K_{AES}		

Figure 5: Exchange of the session key KAES secured by the McEliece scheme as implemented in MICONAV

Daniel M. Mielke M.Sc.

Daniel M. Mielke received his B.Sc./M.Sc. from University of Kiel in 2014/2016 and spent a term at the UBC in Vancouver. He joined DLR in 2016. His research interests are channel modeling and robust wireless communication systems in aviation. He is a PhD candidate at the University of Ulm.

Nils Mäurer M.Sc.

Nils Mäurer has been working as a cybersecurity researcher at the Institute of Communications and Navigation (KN) for the German Aerospace Center (DLR) since 2017. He is currently researching the cybersecurity design of LDACS, the datalink for future terrestrial aviation communications.

Dr. Thomas Gräupl

Thomas Gräupl received the Ph.D. degree in computer science from the University of Salzburg, Austria in 2011. He is a researcher with the institute of communications and navigation of the German Aerospace Center DLR.

Miguel A. Bellido-Manganell

Miguel A. Bellido-Manganell, in DLR since 2016, is contributing to the further development of LDACS and leading the LDACS Air-to-Air Mode design. His research interests include channel modelling, digital signal processing, spectrum compatibility, and medium access for aeronautical ad hoc networks.

Fotos: Deutsches Luft- und Raumfahrtzentrum e. V., Privat

The Quantum What? Advantage, Utopia or Threat?

Michel Barbeau[1], Erwan Beurier[2], Joaquin Garcia-Alfaro[3], Randy Kuang[4], Marc-Oliver Pahl[5] and Dominique Pastor[6]

[1]Carleton University, [2,5,6]IMT Atlantique, [3]Institut Mines-Telecom, [4]Quantropi Inc.

Introduction

Quantum computing is at the top of the agenda for several countries. They acknowledge its strategic importance. They invest significant public funds in the development of this technology. While some show unconditional enthusiasm, others are more moderate and even very critical with respect to the promises of quantum computing. It is not easy to navigate for a non-expert in the field. Does quantum computing have a real advantage or is it rather a utopia? Is quantum computing a threat to cybersecurity? With a non-expert point of view, this article sheds light on these questions. We consider quantum computing as an advantage, a utopia, or a security threat. We look at applications that we think are promising. We review the efforts made by participants engaged in the race for the quantum computer. Finally, we project ourselves into the future.

An Advantage?

In the 1980s, Richard Feynman suggested using the properties of quantum physics to compute chemical interactions at the molecular scales. In the 1990s, the interest in quantum computing increased significantly thanks to Shor's algorithm (Shor 1994). With this algorithm, a quantum computer can rapidly solve a large class of cryptology problems. Standard asymmetric encryption methods used to protect communications can potentially become highly vulnerable. The so-called quantum advantage or quantum supremacy refer to the ability of quantum computers to solve complex problems much faster than classical computers (Preskill 2012). Shor's algorithm is the best-known example Another contribution of importance is Grover's algorithm. In an unsorted list of items, it speeds up the search for a specific element. It is an elementary operation that can accelerate several programs. Furthermore, the quantum advantage may refer to conducting operations that have no analogue in classical computing, e.g., merging multiple quantum states into one of higher quality (Leone et al. 2021).

Some believe that a genuine quantum computer with 50 qubits would achieve quantum supremacy. Some estimations increase that number to, at least, hundreds of qubits (Choi 2020, Dalzell et al. 2020). Computers with such a high number of qubits could achieve computations requiring several thousands of years on today's fastest supercomputer.

Quantum computing is a complex technology. Quantum computers of intermediate size, composed of only a few physical qubits have already been developed by IBM, Google, and Rigetti. They are limited. The realization of a universal quantum computer that can achieve any type of quantum calculation and outperforming any current supercomputer is not expected before 2030.

A Utopia?

Not everyone shares the optimism about quantum computing. It is making extraordinary claims. Extraordinary claims require extraordinary evidence. According to (Dyakonov 2018, 2020), a useful quantum computer requires between 1,000 to 100,000 qubits. Current quantum computers are extremely vulnerable to errors that happen due to noise or manufacturing imperfections. This challenge is not clearly tackled. The quantum threshold theorem states that physical error rates below a certain level can logically be solved using error-correction algorithms. As often in mathematics, this theorem relies on several assumptions that seem unrealistic because they need to be exactly verified. Entanglement – the inherent connection of different qubits - makes the effect of errors even worse than in traditional computing today. An error in a qubit implies a cascade of other errors in related qubits. To counter the noise effects, error-correcting codes are required at the lowest level of the computer. The issue is then that achieving efficient error-correcting codes becomes more difficult as the number of qubits increases.

Shor's algorithm is one of the reasons why there is interest in quantum computing. The initial integer factorization algorithm requires a tremendous number of quantum gates, around 72n3 to factorize an n-bit number. And yet, most of the companies that claim to have realized a quantum computer use it as a test of their computing capabilities. Actually, they use a compiled version of the algorithm that drastically reduces the number of gates by knowing the factorization to compute. One could see this as plain cheating. Thus, even if quantum computing is a promising technology, it seems mainly driven by optimism. Dyakonov argues that, albeit solid technological attempts, the quantum computing fervor is nearing its end; much energy and money were put into it for little results so far. But there is hope: recent research dramatically improved the number of qubits required for integer factorization (Gidney and Ekerå 2021).

The development of a quantum computer is extremely challenging. It requires overcoming several technical issues. The realization of two qubits with the same nominal behavior requires a high level of reproducibility of several physicochemical parameters because we want those multiple runs of the same program output the same results. The current mass production technologies are insufficient to guarantee such a reproducibility for a high qubit volume.

Qubits interact with their environment. Superposition of qubit states eventually disappears. This unavoidable phenomenon is called decoherence. The decoherence time is crucial to control. It represents the time during which we can benefit from the superposition of the two possible states of a qubit to achieve several computations at the same time.

The efficiency of quantum computers relies on their ability to use few qubits to deal with large amounts of data. Unfortunately, there is currently no known method to efficiently transcribe a large set of data into a single quantum state. For problems involving large amounts of data, the initialization of a quantum computer becomes dominating in time over the computation. This significantly reduces the quantum advantage.

Clearly, these challenges are of different nature. Overcoming them will require cooperation between various fields of expertise, such as computer science, complexity theory, quantum physics, mathematics, systems engineering, process engineering, and materials. Such a cross-fertilization may be difficult to setup. On the one hand, we have physicists who are motivated by scientific knowledge, discovery, and experimentation. On the other hand, we find computer scientists and electronic engineers who reckon that technical achievements are possible without full knowledge of the underlying physics and who, therefore, may underestimate and even neglect fundamental issues of importance.

A Security Threat?

Shor recently raised awareness about complacency over Internet security (Castelvecchi 2020). The strength of Diffie-Hellman and Elliptic Curve Cryptography relies on the discrete-logarithm problem. The security of Rivest, Shamir and Adleman (RSA) depends on the problem of factoring large numbers. Due to recent advances in quantum computing, the security of classical Public Key Infrastructure (PKI) is at risk. Shor's algorithm provides an exponential speedup in breaking it. In 2019, Google declared quantum supremacy with their Sycamore 54-qubit quantum computer (Arute 2019). In 2020, Wang et al. made a milestone on prime factorization with the D-Wave annealing quantum computer (Wang et al. 2020). They successfully factorized into prime numbers all numbers up to 10 000. D-Wave paves the way to a new cracking strategy for PKI. It may be closer to cracking practical RSA than a general-purpose quantum computer running Shor's algorithm. The commercial availability of quantum computers, especially the quantum annealers, shakes the foundations of contemporary information security.

Applications

One of the first applications of the quantum technology is its use to secure classical data. Leveraging the laws of quantum physics, Bennett and Brassard proposed the Quantum Key Distribution (QKD) protocol (Benn 84). QKD has been widely explored resulting in a variety of implementations and improvements (Giampouris 2017). Despite its name, QKD is in fact a key expansion protocol. Its operation relies on a companion authenticated classical channel. It is not a complete solution, a barrier to its adoption. Other barriers include the need for special hardware. It cannot run over the classical Internet. Furthermore, although theoretically secure, QKD is vulnerable to several practical attacks (National Security Agency 2020).

Machine learning is another application of quantum computing whose interest is growing (Biamonte et al. 2017). Phenomena unique to the quantum level, such as entanglement, could make quantum computers learn things that classical computer cannot. Another potential advantage is to make the time complexity of classification independent of the number of data points. Quantum machine learning is a situation where large amounts of data are involved. The setup and initialization of quantum machine learning are preponderant in time over the computation, thus reducing the quantum advantage. Quantum machine learning is promising but requires further research.

Quantum-resistant routing is another positive outcome of the quantum challenge. It has inspired researchers into modeling new threats against the quantum Internet (Kimble 2008, Wehner et al. 2018). The main goal is to achieve secure and sustainable quantum repeaters (Satoh et al. 2020). Classical information-oriented attacks, such as those compromising confidentiality, seem to have less of a hold over quantum information. The non-cloning theorem of quantum mechanics reframes secrecy related issues.

The Quantum Race

We make a world tour of initiatives and investments in quantum computing. The Quantum Manifesto prompted European states to establish a strategy to maintain Europe at the forefront (Collective 2016). This was deemed crucial to avoid dependence on a single technological path that could result from a concentration of expertise in China and USA. Quantum computing became a priority for the European Union (EU) with an advanced strategy and funding scheme. The EU invested 550 M€ in quantum computing research from 1997 to 2017. The EU started a Future and Emerging Technologies action on quantum communication, sensing, computers, and simulators.

The roadmap is having QKD in systems for inter and intra-city communication in 2023. The goal is to achieve by 2027 quantum Internet links across distances longer than 1000 kms. By 2023, they aim to achieve quantum computers with error correction outperforming physical qubits, and in 2027 quantum algorithms outperforming classical computers. For quantum simulation, the objective is to achieve by 2027 a quantum advantage in solving important problems in science, demonstrate quantum optimization, and realize prototype solving problems beyond supercomputer capability, for application domains such as quantum chemistry, new material design. The roadmap for quantum sensing and metrology is, for 2023, integrated quantum sensors, imaging systems and metrology standards at the prototype level; and in 2027 transition from prototypes to commercially available devices. In October 2018, the European Commission launched the Quantum Technologies Flagship with a 1 B€ budget for ten years to support the transformation of research into commercial applications exploiting the potential of quantum technologies.

In parallel, EU countries set up their own initiatives. France aims to acquire a general-purpose quantum computer. In 2021, France launched the Quantum Plan and announced a public-private investment of 1.8 B€ in quantum technology, over five years (Frésillon 2021, Gouvernement Français 2021), with public investments of 200 M€ per year leading to the creation of three interdisciplinary quantum information institutes (Le Monde 2021). The strategy builds upon public-private sector partnerships, flagship research regions, and training with new graduate programs. Startups are supported, which is another strategy to increase technological advance. There are seven focus areas. Their monetary attributions in parenthesis give an idea of the prioritization: i) developing and disseminating the use of Noisy Intermediate Scale Quantum (NISQ) simulators and accelerators (352 M€), ii) developing the Large Scale Quantum computer (432 M€), iii) developing quantum sensor technologies and applications (258 M€), iv) developing the post-quantum cryptography offer (156 M€), v) developing quantum communication systems (325 M€), vi) developing a competitive enabling technology offering (292 M€), and vii) structuring the ecosystem across the board.

As emphasized in (Forteza et al. 2020), to anticipate the advent of quantum computing and benefit completely from this technology once it is mature, a challenge is to disseminate its use and practice and, more generally, to teach quantum computing in priority sectors, such as chemistry, logistics, artificial intelligence, pharmacology, materials, fertilizers, catalysts, and logistics finance. Several French companies are investing in the field. For instance, Électricité de France (EDF) and Total set up programs dedicated to quantum computing in collaboration with the startup Pasqal, specialized in programmable quantum simulators and quantum computers composed of 2D and 3D atomic arrays.

The Atos company program reflects the strategies of involved companies. Launched in 2016, it aims to make available the benefits of the already existing NISQ technology. In particular, the Atos Quantum Learning Machine provides a simulation environment for developers, training, build use cases and assess quantum implementation benefits. Atos collaborates with national players such as Grand Equipement National de Calcul, the Commissariat à l'Energie Atomique and Pasqal. It is desirable that other private stakeholders emerge to help anticipate the possible breakthrough and advent of quantum technologies in an open and highly competitive economy.

In the vein of recommendations in (Forteza et al. 2020), the emergence of other European competitors will help avoid too much dependence of Europe on a single private partner. In addition, in a market economy, companies face challenges and adopt strategies that do not always align with the governmental ones. They may fluctuate according to market developments. This challenges the ability of countries to protect their scientific and technological heritage as well their advances achieved through public financial support.

Germany invests 100 M€ per year in quantum computing, with an overall funding of 650 M€ between 2018 and 2022 (Bundesministeriums für Bildung und Forschung 2018, 2021). In 2021, a further investment of 1.1 M€ had been announced. Germany favors four directions: quantum computers, quantum communication, quantum-based measurement technology, and enabling technologies for quantum systems. The focus is on developing the quantum technology research landscape, creating research networks for new applications, flagship projects with the industry, sovereignty, international collaboration, and getting the commitment of the population. Showing the importance of the strategy, the research organizations involved in the enacting of the plan include all major German actors such as German Research Foundation, Max Planck society, Fraunhofer society, Helmholtz Association, Leibniz Association, National Meterology Institute, Federal Office for Information Security, and Agency for Innovation in Cybersecurity.

In 2013, the United Kingdom (UK) was the first European country to announce a quantum strategy, investing 370 M€ over five years and creating in 2018, a national center aimed at developing a quantum computer. In June 2019, UK announced an additional £153 M investment on quantum, together with a £205 M commitment from industry. In early 2020, the Netherlands announced that about 23.5 M€ will be invested in quantum technologies over the next five years. Quantum technologies in Spain are being promoted by public-private partnerships, including large multinational companies such as Telefónica (telecommunications) and Hispasat (satellites), research centers such as Institute of Photonic Sciences and Spanish National Research Council, and start-up initiatives such as Quside, Multiverse Computing, and Qilimanjaro Quantum Tech. Investment plans are expected to grow from 20 M€, for the period 2015-2017, to 400 M€, for the period 2021-2027. An aim is to promote quantum solutions in financial, pharmaceutical, automotive, and aeronautical sectors (Ametic 2019).

In the USA, coordination of quantum research started in October 2014. Since 2018, research and development in this area is a national priority by the National Quantum Initiative Act. The plan is to inject $1.2M in development of quantum information systems over the next decade (INRIA 2020). Over five years, $625M will be invested in five research centers across the country. Furthermore, the USA private sector and academia are contributing an additional $340M to these research centers.

The Big Tech are at the forefront in the soaring of quantum computing in the USA, with especially Google, IBM and Microsoft leading the way by striving to make the technology emerge via tremendous investments in it. Ultimately, big-data, artificial intelligence and quantum computing are to meet for such companies to maintain their leadership in the digital world. Google has been developing its own quantum computer and announced in August 2020 that its computer Sycamore had performed the first-ever quantum simulation of a chemical reaction. At the same time, IBM claimed that its quantum computer handled 64 qubits. Microsoft is developing technology on topological quantum computing and has developed its own open-source quantum programming language Q#. Behind the Big Tech, it is worth mentioning the existence of companies such as the Canadian D-Wave with a new generation of quantum computer and the American startup Rigetti, which announced in August 2020 that it had raised $79M to support the development of a 128-qubit computer.

While it has invested over $1B over the last decade (National Research Council Canada 2017), Canada has announced a $360M budget over seven years, starting in 2021, to support its National Quantum Strategy (Department of Finance Canada 2021). It emphasizes training of qualified personnel and development of job opportunities in the area. Historic strengths of Canada are cryptography, Information and Communications Technology (ICT) and photonics.

China is quickly catching up with the construction of a $10B national laboratory dedicated to quantum information science. China's leading quantum research group announced in December 2020 that their computer Jiuzhang attained the quantum supremacy (Conover 2020, Zhong et al. 2020), with a computation that took 200 seconds whereas the world fastest non-quantum computer would have needed 600 million years to achieve the same result. China is thus the second country achieving quantum supremacy, after the USA with Google's Sycamore (Conover 2019). This achievement is of prime importance. The technology is based on photons, a technology that seemingly received less attention than others, whereas Sycamore relies on superconducting materials conducting energy without resistance and not light.

The private Chinese company Alibaba launched in 2015 its Quantum Computing Laboratory aimed at producing a prototype of a general-purpose quantum computer involving 50 to 100 qubits by 2030. The company has also invested $15B in artificial intelligence and quantum research. In 2018, the search engine Baidu announced the creation of the Institute of Quantum Computing. Tencent set up a lab dedicated to scientific research in quantum computing.

An Obstacle Race

From a very general point of view, two main issues could slow down the successful realization of private and public plans. A first issue is the lack of skills in the quantum computing job market. This may affect the dissemination, use and practice of quantum practice. In contrast to machine learning, the number of computer engineers and scientists familiar with quantum computation is very limited. It is necessary to significantly increase the skills of engineers and scientits in quantum computing to speed up its diffusion.

A second issue for Western countries is their dependence on the most advanced producers of semiconductors. Specifically, qubits out of silicon are among the most robust available (Gonzalez-Zalba et al. 2019, Petit et al. 2020). This allows for maintaining a sufficiently long decoherence time to benefit from superposition and thus parallelization. The development of silicon-based quantum computers could furthermore leverage the previous infrastructure investments in microchip technology to maintain low-level production costs. The ambition of many countries is to explore the silicon path by relying on their strong research and industrial experience in microelectronics, as well as the pertaining industrial facilities. Semiconductors have thus become the new oil in a global economy dominated by the tensions between China and the USA. For several months now, we have been aware of a shortage of semiconductors already affecting the video game, automotive, communication industries, among others. Since the European semiconductors industry has dropped significantly over the last ten years to end up with merely 10% of the market share, we easily understand why the EU aims to boost Europe's position in the semiconductor market. If the chip war continues and intensifies, it may jeopardize programs and schedules established by governments and industries.

Conclusion

Countries invest in quantum computing to maintain their technological advance. One may not expect the race to result into a definite winner, but rather to maintain a technological advancement equilibrium across leading countries. We are facing a very risky technology that opens many uses, some possibly yet unthinkable because new algorithms will emerge from current and future research. Nobody can reasonably predict how quantum technology will evolve.

Various aspects of the quantum technology have already proved to be feasible. For more than twenty years, researchers and industrialists have come up with realistic methodological plans, achieved findings with potential high impacts, and succeeded in elaborating the very first generations of quantum computers and sensors. The literature on the topic shows that researchers and industrialists are capable of continuously adapting to deal with unforeseen issues. On the other hand, the same literature puts forward that the technology is ambitious, with the potential to have a high scientific, technological, economical, and even societal impact. For sure, quantum technology entails much uncertainty and unpredictability. Quantum technology is a high-risk high-gain technology. The issue is thus not whether researchers and industry will be able to provide various tech-

nological bricks or not. They will! Even in case of failures, the amount of work achieved will provide --- and has already opened --- new research paths that contribute to the classical technology of computers communications and cybersecurity.

Quantum computing is an incentive to classical computer science. As mentioned by Chao-Yang Lu who co-authored (Zhong et al. 2020) "It's a continuous competition between constantly improved quantum hardware and constantly improved classical simulation" (IQT News 2020). For example, very rapidly after Google announced that its quantum computer Sycamore had reached quantum supremacy, IBM claimed to have developed a supercomputer capable of simulating the 54-qubit Sycamore circuits and performing the same tasks.

Above all the technical advances in quantum computing, the main issue remains political. There is a short list of stakeholders that are strong enough to support a sufficiently long-term investment in this high-risk, high-gain technology. As in martingale pricing, such will probably get the expected significant return on their investment. In this respect, we currently have two types of major stakeholders. On the one hand, two countries are noticeably key players, namely, China and the USA. These countries keep on funding research and application of quantum computing, simply because it is well accepted that the country that will lose the race for innovation will fall. On the other hand, we have industrial stakeholders, that include Google and Microsoft, two of the GAFAM, as well as Alibaba, Baidu and Tencent, three of the BATX. Among the major stakeholders in quantum computing, we find data rich countries and leaders in artificial intelligence. Otherwise said, big data, artificial intelligence and quantum technologies are poised to meet each other and merge. Major players in artificial intelligence invest tremendous amounts of money in quantum technology, positioning them ipso facto as leaders of the digital world. For instance, Microsoft is fully playing the game of the high-risk high-gain technology. It is one of the few players addressing topological quantum technology. This technology is in its infancy. The feasibility of topological qubits is not demonstrated yet. However, Microsoft Station Q is a research group fully dedicated to this field. Topological quantum computing is expected to be more stable and robust to noise than standard quantum computing.

Where do we go from here?

For countries, research institutions and industrials other than the unrivalled few, what can be done to avoid becoming digital colonies of two main leaders of the digital world? There is probably no other choice than continuing research on the topic for mainly political reasons. Indeed, it is crucial for countries to keep some independence, at least on niches that may provide prominent advantage on some aspects and trigger further cooperation.

The sanitary crisis put forward the importance of supporting research in pharmacology, biology, and personalized therapy. A - perhaps too simple - point of view could be that research in such areas should prevail at the expense of quantum computing. However, quantum computing is expected to help model chemical reactions at the molecular scale, thus making possible the study of interactions between proteins and medicine. So, instead of choosing between pharmacology, biology and quantum computing, a possible way involves combining them. If we cannot win the race and become leaders on quantum computing, we can still become key stakeholders on topics requiring hybridization of two or more research areas including some specific aspects of quantum computing. Hybridization and interdisciplinary research seem unavoidable, simply because quantum computers are not aimed at replacing standard computers or supercomputers. The quantum computer is akin to a co-processor, tailored to speed up specified computations such as simulations in meteorology or the prediction of a protein folding. Albeit highly desirable, hybridization and interdisciplinary advancement will depend on our research and industrial tissues and organizations. International cooperation is beneficial to attain the critical mass required to play this high-risk, high-gain game. International cooperation is strongly conditioned by our ability to smooth out respective ways to handle and support research, development, and innovations.

It is worth emphasizing that sustainability and ecological issues are poorly addressed in the literature on the topic. What is the carbon footprint of research in quantum computing? Can we expect that this technology, once it is mature, render our world more sustainable thanks to its capacity to carry out computations that would otherwise consume our planet? For Pan Jianwei, one of Jiuzhang's designers, the answer is clear since he deems that Jiuzhang discovery means a gain in computing capacity without an increase in energy consumption, in contrast to supercomputers, which are very energy intensive.

If the quantum technology holds its promises, we can expect decisive advantages in chemical and physical simulations that should induce applications with high impact in agriculture, drug discovery and battery design. It could contribute significantly to environmental preservation by reducing the energy footprint of fertilizer production, leading to substantial savings and helping reduce the ecological impact of the food industry.

This technology may also allow speed-ups in optimization and machine learning applications, including finance, energy, automotive, traffic improvement, environmental sciences, actions against global warming, with possibly new processes for efficient CO2 recycling, or even the identification of early warning signs of natural disasters with quantum sensors embedded in satellites.

Several researchers, engineers and scientists highly involved in this technology reckon that it could potentially affect every aspect of our everyday life. Great! But current quantum computers are devoted to very specific tasks of relatively poor practical interest with respect to the expectations. The general-purpose quantum computer is not for tomorrow.

What will be the environmental price integrated over all these years before the technology is mature, deployed and meets all the expectations? Once the technology reaches maturity, will we not be tempted to carry out even more calculations to the point where the possible gain in sustainability brought by quantum computing could finally be cancelled out? The way is long, but the camel is patient and watchful. What is your opinion? Is Quantum Computing a utopia, an advantage, or a threat?

References **Ametic (2019). AMETIC** (Asociación de empresas de electrónica, tecnologías de la información, telecomunicaciones y contenidos digitales) impulsa el ecosistema de tecnologías cuánticas para lograr un país más competitivo. Online: https://ametic.es/es/prensa/ametic-impulsa-el-ecosistema-de-tecnologias-cuanticas-para-lograr-un-pais-mas-competitivo **Arute, F., Arya, K., Babbush, R. et al.** (2019). Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510. **Bennett, C. H. and Brassard (1984),** G. Quantum cryptography: Public key distribution and coin tossing. in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York. **Biamonte, J. et al.** (2017). Quantum machine learning. Nature 549, 195–202. **Bundesministeriums für Bildung und Forschung** (2018). Quantentechnologien – von den Grundlagen zum Markt. Online: https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf **Bundesministeriums für Bildung und Forschung** (2021). BMBF erhält rund 1,1 Milliarden Euro aus dem Konjunkturpaket zur Förderung der Quantentechnologien. Online: https://www.bmbf.de/files/2021-05-11_102%20PM_F%c3%b6rderung%20von%20Quantentechnologien.pdf **Collective** (2016). Quantum Manifesto. Online: https://time.tno.nl/media/7638/quantum_manifesto.pdf **Castelvecchi, D.** (2020), Quantum-computing pioneer warns of complacency over Internet security, Nature, Volume 587, p. 169. **Choi, C. Q.** (2020), How Many Qubits Are Needed for Quantum Supremacy? Whether Google achieved quantum supremacy depends on perspective, IEEE Spectrum, Online: https://spectrum.ieee.org/tech-talk/computing/hardware/qubit-supremacy **Conover, E.** (2019). Google officially lays claim to quantum supremacy. Online: https://www.sciencenews.org/article/google-quantum-computer-supremacy-claim **Conover, E.** (2020). The new light-based quantum computer Jiuzhang has achieved quantum supremacy. ScienceNews. Online: https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy **Dalzell, A. et al.** (2020). How many qubits are needed for quantum computational supremacy? Quantum, 4, pages 264, Online: https://doi.org/10.22331/q-2020-05-11-264 **Department of Finance Canada** (2021), A Recovery Plan or Jobs, Growth, and Resilience – Budget 2021, Online: https://www.canada.ca/en/department-finance.html **Dyakonov, M.** (2018), The Case Against Quantum Computing, IEEE Spectrum, Online: https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing **Dyakonov, M.I.** (2020). Will We Ever Have a Quantum Computer?. Swiss: Springer International Publishing. **Forteza, P., Herteman and J.-P., Kerennidis, I.** (2020). Quantique: Le virage technologique que la France ne ratera pas, Online : https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf **Frésillon, C.** (2021). French research at the heart of the Quantum Plan. CNRS News. Online: https://news.cnrs.fr/articles/french-research-at-the-heart-of-the-quantum-plan **Giampouris D.** (2017). "Short Review on Quantum Key Distribution Protocols". Adv Exp Med Biol; 988:149-157. **Gidney, G. and Ekerå, M** (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433. **Gonzalez-Zalba, F. Yang, T.-Y. and Rossi. A.** (2019). Manufacturing silicon qubits at scale, physicsworld. Online: https://physicsworld.com/a/manufacturing-silicon-qubits-at-scale/ **Gouvernement Français** (2021). 1,8 M € en faveur des technologies quantiques. Online: https://www.gouvernement.fr/18-m-eu-en-faveur-des-technologies-quantiques **INRIA** (2020). Quels sont les principaux acteurs de l'informatique quantique ? Online: https://www.inria.fr/fr/acteurs-informatique-quantique **IQT News** (2020). China's Photonic Computer Jiuzhang Achieves Quantum Supremacy. Inside Quantum Technology. Online: https://www.insidequantumtechnology.com/news-archive/chinas-photonic-computer-jiuzhang-achieves-quantum-supremacy/ **Kimble, H. J.** (2008). The quantum Internet, Nature, vol. 453, pp. 1023–1030. **Le Monde** (2021). Emmanuel Macron veut mettre la France dans le trio de tête mondial des technologies quantiques. Online : https://www.lemonde.fr/politique/article/2021/01/21/emmanuel-macron-presente-un-plan-quantique-de-1-8-milliard-d-euros-sur-cinq-ans_6067037_823448.html **Leone, H. et al.** (2021). QuNet: Cost vector analysis & multi-path entanglement routing in quantum networks, Online: https://arxiv.org/abs/2105.00418 **National Research Council Canada** (2017). Quantum Canada – Survey overview, Online: https://nrc.canada.ca/sites/default/files/2019-03/Quantum_Canada_Report_e.pdf **National Security Agency – Central Security Service** (2020), Quantum Key Distribution (QKD) and Quantum Cryptography (QC), Online: https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/. **National Institute of Standards and Technology** (2016). NIST Post-Quantum Cryptography Competition. Online: https://csrc.nist.gov/projects/post-quantum-cryptography **Petit, L., Eenink, H.G.J.,** Russ, M. et al. Universal quantum logic in hot silicon qubits. Nature 580, 355–359 (2020). **Preskill, J.** (2012). Quantum computing and the entanglement frontier. Online: https://arxiv.org/abs/1203.5813 **Satoh, T. et al.** (2020). Attacking the Quantum Internet. arXiv preprint. Online: https://arxiv.org/pdf/2005.04617 **Schiermeier, Q.** (2019). Russia joins race to make quantum dreams a reality. Online: https://www.nature.com/articles/d41586-019-03855-z **Shor, P.W.** (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134. **Collective** (2016). Quantum Manisfesto. Online: https://time.tno.nl/media/7638/quantum_manifesto.pdf **Wang, B., Hu, F., Yao, H. et al** (2020). Prime factorization algorithm based on parameter optimization of Ising model. Sci Rep 10, 7106. **Wehner, D. et al.** (2018). Quantum internet: A vision for the road ahead. Science, vol. 362, no. 6412. **Zhong, H.-S. et al.** (2020). Quantum computational advantage using photons. Science, December, 1460-1463.

Prof. Dr. Michel Barbeau

Michel Barbeau is a professor of Computer Science at Carleton University, Canada. He got a Ph.D., in Computer Science (Universite de Montreal 1991). Specific research interests include underwater communications and networks, flying drone networks, quantum networks and network control systems.

Dr. Erwan Beurier

Erwan Beurier is a recently graduated Doctor in Mathematics from IMT Atlantique, France. He studied artificial intelligence, complexity and logic. His PhD thesis at the interface of biology, category theory and statistics won him the Prize of the best thesis of the Fondation Mines-Télécom 2021.

Prof. Dr.-Ing. Joaquin Garcia-Alfaro

Joaquin Garcia-Alfaro is a professor of Computer Science. He got a PhD (Université de Rennes, France '07) and a research Habilitation (Université Pierre et Marie Curie, France '13) in Computer Science. He is full professor and research axis leader at Télécom SudParis, Institut Mines-Télécom, France.

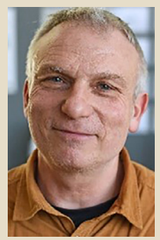
Dr. Randy Kuang

Randy Kuang holds a doctorate in quantum physics. His research findings have been published in top international. He co-founded inBay Technologies in 2009. Randy is a prolific inventor, with 30+ U.S. patents in broad technology fields. He is presently Chief Scientist at Quantropi Inc.

Dr. Marc-Oliver Pahl

Marc-Oliver Pahl heads the Chair Cybersecurity for Critical Networked Infrastructures at the Technical University IMT Atlantique in Rennes, France. He is an adjunct professor of Carleton University in Canada. Marc-Oliver's research focus is on a holistic approach to cybersecurity.

Prof. Dr. Dominique Pastor



Dominique Pastor got an engineering degree (Telecom Bretagne, France, 1986), a PhD (University of Rennes, France, 1997) and a research habilitation (Université de Bretagne Occidentale, '07). He is full Professor at IMT Atlantique. His current research focuses on mathematical models of resilience.

Fotos: Privat

Vielversprechend: Monte-Carlo-ähnliche Methoden auf dem Quantencomputer

Carsten Blank[1], Francesco Petruccione[2]
[1]data cybernetics, [2]University of KwaZulu-Natal

Klassische Monte-Carlo-Simulationen besitzen eine Varianz Var(X)/N mit der zugrunde liegenden zu simulierenden Zufallsvariable X. Nun wird berichtet, dass eine quadratische Verbesserung der Konvergenz und eine von X unabhängige Varianz möglich ist, wenn die Simulation auf einem Quantencomputer durchgeführt wird. Wir wollen aufzeigen, wie dieser Vorteil der Quantum Computer möglich ist, und damit Einblick geben, was wir zu erwarten haben.

Motivation & Kontext

Die alles bestimmende Frage, welche jeder Aussage einer Quanten-Überlegenheit vorweggenommen werden muss, sollte am besten gleich zu Anfang angesprochen werden, um nicht den Eindruck zu vermitteln, man sei realitätsfern auf seinem Elfenbeinturm verhaftet. Jedem brennt die eine Frage unter dem Nagel: Werden wir bald in den Genuss dieser neuen Kraft kommen können? Das Forschungslabor der IBM in Zürich, Goldman Sachs und die Universität von Maryland, USA, haben sich dieser Frage angenommen und die Anzahl von (fehlertoleranten) Qubits sowie der Operationen für die Bepreisung einer Option (TARF Derivate) berechnet und sie der Rechenzeit gegenübergestellt, in der man nach heutigen Maßstäben rechnen möchte: 1 Sekunde[1]. Dieses ergab, dass die Rechengeschwindigkeit der teuersten Operationen bei 10MHz liegen muss, jedoch wird derzeit angenommen, dass lediglich 10kHz erreicht werden können[2].

Es besteht aus dieser Sicht Zweifel an der Anwendbarkeit, und doch sollte man gerade im Bereich neuer Technologien vorsichtig sein, denn der Stand der Technik ändert sich rasant. In der Zwischenzeit – also bevor „richtige“ Quantencomputer mit hunderten fehlertoleranten Qubits zur Verfügung stehen – ist man bestrebt, Algorithmen zu finden, welche explizit jetzige oder nächste Generationen von Quantenprozessoren nutzen möchten. Diese werden auch NISQ (Noisy Intermediate Scale Quantum) Prozessoren genannt[3].

Nicht ohne Grund hat sich das oben genannte Konsortium ein Problem ausgesucht, das eine Monte-Carlo-Simulation als Grundlage hat. Diese Methode ist ein in Industrie und Wissenschaft häufig eingesetztes stochastisches Verfahren zur nummerischen Approximation wichtiger Kennzahlen. Durch Mittelwertbildung über eine sehr große Anzahl an zufällig generierten Experimenten ermöglichen sie eine Schätzung der gesuchten Größe.

Wie effizient und präzise diese Approximation ist, wird durch die Varianz der zugrunde liegenden Zufallsvariable und die Stichprobengröße bestimmt. Um die Präzision der Schätzung zu verbessern, versucht man häufig, die Varianz der verwendeten Zufallsvariable zu reduzieren, ohne dabei das Ergebnis der Durchschnittsbildung zu verändern. Eine der bekanntesten Methoden ist der Metropolis–Hastings-Algorithmus, welcher in die Klasse Variance-Reduction-Methoden fällt.

In der Tat haben sich in letzter Zeit gleich mehrere Fachbeiträge dem Thema Monte-Carlo-ähnlicher Methoden für Quantencomputer angenommen [4–8]. Daraus ergibt sich die These, dass die Berechnung von Erwartungswerten unter Transformationen sich quadratisch besser approximieren lassen, als es für klassische Computer der Fall ist. Diese Erkenntnis scheint auf einer sehr wichtigen Eigenschaft der Quantenmechanik zu fußen, der Quantenverschränkung. Im Quantum Computing gibt es zwei wesentliche und sehr bekannte Algorithmen, die die theoretische Überlegenheit von Quantenberechnungen in den 1990er-Jahren belegten, die Primfaktorzerlegung[9,10] und das effizientere Suchen einer Datenbank[11]. Es ist damit nicht verwunderlich, dass beide Prinzipien in diesem Trick genutzt werden, namentlich die Amplitude Amplification[12].

Methode	Fehler	Algorithmen auf Quanten Prozessor	Anzahl Experimente
Amplitude Estimation	$\lvert\mathbb{E}[f(X)] - \tilde{a}\rvert \leq \frac{\sqrt{3}}{M}$	M	*
Ein-Qubit-Messung	$\lvert\mathbb{E}[f(X)] - \tilde{e}\rvert \leq \frac{1}{2\sqrt{N}}$	1	N
Monte-Carlo[1]	$\lvert\mathbb{E}[f(X)] - \tilde{e}\rvert \leq \frac{Var(f(X))}{\sqrt{N}}$	0	N

Tabelle 1: Der Vergleich der Fehler. Die ersten beiden Einträge sind Quantenalgorithmen, die letzte ist die bekannte Monte-Carlo-Methode, ohne Varianzreduktion. Die Amplitude Estimation* muss nur ein paar Mal ausgeführt werden, um bei einer Erfolgswahrscheinlichkeit von π^2/8 statistische Sicherheit zu erhalten, wohingegen beide andere Verfahren N Mal wiederholt werden. Man sieht hier recht eindrucksvoll, dass Quantenalgorithmen einen Vorteil bringen können.

Jedoch stellt sich die Frage, wie lässt sich diese „quadratische“ Quantenüberlegenheit denn mit klassischen Algorithmen vergleichen? Dies lässt sich jedoch so direkt nicht beantworten. Beispielsweise könnte man die Anzahl der Anwendungen der Simulationsalgorithmen für den klassischen und auch den quantenartigen Fall ermitteln und diese dann mit der erreichten Präzision in Relation setzen. Diese Ansicht ist allerdings nicht unumstritten. Während im klassischen Verfahren mit jeder einzelnen Anwendung der Simulation eine Realisation erzielt wird, lädt Quantenalgorithmus die vollständige Verteilung in den Quantenzustand. Man sieht also schon hier, dass eine direkte Vergleichbarkeit nicht gegeben ist.

In unserer Arbeitsgruppe wurde gezeigt[7], dass mit Monte-Carlo-ähnlichen Methoden auf dem Quantencomputer nicht nur die oben genannte Amplitude Estimation, sondern ebenso eine Ein-Qubit-Messung als Alternative genutzt werden kann, die konsequenterweise keine quadratische Verbesserung der Präzision mit sich bringt. Eine der Behauptungen dieser Arbeit ist jedoch, dass Quantenalgorithmen für Monte-Carlo-ähnliche Methoden eine Varianzreduktion erreichen können, in der Tat wird die Varianz einer Bernoulli-Verteilung identifiziert. Was bedeutet dies aber konkret? Klassische Monte-Carlo-Simulationen besitzen die Varianz Var(X)/N mit der zugrunde liegenden Zufallsvariable X, die simuliert wird. Nun wird berichtet, dass die Varianz unabhängig von X ist, wenn die Monte-Carlo-Simulation auf dem Quantencomputer durchgeführt wird.

Wir zeigen, dass dieses faszinierende Detail in der Tat für beide Ansätze gleichermaßen gilt, der Anwendung der Amplitude Estimation mit dem quadratischen Vorteil und der Ein-Qubit-Messung für heutige fehlerhafte Quantenprozessoren. Die Konsequenzen dieser Erkenntnis würden viele Industrien berühren, an denen hoch-komplexe Monte-Carlo-Modelle berechnet werden. Dazu gehören Wettermodelle, Chemische Reaktionen, Medizinische Forschung, Finanzen & Märkte, Versicherungen und Logistik, um ein paar zu nennen.

Wir wollen mit steigender Komplexität den Leser in die Höhle der Quantenalgorithmen locken. Die Einführung sollte die wichtigsten Aussagen beinhalten, um eine Idee zu bekommen, was Quantencomputer für die Berechnung von Erwartungswerten machen können und wie realistisch dies auch ist. Das nächste Kapitel soll es mit dem Wissen über Quantenalgorithmik noch gemächlich angehen, jedoch unsere Kernaussage – die der quadratischen Konvergenzsteigerung und der Varianzreduktion – mit mehr Mathematik untermauern. Wir wollen nicht in den Algorithmus der Amplitude Estimation tauchen, denn das sprengt diesen Bericht bei Weitem. Das darauffolgende Kapitel geht deutlich tiefer in die Quantenalgorithmik und zeigt auf, wie man konkret einen vergleichsweise einfachen – aber nicht trivialen – diskreten stochastischen Prozess auf einem Quantencomputer modelliert. Dieses Kapitel ist für all jene, die eine Idee brauchen, um in den Ansatz Vertrauen zu gewinnen. Das letzte Kapitel widmet sich der Zusammenfassung sowie der Diskussion und soll für den interessierten Leser wieder verständlich sein.

Der Quantenvorteil beim Monte-Carlo-Sampling

Nun wollen wir einige der obigen Aussagen präzisieren. Sei X eine Zufallsvariable und eine Transformation f:R→R, dann wissen wir

$$\left|\mathbb{E}[f(X)] - \frac{1}{N}\sum_{i=1}^{N} f(X_i)\right|^2 \leq \frac{Var(f(X))}{N} \qquad (1)$$

wobei wir X_i (i=1…N) als identisch und unabhängige verteilte

[1] Ohne das Variance Reduction Methoden angewandt wurden.

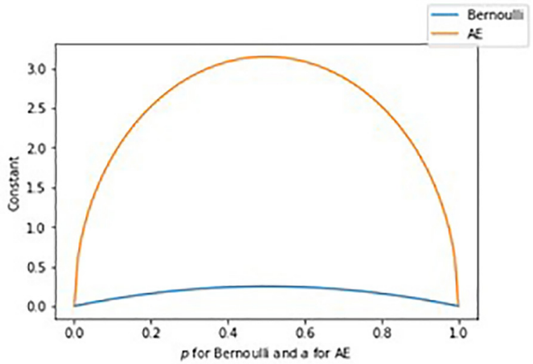


Abbildung 1: Die Konstanten bei der Bernoulli-Verteilung haben ihr Maximum bei p=1/2 mit C=0.25 und für die Amplitude Estimation liegt das Maximum ebenfalls bei a=1/2 und zwar bei C=3. Beim AE sind zudem Annahmen bei M=2^{10}, k=1.

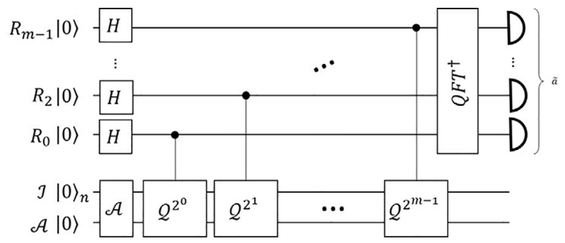


Abbildung 2: Der Quantenschaltkreis für Amplitude Estimation, wobei Q=$AS_0A^{-1}S_f$ mit Reflektionen S_0,S_f, siehe[12] für Details. Relevant ist hier einzig die Anzahl der Anwendungen von A: 2^{m+1}+1 mal, sprich M^2+1, da $M=2^m$ gilt.

Irrfahrt	Zustand	Amplitude	Wahrscheinlichkeit
-1, -1	$\|\mathbf{0}\rangle\|\mathbf{0}\rangle$	$\frac{1}{\sqrt{2}}\sqrt{q_2}$	$\frac{1}{2}\cdot q_2$
-1, +1	$\|\mathbf{0}\rangle\|\mathbf{1}\rangle$	$\frac{1}{\sqrt{2}}\sqrt{1-q_2^2}$	$\frac{1}{2}\cdot(1-q_2)$
+1, -1	$\|\mathbf{1}\rangle\|\mathbf{0}\rangle$	$\frac{1}{\sqrt{2}}\sqrt{1-p_2^2}$	$\frac{1}{2}\cdot(1-p_2)$
+1, +1	$\|\mathbf{1}\rangle\|\mathbf{1}\rangle$	$\frac{1}{\sqrt{2}}\sqrt{p_2}$	$\frac{1}{2}\cdot p_2$

Tabelle 2: Nach zwei Schritten sind die Wahrscheinlichkeiten für die Irrfahrt korrekt wiedergegeben.

Zufallsvariablen mit derselben Verteilung wie X annehmen. Die Summe ist lediglich der approximierte Wert, welcher durch die Monte-Carlo-Simulation ermittelt wird, mit N Simulationen. Die Aussage, die sich nun hinter den Arbeiten von Montanaro[4], Rebentrost et al.[5], und Wörner et al.[8,13,14] verbirgt, ist, dass dieser Fehler

$$|\mathbb{E}[f(X)] - \tilde{a}|^2 \leq \frac{C}{M^2} \qquad (2)$$

beträgt, wobei $\tilde{a}$ die Messung nach der Amplitude Estimation[12] beziffert. Mit etwas Rücksicht auf die Tatsache bezogen, dass N und M zwei unterschiedliche Bedeutungen haben, legt dies dennoch nahe, dass es eine Methode gibt, die die Anzahl von Anwendungen des Monte-Carlo-Algorithmus reduzieren kann. Die Sache ist selbstverständlich nicht offensichtlich, denn was wirklich passiert, ist, dass m neue Auslese-Qubits in das System eingeführt werden und es $M = \mathcal{O}(2^m)$ Anwendungen des Monte-Carlo-ähnlichen Algorithmus gibt, mit dem Messfehler wie in Gleichung (2) beschrieben. So wird die Anzahl von Anwendungen miteinander verglichen, und zwar auf sehr unterschiedlichen Architekturen. Dennoch macht dies Sinn, obwohl man diesen Hintergrund nicht vergessen sollte.

Die Frage, die in diesem Zusammenhang noch nicht erklärt wurde, ist nun, wie sieht ein Monte-Carlo-Algorithmus aus, welcher auf einem Quantencomputer ausgeführt wird? Dazu wurden Arbeiten in den letzten Jahren verfasst[7,8,13,14], welche Konstruktionen unter Anwendungen erklären. Der einfachste Erklärungsansatz umfasst, dass die Zufallsvariable X auf k>0 Werte diskretisiert wird und mit der Wahrscheinlichkeitsdichte in einen Quantenzustand gebracht wird. Anschließend wird die Transformationsfunktion f auf ein extra Qubit angewandt, sodass die Anwendung der Amplitude Estimation die Summe aus Wahrscheinlichkeiten und der Transformationsfunktion „ausgelesen“ wird. Konkret sei die Wahrscheinlichkeitsdichte $p(i) = \mathbb{P}[X' = x_i]$ $(x_i \in \{0, \dots, k-1\})$ der diskretisierten Zufallsvariablen X berechnet, wodurch ein Quantenzustand

$$\mathcal{R}|0\rangle_n = |\psi\rangle = \sum_{i=0}^{k-1} \sqrt{p_i}|i\rangle \qquad (3)$$

erzeugt wird. Sodann wird ein neues Qubit hinzugefügt, auf dem im Anschluss eine Operation ausgeführt wird, welche den vorherigen Zustand überführt in

$$F|\psi\rangle|0\rangle = \sum_{i=0}^{k-1} \sqrt{p_i}|i\rangle\left(\sqrt{1-f'^{(i)}}|0\rangle + \sqrt{f'^{(i)}}|1\rangle\right) \qquad (4)$$

mit $f'(i) = f(x_i)$, sodass $\mathcal{A} = F\mathcal{R}$ eine Anwendung des Algorithmus ist. Die Anwendung der Amplitude Estimation schätzt den Wert $a = \langle\Psi_1|\Psi_1\rangle$ mit $|\Psi_0\rangle = \sum_{i=0}^{k-1}\sqrt{p_i}\sqrt{1-f'^{(i)}}|i\rangle|0\rangle$, $|\Psi_1\rangle = \sum_{i=0}^{k-1}\sqrt{p_i}\sqrt{f'^{(i)}}|i\rangle|1\rangle$ somit gibt es die orthogonale Zerlegung $F\mathcal{R}|0\rangle_n|0\rangle = |\Psi_0\rangle + |\Psi_1\rangle$. Anstatt Amplitude Estimation anzuwenden, wurde eine NISQ freundliche Alternative aufgewiesen[7], indem man eine Ein-Qubit-Messung auf dem letzten Qubit durchführt und die Wahrscheinlichkeit schätzt, in der der Zustand 1 vorkommt. Nun wollen wir zeigen, dass in diesen beiden Mess-Ansätzen auch ein weiterer Quanteneffekt in der Berechnung von Erwartungswerten auftritt: eine Varianzreduktion unabhängig von der Varianz der Zufallsvariablen X oder deren Diskretisierung X‘.

Betrachten wir die Gleichung (4) und führen eine Ein-Qubit-Messung z.B. mit einer Pauli $\sigma_z = P_1 + P_{-1} = |0\rangle\langle 0| - |1\rangle\langle 1|$ Observablen durch. Nur das Ergebnis -1 interessiert uns, sodass wir die Observable P_{-1} etwas genauer betrachten. So erhalten wir

$$\begin{aligned}\langle P_{-1}\rangle = Tr(|1\rangle\langle 1|\mathcal{A}|0\rangle_{n+1}) &= \sum_{i=0}^{k-1} p_i f'^{(i)} \\ &= \sum_{i=0}^{k-1} f(x_i)\mathbb{P}[X' = x_i] \\ &= \mathbb{E}[f(X')] \\ &\approx \mathbb{E}[f(X)]\end{aligned} \qquad (5)$$

Jedoch ist die Varianz dieser Messung nicht abhängig von der Zufallsgröße X‘ , wie es für Monte-Carlo-Methoden der Fall wäre. Stattdessen gilt die Varianz der Observablen P_{-1}. Für die zugehörige Zufallsvariable Y_P der Messung gilt nämlich

$$Y_P \sim Ber(p) \qquad (6)$$

mit $p = \mathbb{E}[f(X')]$, daher $Var(Y_P) = \Delta P_{-1} = p(1-p)$. Dieses recht einfache Ergebnis resultiert aus $\langle P_{-1}^2\rangle = 0^2(1-p) + (-1)^2 p = p$ und somit $\Delta P_{-1} = \langle P_{-1}^2\rangle - (\langle P_{-1}\rangle)^2 = p - p^2 = p(1-p)$. Vergleichend mit Gleichung (1) ist offensichtlich, dass die Statistiken der Zufallsgrößen X oder deren diskretisierte Zufallszahl X‘ keinerlei Einfluss haben.

Diese Tatsache gilt ebenso für die Amplitude Estimation, wie durch Gleichung (2) deutlich gemacht. Die Konstante C>0 ist ebenfalls unabhängig von diesen beiden Zufallsvariablen, konkret gilt C=2πj√(a(1-a))+(j^2 π^2)/M, für jedes beliebige j>0. Man betrachte die Abbildung 1, welche die Konstanten beider Methoden zeigt. Zusammenfassend gibt die Tabelle 1 eine Übersicht.

Quantum-Brute-Force für eine Irrfahrt

Wir sehen aus diesen Überlegungen, dass Quantencomputer vor allem in einer Sache großartig sind: große Summen zu bilden [15]. Diese Eigenschaft ist gerade in der Berechnung von Erwartungswerten hilfreich, wie wir gerade gesehen haben. Nicht umsonst wurde der vorgeschlagene Ansatz „Quantum-Brute-Force“[7] genannt, denn man encodiert die gesamte Zufallsvariable, also alle möglichen Realisationen und deren Wahrscheinlichkeiten. Doch jeder, der Monte-Carlo-Methoden bereits angewandt hat, weiß zu berichten, dass gerade das Fehlen dieser Möglichkeit die Methode attraktiv macht. Hier besteht größtenteils die Problematik des Quantenansatzes. Die nötigen Werte der Wahrscheinlichkeitsdichte in Quantenzustände zu übertragen, kann für sehr komplexe diskrete Zufallsvariablen so groß sein, dass die sog. State Preparation[16–20] die realistische Anwendung unmöglich machen würde. Konkret bedeutet dies, dass für die Erstellung des Zustandes (3) auch eine von der Zahl N abhängige Anzahl elementarer 2-Qubit-Quantengatter (c-not) angewandt werden muss. Um dieses Problem jedoch zu umgehen, gibt es interessante Ansätze: variationelle Methoden[21–24], generative Methoden[25] und konstruktive Methoden[7,15,26]. Variationelle Methoden bedienen sich eines Quantum-Klassisch Hybridalgorithmus, um meist durch ein Gradienten-Verfahren nah an die gewünschte Verteilung zu kommen. Ähnlich sind generative Methoden zu verstehen, jedoch wird hier der Fokus auf Deep Learning-Netzwerke gelegt, insbesondere deren Quantum-Varianten.

Aus eigener Praxis stellen wir eine konstruktive Methode vor[7]. Anhand eines Beispiels soll erläutert werden, wie eine sog. korrelierte Irrfahrt erzeugt wird.

Definition: Eine korrelierte Irrfahrt X_n ist ein diskreter stochastischer Prozess und besitzt folgende Eigenschaften.
$\mathbb{P}[X_1 = +1] = \mathbb{P}[X_1 = -1] = \frac{1}{2}$ sowie
$\mathbb{P}[X_n = +1|X_{n-1} = +1] = p_n, \mathbb{P}[X_n = -1|X_{n-1} = +1] = 1 - p_n$
und
$\mathbb{P}[X_n = -1|X_{n-1} = -1] = q_n, \mathbb{P}[X_n = +1|X_{n-1} = -1] = 1 - q_n$
für Folgen $q = (q_2, q_3, q_4, \dots), p = (p_2, p_3, p_4, \dots)$.

Nun wollen wir den Prozess bis zu einer Länge n>1 als Wahrscheinlichkeitsdichte berechnen, es gibt daher $\leq 2^n$ Pfade. Da dieser

Prozess autokorreliert ist, insbesondere für den Spezialfall q=p gilt $\mathbb{E}[(X_n - X_{n-1})(X_{n+m} - X_{n+m-1})] = (2p-1)^m$, siehe Enriquez[27]. Somit ist die Berechnung von der Wahrscheinlichkeitsdichte nicht trivial. Mit einer Monte-Carlo-Simulation lassen sich natürlich Realisierungen und deren Wahrscheinlichkeiten errechnen, und die Definition gibt die Regel an, wie die Vorwärtssimulation durchgeführt werden muss. Diese Idee kann nun elegant in einen Quantenalgorithmus umgesetzt werden. Es bedarf für die Länge n dieselbe Anzahl an Qubits und der erste Schritt wird durch ein Hadamard-Gatter in die Superposition gebracht

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \qquad (7)$$

Wir identifizieren den Grundzustand mit dem Inkrement -1, behaften diesen mit der Amplitude $1/\sqrt{2}$, welches der Wahrscheinlichkeit 1/2 entspricht, und identifizieren analog den angeregten Zustand mit +1. Nun führen wir ein weiteres Qubit und kontrollierte Rotationen (um die y-Achse) ein, sodass die Wahrscheinlichkeiten den q_2,p_2 entsprechen. Dadurch erhalten wir

$$\begin{aligned} H|0\rangle|0\rangle &= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle \\ &\to \frac{1}{\sqrt{2}}|0\rangle\left(\cos\theta_{q_2}|0\rangle + \sin\theta_{q_2}|1\rangle\right) \\ &\quad + \frac{1}{\sqrt{2}}|1\rangle\left(\cos\theta_{p_2}|0\rangle + \sin\theta_{p_2}|1\rangle\right) \end{aligned} \qquad (8)$$

sodass $\cos\theta_{q_2} = \sqrt{q_2}$ und $\sin\theta_{p_2} = \sqrt{p_2}$. Würden wir nun Messungen auf beide Qubits anstellen und deren Statistiken sammeln, so würden nach Tabelle 2 die Werte ermittelt.

Man möge sich kurz klar machen, wie diese Konstruktion funktioniert, dann argumentieren wir, dass man dieses Verfahren auch n-Mal wiederholen kann. Einen Quantenschaltkreis könnte man ebenfalls einfach beschreiben, siehe Abbildung 3.

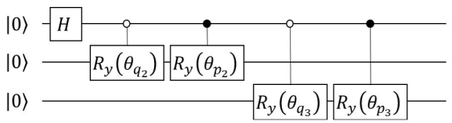


Abbildung 3: Die ersten drei Schritte auf einem Quantenschaltkreis dargestellt.

Nach n Schritten haben wir daher 2^n Äste des Quantenzustands, der Basisvektor zeigt daher auf, wie die Irrfahrt aussieht. Ein Beispiel: Gegeben sei der Basisvektor |01001100101011111011011⟩ so können wir die Irrfahrt ablesen, sie lautet

-1,+1,-1,-1,+1,+1,-1,-1,+1,-1,+1,-1,+1,+1,+1,+1,-1,+1,+1,-1,+1,+1

und in Summe haben wir 5. Mit diesem Verfahren ist es daher möglich, die Wahrscheinlichkeiten zu erzeugen, die passend sind zu dem stochastischen Prozess.

Um das Verfahren abzuschließen, zeigen wir zudem auf, wie man Gleichung (4) bzw. Operator F erzeugen kann. Dazu weisen wir auf ein Verfahren hin[7], welches ermöglicht, die charakteristische Funktion zu berechnen. Zuerst wird ein Akkumulator-Qubit in das System hinzugefügt. Wir erinnern uns, in jedem Schritt wurde eine Rotation angewandt (außer der ersten, dort nutzten wir ein Hadamard-Gatter). Nun nutzen wir ein kontrolliertes Phasengatter vom ersten Qubit – bedingt auf dem Grundzustand – und dem Akkumulator-Qubit als Ziel, mit der Aktion, eine relative Phase -1 zu erzeugen. Ein analoges kontrolliertes Phasengatter – nun bedingt auf den angeregten Zustand – soll die relative Phase +1 auf dem Ziel-Qubit erzeugen. Wiederholen wir dieses Verfahren nun auf allen Qubits, so stellen wir fest, dass wir eine Summe der einzelnen Realisationen von X_1,X_2,…,X_n in der relativen Phase haben. Für unser obiges Beispiel aus Gleichung (8) erhalten wir

$$\begin{aligned} &\frac{1}{\sqrt{2}}\cos\theta_{q_2}|00\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i(-1-1)}\right) \\ &+\frac{1}{\sqrt{2}}\sin\theta_{q_2}|01\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i(-1+1)}\right) \\ &+\frac{1}{\sqrt{2}}\cos\theta_{p_2}|10\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i(+1-1)}\right) \\ &+\frac{1}{\sqrt{2}}\sin\theta_{p_2}|11\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i(+1+1)}\right) \end{aligned} \qquad (9)$$

Mit einer Pauli X Messung erhält man nun $\mathbb{E}[\cos X_n]$ und mit einer Pauli Y Messung $\mathbb{E}[\sin X_n]$. Man kann nun folgendes tun: Mit $\varphi_{X_n}(v) = \mathbb{E}[\cos(vX_n)] + i\mathbb{E}[\sin(vX_n)]$ können wir das charakteristische Polynom errechnen, wenn wir je v ∈ R zwei Experimente ausführen. Das Ergebnis nach Konvergenz, welche unabhängig von der Varianz von X_n ist, kann man der Abbildung 4 entnehmen. Damit kann man zeigen, dass die Methode durchaus auf heutigen Prozessoren anwendbar ist. Zu Details verweisen wir auf unsere Arbeit[7].

Zusammenfassung & Diskussion

Wir halten daher zunächst fest, dass Quantencomputer hervorragend sind, wenn es um die Berechnung von großen Summen geht. Jedoch müssen Zustände erzeugt werden, die einen großen Aufwand mit sich bringen. Wenn dies aber gelänge, können Operationen wie die von (4), gefolgt von der Amplitude Estimation oder die Ein-Qubit-Messung angewandt werden, um schneller an ein Ergebnis zu kommen.

Somit wollten wir in diesem Bericht auf die Tatsache aufmerksam machen, dass Quantencomputer einen Vorteil bei Monte-Carlo-ähnlichen Simulationen aufweisen können. Eine der bedeutendsten Steigerungen wird durch die Amplitude Estimation erreicht, welche aber derzeit nicht für NISQ-Prozessoren infrage kommt. Es wurde zwar eine NISQ-freundlichere Alternative vorgestellt, jedoch kann sie den Zugewinn von Leistung nicht erreichen. Beide Verfahren können jedoch mit dem Vorteil aufwarten, dass deren Varianz nicht von den zugrunde liegenden Zufallsvariablen abhängt. Damit erfüllen beide eine Varianzreduktion. Aufgrund der großen Beliebtheit dieser Techniken kann man folgern, dass Quantencomputer auch bei der Simulation von Zufallszahlen und Berechnungen von Erwartungswerten eine Rolle spielen werden.

Die Hürden dieser Verfahren liegen in der State Preparation, dem Vorgang, einen gewollten Quantenzustand mit hoher Präzision zu erzeugen. Während auch andere Methoden existieren, wollten wir ein einfaches konstruktives Beispiel zeigen. Für ein kleines Spielzeugbeispiel sind bereits heutige 5-Qubit-Prozessoren von IBM in der Lage, das vorhergesagte Verhalten aufzuzeigen. Jedoch muss eine Analyse interessanter Anwendungsfälle aus der Industrie, Wirtschaft und Forschung nun eine Aufgabe zukünftiger Forschung sein.

Der Wunsch dieses Berichts war es, diese Tatsache etwas zu beleuchten und somit insbesondere der Wirtschaft einen verständlichen Zugang zu diesem Quantenvorteil zu ermöglichen. Bereits heute sehen wir Ergebnisse, wie sie in den Arbeiten[7,8,13] dargelegt werden, als zeitnahe Anwendung der frühen Quantenprozessoren. Es sei jedoch auch gesagt, dass es noch ein paar Jahre braucht, die angeführten Techniken in einem Umfang berechnen zu können, sodass „klassische“ Computer nicht mehr mithalten können. Wie in allen sich schnell ändernden High-Tech-Bereichen ist die Entwicklung auch für Experten schwer vorherzusagen.

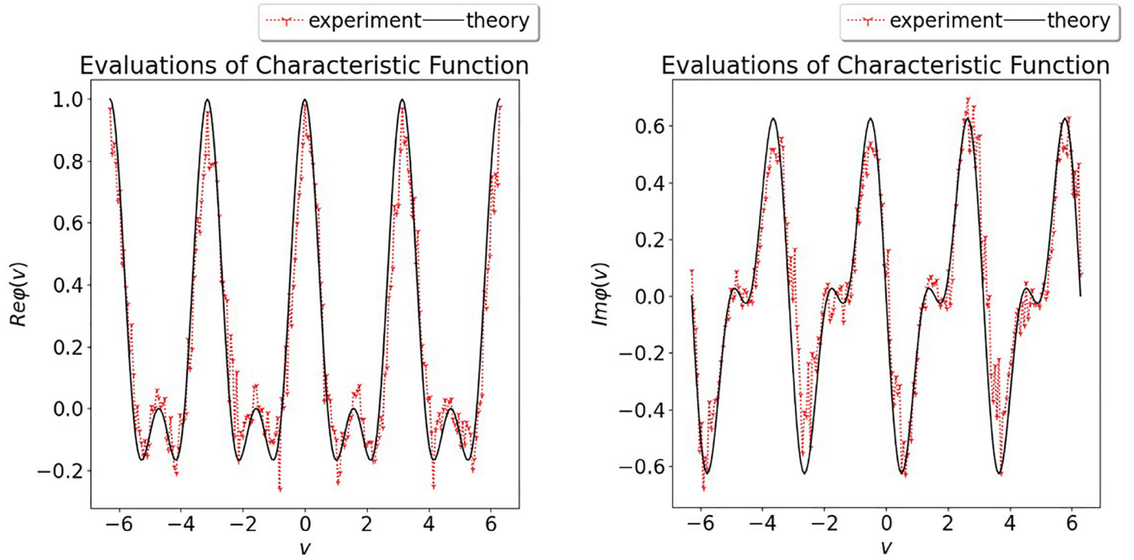


Abbildung 4: Die charakteristische Funktion einer korrelierten Irrfahrt mit $p = \left(\frac{2}{3}, \frac{5}{6}, 1\right)$, $q = \left(\frac{1}{3}, \frac{1}{6}, 0\right)$ auf dem ibmqx2 von IBM Q mit 8192 „shots“ pro v.

Danksagung

Wir wollen uns bei Philipp Leser & Daniel K. Park für die vielen wertvollen Diskussionen zu diesem Thema bedanken. In dieser Arbeit werden Ergebnisse zitiert und gezeigt, die mit dem IBM Q erstellt wurden. Die Aussagen in dieser und in zitierten Arbeiten sind die der Autoren und nicht die offizielle Position der IBM oder des IBM Q Teams.

Referenzen: **[1]** Chakrabarti, S. et al. A Threshold for Quantum Advantage in Derivative Pricing. Arxiv (2020). **[2]** Fowler, A. G. & Gidney, C. Low overhead quantum computation using lattice surgery. Arxiv (2018). **[3]** Preskill, J. Quantum Computing in the NISQ era and beyond. Quantum 2, 79 (2018). **[4]** Montanaro, A. Quantum speedup of Monte Carlo methods. Proc Royal Soc Math Phys Eng Sci 471, 20150301 (2015). **[5]** Rebentrost, P., Gupt, B. & Bromley, T. R. Quantum computational finance: Monte Carlo pricing of financial derivatives. Phys Rev A 98, 022321 (2018). **[6]** Rebentrost, P. & Lloyd, S. Quantum computational finance: quantum algorithm for portfolio optimization. Arxiv (2018). **[7]** Blank, C., Park, D. K. & Petruccione, F. Quantum-enhanced analysis of discrete stochastic processes. Arxiv (2020). **[8]** Woerner, S. & Egger, D. J. Quantum Risk Analysis. Npj Quantum Information 5, 15 (2019). **[9]** Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Siam J Comput 26, 1484–1509 (1997). **[10]** Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. Proc 35th Annu Symposium Found Comput Sci 124–134 (1994) doi:10.1109/sfcs.1994.365700. **[11]** Nielsen, M. A. & Chuang, I. L. Quantum Computation and Quantum Information. (2009) doi:10.1017/cbo9780511976667. **[12]** Brassard, G., Hoyer, P., Mosca, M. & Tapp, A. Quantum Amplitude Amplification and Estimation. Arxiv (2000). **[13]** Stamatopoulos, N. et al. Option Pricing using Quantum Computers. Quantum 4, 291 (2020). **[14]** Egger, D. J., Gutiérrez, R. G., Mestre, J. C. & Woerner, S. Credit Risk Analysis using Quantum Computers. Arxiv (2019). **[15]** Park, D. K., Sinayskiy, I., Fingerhuth, M., Petruccione, F. & Rhee, J.-K. K. Parallel quantum trajectories via forking for sampling without redundancy. New J Phys 21, 083024 (2019). **[16]** Iten, R., Colbeck, R., Kukuljan, I., Home, J. & Christandl, M. Quantum circuits for isometries. Phys Rev A 93, 032318 (2016). **[17]** Malvetti, E., Iten, R. & Colbeck, R. Quantum Circuits for Sparse Isometries. Arxiv (2020). **[18]** Shende, V. V., Bullock, S. S. & Markov, I. L. Synthesis of quantum-logic circuits. Ieee T Comput Aid D 25, 1000–1010 (2006). **[19]** Plesch, M. & Brukner, Č. Quantum-state preparation with universal gate decompositions. Phys Rev A 83, 032302 (2011). **[20]** Mottonen, M., Vartiainen, J. J., Bergholm, V. & Salomaa, M. M. Transformation of Quantum States Using Uniformly Controlled Rotations. Arxiv 5, 467–473 (2005). **[21]** Peruzzo, A. et al. A variational eigenvalue solver on a photonic quantum processor. Nat Commun 5, 4213 (2014). **[22]** Romero, J. & Aspuru-Guzik, A. Variational quantum generators: Generative adversarial quantum machine learning for continuous distributions. Arxiv (2019). **[23]** Wecker, D., Hastings, M. B. & Troyer, M. Progress towards practical quantum variational algorithms. Phys Rev A 92, 042303 (2015). **[24]** Chowdhury, A. N., Low, G. H. & Wiebe, N. A Variational Quantum Algorithm for Preparing Quantum Gibbs States. Arxiv (2020). **[25]** Zoufal, C., Lucchi, A. & Woerner, S. Quantum Generative Adversarial Networks for learning and loading random distributions. Npj Quantum Information 5, 103 (2019). **[26]** Araujo, I. F., Park, D. K., Petruccione, F. & Silva, A. J. da. A divide-and-conquer algorithm for quantum state preparation. Arxiv (2020). **[27]** Enriquez, N. A simple construction of the fractional Brownian motion. Stoch Proc Appl 109, 203–223 (2004).

Dr. rer. nat. Carsten Blank

Carsten Blank promovierte 2010 am KIT, im Anschluss die Mitgründung einer eCommerce Plattform. Die Software-Entwicklung wurde fortan Schwerpunkt, schließlich gründete er die data cybernetics (ab 2016). Heute berät er Energieunternehmen zum Thema Software & Data Science und forscht im Quantum Computing.

Prof. Dr. rer. nat. habil. Francesco Petruccione

Francesco Petruccione erhielt seine Habilitation an der Universität von Freiburg 1994. Heute führt er den Lehrstuhl „Quantum Information Processing and Communication“ der Universität KwaZulu-Natal. Unter anderem ist er Pro-Vize-Kanzler für „Big Data und Informatics“ und ist Interimsdirektor des NITheCS in Südafrika

Fotos: Privat

How test and measurement technology can bring quantum computers to life

Christian Dille, Philipp Kurpiers
Rohde & Schwarz

During the last decade, considerable advances have been made to bring quantum computing closer to realization. The technology offers many possibilities, thanks to its unprecedented calculation speed and alternative methodology, and is expected to have a great influence in everyday life, with applications such as molecular and material simulations, climate analysis and cryptography. However, this powerful technology poses new technical challenges and also means that testing quantum computing systems calls for innovative T&M solutions.

Great Expectations

The Gartner hype cycle describes technology hype, and quantum computing has earned its place in it. According to claims by many of its experts, quantum computing will change everything forever. The potential for decryption could obviously affect distributed ledger technologies like blockchain that are slated to support financial systems of the future. While the Bitcoin system, for example, is not expected to be mined by classical computers until 2140, brute force decryption using a quantum computer could theoretically mine every token almost instantaneously.

Although it is fair to say that quantum computers could spell the end for conventional cryptography, the reality is likely to be somewhat less dramatic. The decryption estimate is based on the assumption that quantum computing will become usable and affordable on a widespread scale. From the current perspective, this certainly seems achievable, if not an inevitability. Serious computing players such as IBM, Honeywell, Google and Microsoft and research institutes such as the QuTech, as well as newer specialist startups, have active programs for putting quantum computing in the cloud and inviting engagement from the wider computing community. There are also introduction packs and development kits to help new users get started.

Widening the User Base

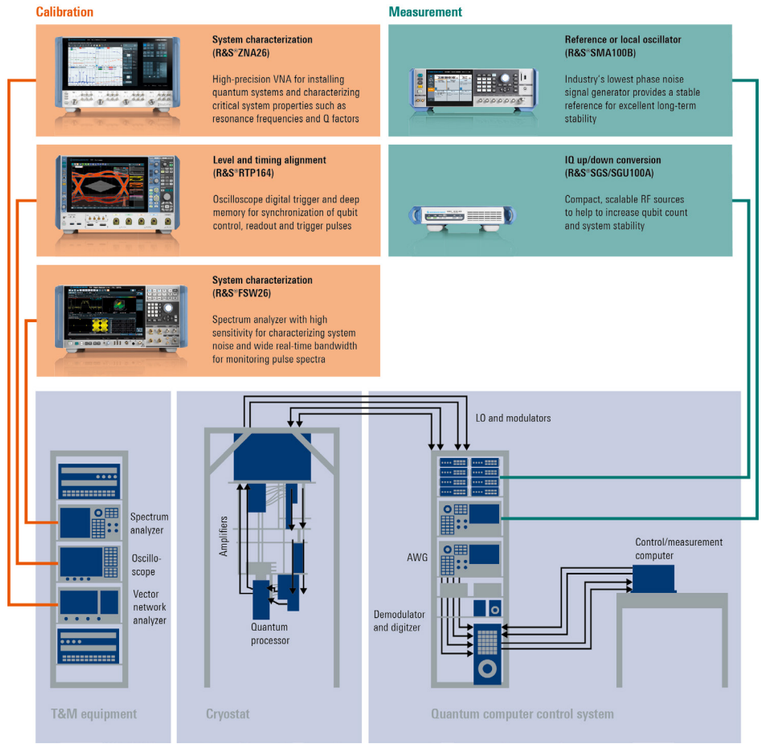
The advancements that could be made possible by quantum computing are significant and will almost certainly drive further progress as users come up with more diverse and demanding workloads and discover ways of handling them using quantum technology. Equally important is that quantum computing is expected to allow more people from a wider variety of backgrounds to come into contact with the technology; to understand it, use it, and influence its ongoing development.

Although the age of quantum computing is closer, it still remains at a very experimental stage. In the future, commercial cloud services could provide affordable access in the same way as scientific or banking organizations can today rent cloud-based AI applications to handle complex workloads that are billed according to the number of computer cycles used. Hospitals, for example, are taking advantage of genome sequencing applications hosted on AI accelerators in hyperscale data centers to identify genetic disorders in newborn babies. This process costs just a few dollars and the results are back within minutes enabling timely and potentially life-saving interventions by clinicians.

Quantum computing as a service could further transform healthcare and also deeply affect many other fields such as materials science. As an example, creating a simulation of a caffeine molecule is incredibly difficult to do with current computers, demanding the equivalent of over 100 years of processing time. A quantum computer could theoretically complete the task in a matter of hours. Other applications that could benefit from quantum computing include climate analysis, transportation planning, bioinformatics, financial services, encryption and codebreaking.

Creating a Roadmap

Despite its anticipated, unprecedented power of calculation, quantum computing will not kill off binary computing or turn



Setup of a superconducting quantum computer. The quantum processor is hosted inside a cryostat at millikelvin temperatures and controlled by microwave electronics. The installation of the setup and fast sample testing is performed using T&M equipment.

the entire world upside down. Unlike conventional binary bits that are in one state or another, quantum bits (qubits) can be in both states, 0 and 1, enabling quantum computers to process and store exponentially more information. This exponential advantage of quantum computers might one day open up possibilities undreamed of in computing for currently unsolvable problems.

There are drawbacks. When measured, the state of each qubit collapses probabilistically to either 0 or 1, obtaining only 1 bit of information per qubit. Due to this probabilistic collapse, quantum algorithms need to be repeated many times to build statistics of the outcome and finally concentrate a large probability on the correct result. This fundamental feature of the architecture restricts the speedup of quantum algorithms to only certain types of problems, while others can still be better handled by binary computers. Just as quantum mechanics has not replaced classical mechanics for most engineering calculations, quantum computing will not replace binary computing for most every day computing applications.

In addition, building and running a quantum computer is highly difficult and complex. Moreover, the challenges intensify when trying to increase the number of qubits in the system. As with any computer, more parallel data values correspond to more processing power, making increasing the number of qubits a key objective for quantum computer architects. Another key objective is to keep the coherence of the quantum system stable, at lower error rates and for longer periods.

To reach these goals simultaneously, university and industrial research facilities worldwide are investigating various hardware platforms. The development of these quantum platforms is substantially supported by modern microwave technologies in several aspects. Optical systems for quantum computing such as trapped ion and cold atom qubits, need to be complemented by microwave devices to operate acousto- and electro-optic modulators, or to directly drive atomic hyperfine and Zeeman transition in the microwave domain. These hyperfine and Zeeman transitions form qubits with long coherence times of up to tens of seconds (the period for which a value is reliably stored) and require extremely stable microwave equipment to be operated without larger errors. For quantum systems with all transition frequencies in the microwave domain, quantum processors based on superconducting circuits and spin qubits in semiconductors have shown high potential to be scalable at low-error rates. To eliminate thermal noise, these microwave systems need to be cooled to cryogenic temperatures near absolute zero. In addition, high-performance microwave equipment is needed for the external control of the quantum system at room temperature. A pure and low-noise microwave signal helps to reduce the loss of quantum information potentially introduced by the qubit control tone. This is where high-end test and measurement equipment is brought into play, enabling flexible

solutions for quantum systems (See figure). Rohde & Schwarz is working with its academic partners to provide stable and compact microwave signal generators to help scale the quantum computing system up, while decreasing the error rate.

Multi-channel arbitrary waveform generators (AWGs) are necessary to obtain high-quality multi-qubit control by generating both RF and microwave pulses with optimized shapes, as required. The output of high-resolution AWGs can either be directly applied at frequencies of less than a gigahertz, for example, to activate interactions between qubits. Or the AWG signals can be up-converted to higher frequencies using external IQ modulators or inputting them to a vector signal generator.

In the process of reading out the results of the quantum computation, high-performance microwave sources are essential, as they significantly mitigate errors due to phase drifts. During the readout, the quantum system interacts with a pulse in the readout circuit, encoding information about the qubit state in the amplitude and phase of the readout signal. This information needs to be extracted during a time which is much smaller than the coherence time of the qubit. This puts substantial requirements on the performance of the cryogenic detection equipment after the quantum system, the room-temperature digitizers, and the digital signal processing. In pursuit of delivering a complete solution, Rohde & Schwarz provides the T&M expertise, to combine with the software and system know-how of quantum computing partners.

Additionally, the search continues for new materials and cleaner fabrication processes to be applied in quantum computing chips, and for test and measurement equipment to help accurately determine the exact properties. To obtain detailed feedback from new fabrication runs, the resonance frequencies and quality factors of the test chips, which can be directly mapped to the coherence times of quantum systems, need to be determined quickly. These characteristic properties can be obtained by multi-tone spectroscopic measurements using a high-performance vector network analyzer (VNA). To further reduce the characterization time, multiple test chips can be measured simultaneously by using a truly multi-port VNA. A suitable high performance VNA can run fast frequency sweeps over a range of 20 gigahertz or more, while maintaining a wide dynamic range to detect undesired resonances and couplings between circuit elements. Moreover, a VNA is an essential tool during the installation of both the room-temperature and cryogenic microwave setups. The DUT-centered operating concept makes an efficient characterization of all active and passive RF components of the microwave system possible, thus helping ensure an optimal performance of the whole setup. During the operation of the quantum setup, a VNA can assist in the debugging process of the quantum computing chips themselves.

Rohde & Schwarz also provides various other test and measurement solutions for its partners to help them increase the performance and capabilities of their quantum computer setups. For example, to read out quantum information with high precision, a careful design and verification of the detection equipment between the quantum chip and the room-temperature digitizer is crucial, as described above. The detection equipment includes superconducting parametric amplifiers, which operate close to the quantum limit of amplification, and ultra-low noise semiconductor amplifiers, the performance of which needs to be verified. High-sensitivity spectrum analyzers from Rohde & Schwarz are ideal devices to obtain the noise performance and compression characteristics of these amplifiers and of the complete detection setup.

Furthermore, Rohde & Schwarz spectrum analyzers are useful for the measurements and calibration of IQ mixers, as spectrum analyzers detect undesired sidebands of the mixers. A third relevant application of a spectrum analyzer with real-time capabilities is the reliable detection of short sporadic interferences.

Another example of how the test and measurement solutions from Rohde & Schwarz support quantum engineers and research is the precise temporal synchronization and alignment of microwave pulses and triggers which are the basis of all quantum algorithms. A high-speed oscilloscope enables real-time measurements of the signal integrity and time-correlated analysis of multiple signals verifying the synchronization of readout and control pulses across multiple qubits. Advanced oscilloscopes also help to detect undesired jitter events and can thus create an essential contribution to the stability of the whole quantum setup.

Rohde & Schwarz works with its partners in the quantum world to extend and customize its products for a better solution fit. This also allows the company to learn how to apply the knowledge gained to other products in the portfolio simultaneously, and hence deliver even better performing solutions across the breadth of applications and markets served. Considering the complex technical challenges of quantum computing, the customers need to be able to have confidence in their T&M partner to deliver reliable solutions for this task. Rohde & Schwarz continues to expand the portfolio of leading-edge test and measurement equipment that addresses these needs.

While cloud access will certainly enable more companies and research institutes to take part in the quantum revolution, the challenge of stabilizing quantum computers with a high number of qubits while keeping the price at a competitive level is of vital importance. To ensure this goal, innovative solutions based on thorough research and development are required.

Christian Dille

Christian Dille finished his master in physics at the Friedrich-Schiller University Jena, Germany with major in Ultra-fast Laser Photonics. After working in the photonics industry for several years he took over the responsibility for the market segment Research and Universities at Rohde & Schwarz in 2019.

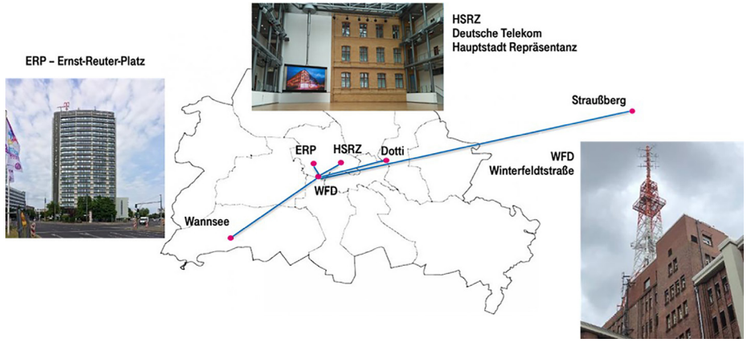
Dr. Philipp Kurpiers

Dr. Philipp Kurpiers studied physics at LMU Munich and ETH Zurich. He received his doctorate from ETH Zurich in 2019 for investigating quantum networks with superconducting circuits. He joined Rohde & Schwarz in 2020 as a microwave hardware developer.

Fotos: Privat

Die Deutsche Telekom erprobt prototypisch Quantencomputing und Quantenkommunikations-anwendungen

Marc Geitz, Ralf-Peter Braun, Oliver Holschke
Deutsche Telekom AG



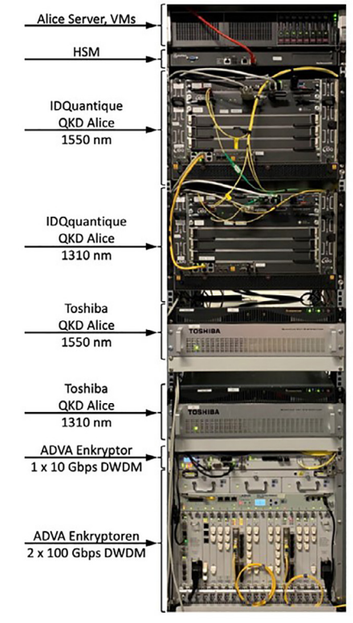


Abbildung 1: Links: das Netz des OpenQKD-Testbed in Berlin, betrieben in den Laboren am Standort Winterfeldtstrasse (WFD), mit diversen Endpunkten im Berliner Raum. Rechts: ein QKD-Knoten mit vier QKD-Systemen, optischen Endpunkten, Verschlüsslern, Hardware Security Modulen, Switchen und Applikationsservern.

Quantencomputing

Lassen sich bereits heute Vorteile aus Quantencomputern der NISQ-Phase (Noisy Intermediate-Scale-Quantum) zur Bewältigung der täglichen Herausforderungen eines internationalen Telekommunikationsproviders und Systemintegrators erzielen?

Zur Beantwortung dieser Frage engagiert sich die Deutsche Telekom aktiv im BMWi[1]-geförderten Projekt PlanQK[2]. Konkret sind die Telekom-Laboratories (T-Labs), Forschungs- und Entwicklungsarm des Vorstandsbereichs Technologie & Innovation, beteiligt. Sie nutzen die fruchtbare Zusammenarbeit mit verschiedenen Universitäten und Industriepartnern, um Optimierungs- und Machine-Learning-Anwendungen mithilfe von Quantencomputern zu lösen. Neben der Mitarbeit in öffentlich geförderten Projekten kooperiert die Telekom auch direkt mit Spezialisten der Optimierung, beispielsweise mit Fujitsu Technology Solutions. Die effektive und effiziente Lösung von Optimierungsproblemen hat direkten Einfluss auf die operativen Aufwände der Telekom und spielt in verschiedenen Bereichen des Unternehmens eine Rolle.

Netzwerkoptimierung: Die Telekom betreibt Kommunikationsnetze basierend auf unterschiedlichen Transportmedien und verschiedener Generationen. Als Beispiel seien Glasfaser-, Kupferkabel- oder Mobilfunknetzwerke genannt. Diese Netzwerke bedürfen einer Optimierung hinsichtlich operativer Leistungsmerkmale, wie Datendurchsatz oder Latenz, sowie planerischer Größen zum Netzausbau, wie Kapazität oder Architektur. Die folgenden Optimierungsprobleme wurden bisher betrachtet:

- Traffic Engineering zur Auslastung von Glasfaser-Backbone-Netzwerken (insbesondere im Kontext des Multi-Commodity-Flow-Routing und des Segment-Routing).
- Einsatz von Quantum Key Distribution (QKD)-Systemen abhängig von der – zur Verschlüsselung der Verkehrsanforderungen notwendigen – Schlüsselanzahl.
- Frequenzzuweisung in GSM-Mobilfunknetzen (Global System for Mobile Communications), um die zur Verfügung stehenden Frequenzen ausschöpfen und gleichzeitig Störungen minimieren zu können.
- Die dynamische spektrale Ressourcenverteilung in Mobilfunkzellen zur Garantie eines Quality-of-Service für den Kunden.

Auch der Ausbau der Glasfasernetze ist ein strategisches Thema für die Telekom. Der größte Kostentreiber für den Netzausbau sind Erdarbeiten. Deshalb wurde u.a. mithilfe von Quantencomputern versucht, mit einer auf einem Kataster basierenden Kostenstruktur die optimalen Grabungswege zur Anbindung von kundenseitigen Endpunkten an die Netzanschlussstellen zu berechnen.

Dienstplanoptimierung: Der technische Außendienst der Deutschen Telekom löst technische Probleme beim Kunden oder an den eigenen Standorten. Störungen werden abhängig von ihrer geographischen Lage, ihrer Schwere oder ihrer Priorität bearbeitet. Auch der Ausbildungsstand der Techniker oder die Öffnungszeit der Störung spielt zur Bestimmung der ressourcenoptimalen Einsatzpläne der Techniker eine Rolle. Diese kombinatorische Optimierung wurde als „Capacitated Vehicle Routing“ -Problem modelliert und anschließend auf einem adiabatischen Quantencomputer berechnet.

Customer-Relationship-Management (CRM): Das Management der Kundenbeziehung ist strategisch eine der wichtigsten Aufgaben eines Kommunikationsunternehmens.

Lassen sich aus den verfügbaren Kundendaten Aussagen über das zukünftige Kundenverhalten treffen? Zur Beantwortung dieser Frage wurden bereits einige Implementierungen im Bereich von Quantum Machine Learning (QML) unternommen, z.B.

- Klassifizierung von Missbrauch und Betrugsverhalten.
- Bestimmung des optimalen Kontaktzeitraumes für den Kundendienst.

Industrielle Anwendungen: T-Systems, Tochter der Deutschen Telekom, bietet Industriekunden weltweit ICT- (Information and Communication Technologies) und Systemintegrationsdienstleistungen an. Sie entwickelt industrienahe Lösungen, die sich durch den Einsatz von Quantencomputern verbessern lassen. In diesem Kontext wurden bereits Lösungen optimiert.

- MixSigma, ein Konzept für eine alternative Qualitätssicherungsmethode, zur Bestimmung der Zuordnung von Bauteilen zu einem letztlich vollintegrierten System.
- Job Shop Scheduling, d.h. die Berechnung von Maschinenbelegungsplänen unter Berücksichtigung von automatisiertem Materialtransport durch Flurförderfahrzeuge.
- Die Verkehrssignalsteuerung zur Verbesserung des Verkehrsflusses in Smart Cities, u.a. um die Emissionen in den Städten zu minimieren.

Alle beschriebenen Anwendungen werden als Micro-Services bereitgestellt, in der Cloud betrieben und erlauben so potenziell eine Integration an bestehende Systeme und Abläufe der Telekom. Verwendete Quantencomputer sind Quanten-Annealer der Firma D-Wave, der Digital Annealer der Firma Fujitsu und, über das Projekt PlanQK finanziert, ein Quantencomputer der Firma IBM. Die Quantencomputer werden von den Micro-Services über eine Cloud API angesprochen und können remote über das Internet genutzt werden.

Die bisher implementierten Programme laufen erfolgreich auf den NISQ-Quantencomputern und erlauben den Vergleich mit bisherigen konventionellen Lösungen. Jedoch lässt sich aus unserer Sicht noch kein Vorteil bei den Ergebnissen durch die Quantenoptimierungs- und QML-Probleme erkennen. Die bisher durchgeführten Arbeiten erlauben aber eine kontinuierliche Re-Evaluierung der Performance zukünftiger Generationen von Quantencomputern und ihre schnellstmögliche Nutzung im Falle von vorteilhaften Lösungen.

[1] Bundesministerium für Wirtschaft und Energie
[2] Plattform für KI-gestütztes Quantencomputing

Quantenkommunikation

Wie schützen wir zukünftig unsere digitale Kommunikation vor Angreifern, die sich einen Quantencomputer zunutze machen?

Quantencomputer werden in der kommenden Dekade in der Lage sein, bestehende asynchrone Verschlüsselungsstandards zu brechen[3]. Die Gefahr, dass systemkritische Information zwischengespeichert und dann zu einem späteren Zeitpunkt entschlüsselt werden kann, besteht schon heute. Alle intelligenten Geräte, die in den kommenden Jahren produziert werden und eine Lebensdauer von mehr als zehn Jahren haben, müssten notwendigerweise schon heute eine Technologie zur quantensicheren Verschlüsselung von Nachrichten einsetzen. Quantensichere Verschlüsselung in den Netzwerken eines Telekommunikationsproviders ist daher eine kritische Komponente in Bezug auf das Geschäftsmodell – auch das der Deutschen Telekom.

Post Quantum Cryptography (PQC) ist als zukünftiges asynchrones, quantensicheres Verschlüsselungsverfahren für den Einsatz auf Kommunikationsendgeräten gesetzt. Doch Netzbetreiber erforschen, auch aufgrund eines fehlenden PQC-Sicherheitsbeweises, den Einsatz von Quantum Key Distribution (QKD) zusammen mit beweisbar quantensicheren synchronen Kryptographie-Verfahren zur Absicherung der Verkehre. Dazu betreibt die Telekom in Berlin eine der vier OpenQKD[4]-Testumgebungen in Europa. Ziel: Eine herstelleragnostische Integration der QKD-Systeme in europäische Providernetze und die Erprobung verschiedener Übertragungsmethoden von klassischen und quantenoptischen Kanälen in Fasernetzwerken. Auch hier wird die Forschungs- und Entwicklungsarbeit über T-Labs und den Vorstandsbereich Technologie & Innovation, in enger Zusammenarbeit mit den Experten aus den Bereichen der Deutsche Telekom Technik und Telekom Security, maßgeblich durchgeführt.

Abbildung 1 (links) zeigt verschiedene Glasfaserstrecken, die im Rahmen des Deutsche Telekom Open Integration Lab aufgebaut wurden und betrieben werden. Das ermöglicht, entsprechende neueste Technologien, Netz- und Systemarchitekturen sowie innovative Entwicklungen und Lösungen zeitnah und im Vorfeld der Markteinführung zu testen und zu demonstrieren.

Beispielsweise zeigt Abbildung 1 (rechts) den Aufbau des QKD-Netzwerkknotens Alice, der im Rahmen des EU Flagship-Projekts OpenQKD im QuantumLab Berlin aufgebaut wurde. Er umfasst neben QKD-Systemen verschiedener Hersteller (Fa. IDQuantique und Fa. Toshiba), einem Hardware Security Modul (HSM) zur sicheren Aufbewahrung der kryptographischen Schlüssel (Fa. Gemalto) und einem optischen Endpunkt der Fa. Adva Optical auch ein voll funktionsfähiges Schlüsselmanagementsystem, das von der Telekom entwickelt und implementiert wurde. Im Vergleich zum ETSI-Standard weist es erhöhte Sicherheitsmerkmale, wie vollständig PQC-verschlüsselte Kommunikationsstrecken, auf. QKD-Netze mit Kommunikationsanwendungen, die die verteilten, quantensicheren Schlüssel verwenden, können untersucht und demonstriert werden.

Im weiteren Verlauf der Arbeiten im OpenQKD-Projekt werden im Quanten-Testbed Berlin unterschiedliche Realisierungsmöglichkeiten des quantenoptischen Kanals untersucht, getestet und demonstriert. Die optimale Ausnutzung der Glasfaser für Quantenkanäle bei gleichzeitiger Nutzung des Glasfasernetzes für klassische Kommunikationskanäle steht dabei im Mittelpunkt.

Dr. Marc Geitz

Dr. Marc Geitz ist seit 2001 bei der Deutschen Telekom in mehreren Positionen und seit 2013 bei den Telekom Innovation Laboratories beschäftigt.Seit 2018 arbeitet er an potenziellen Anwendungsmöglichkeiten der Quantentechnologie, insbesondere Quantenkommunikation und -computing für Netzwerkprovider.

Dr.-Ing. Ralf-Peter Braun

Dr.-Ing. Ralf-Peter Braun diplomierte 1985 und promovierte 1995 an der TU Berlin. Seit 1997 beschäftigt er sich bei der Deutschen Telekom auf Gebieten der optischen und drahtlosen Nachrichtentechnik u.a. mit der Quantenkryptographie. Er ist Mitglied im VDE, ITG und in der IEEE 802.3 Arbeitsgruppe.

Dr.-Ing. Oliver Holschke

Dr.-Ing. Oliver Holschke ist seit 2013 als System Architect im Bereich Strategic R&D bei den T-Labs beschäftigt. Dort entwickelte er eine Netzverkehrs-Monitoring-Lösung für internationale Telko-Kunden. Seit 2020 verantwortet er das R&D-Programm zu Quantentechnologien und zukünftigen Netzkonzepten.

Fotos: Privat

[3] IBM Roadmap, die veröffentlichte Steigerung der Qubit-Anzahl pro Jahr extrapoliert, unter der Annahme einer funktionsfähigen Fehlerkorrektur zur Anwendung des Shor-Algorithmus.

[4] OpenQKD, EU Flagship-Projekt, gefördert durch die Europäische Kommission im Rahmen des Innovationsprogrammes „Horizon 2020".

1.1 QUANTUM APPLICATIONS

Practical Quantum Computing

Auch wenn Quantum Computing in den letzten Jahren immer mehr Aufmerksamkeit findet, erscheint es doch für viele so belanglos wie die Entwicklung von Fusionsenergie

oder dem Ionenantrieb. Gegenüber diesen hat Quantum Computing jedoch einen entscheidenden Unterschied: Es ist bereits zugänglich - für jeden.

Dieser Umstand mag für den einen oder anderen zunächst verblüffend klingen, aber in der Tat stellen verschiedene Unternehmen diese Multimillionen-Dollar-Geräte für jeden, der genug Interesse zeigt, zur Verfügung – in manchen Fällen sogar gratis.

Im Folgenden sollen kurz die Herausstellungsmerkmale von Quantum Computern umrissen werden. Wie man heute schon mit diesen arbeiten kann und was dafür spricht, dies auch zu tun, erklärt Jannes Klinck Software-Entwickler und Data Scientist von bytabo®. Dabei liegt der zusätzliche Fokus darauf, praktische Anwendungsfälle aufzuzeigen, die aktuell von Unternehmen mit der Hilfe von Quantum Computern umgesetzt werden.

Quantum Computing - Grundlagen

Für diejenigen, die sich bisher noch gar nicht mit Quantum Computing befasst haben, soll knapp erläutert werden, wodurch sich Quantum Computer überhaupt von herkömmlichen PCs unterscheiden und wieso sich daraus so bemerkenswerte Potenziale ableiten lassen. Jedoch sei vermerkt, dass es sich dabei um eine äußerst vereinfachte Erklärung handelt.

Wie aus dem Namen schon ersichtlich, beruht das Grundprinzip der Quantum Computer auf den Grundgesetzen der Quantenmechanik. Hierdurch wird es möglich, dass die kleinstmögliche Speichereinheit des Quantum Computers, die sogenannten Qubits, nicht nur die Ausprägung 0 oder 1 annehmen können, sondern auch jegliche Kombination derselben (abgeleitet aus dem quantenmechanischem Phänomen der Superposition). Des Weiteren ist ein Quantum Computer nicht an das sequentielle Abarbeiten von möglichen Lösungen gebunden, sondern ist in der Lage, diese simultan zu evaluieren (was durch den quantenmechanischen Effekt des Entanglements ermöglicht wird). Somit ist der mögliche Informationsgehalt von Qubits exponentiell höher als jener von klassischen Bits (siehe Grafik 1).

Während diese Fakten in der Debatte um Quantum Computing oft hervorgebracht werden, so wird doch selten darauf eingegangen, warum genau dieser Anstieg an Rechenleistung so große Potenziale birgt. Dabei gibt es viele, vergleichsweise banale Beispiele, anhand derer man zeigen kann, dass selbst harmlos klingende Optimierungsaufgaben verblüffend rechenintensiv sind.

Man stelle sich zum Beispiel vor, man hat 9 Freunde zum Geburtstag eingeladen. Nun verstehen sich manche von ihnen besser und andere schlechter. Sucht man nun nach der bestmöglichen Konstellation, alle Gäste an einen Tisch zu platzieren, so dass die meisten mit ihren Sitzpartnern zufrieden sind, stößt man allerdings schnell auf ein Problem. Sich selber eingerechnet gibt es gerade mal 10 Personen, die man zu bedenken hat. Wieviele Möglichkeiten kann es da schon geben, diese an einem Tisch zu platzieren? 3.628.800.

Zwar ist diese Anzahl an Kombinationen noch mit herkömmlichen PCs berechenbar, allerdings soll es verdeutlichen, warum vermeintlich einfache Probleme wie z.B. Tischplatzierungen oder die optimale Route zu finden, um Pakete auszutragen, rechnerisch unglaublich komplex sind.

Hands-on in die Quantenwelt

Für jene, die sich der Herausforderung des Quantum Computings nun selber stellen wollen, kommt hier die gute Nachricht: Dies ist auch im Jahre 2020 schon möglich. Um einen waschechten Quantum Computer sein Eigen nennen zu können, erfordert es allerdings das nötige Kleingeld. Die kanadische Firma D-Wave Systems vertreibt seit 2011 Quantum Computer, wobei das aktuelle kommerzielle Modell, der D-Wave 2000Q, für die bescheidene Summe von 15.000.000 Dollar zu erwerben ist. Die bedeutendere Entwicklung im Quantum Computing ist jedoch ohnehin, wie in so vielen anderen Sektoren der Informationstechnik auch, die Cloud. Mit der Möglichkeit, die enorme Rechenleistung von Quantum Computern auf Abruf beziehen zu können und dabei nur genau die Ressourcen zahlen zu müssen, die bei der Nutzung entstanden sind, verändert sich die Kostenkalkulation grundlegend. Somit stellt die Fusion aus „klassischen" Technologien mit Quantum Computern möglicherweise den nötigen Schritt dar, der Quantum Computing letztendlich zur Salonfähigkeit verhelfen könnte.

Wenig verwunderlich ist es deswegen auch, dass viele der namhaften Tech-Giganten mittlerweile schon Quantum Computing in der Cloud anbieten oder daran arbeiten. Erwähnenswerte Vertreter sind unter anderem Alibaba, Amazon, Google, IBM und Microsoft. Wohingegen das Verwenden von Quantum Computern in der Regel an kostspielige Abonnements gebunden ist, bietet IBM mit der IBM Quantum Experience zusätzlich einen Service an, der von jedermann komplett gratis genutzt werden kann. Auf dieser Spielwiese ist es für alle möglich, einen ersten Geschmack von Quantum Computing zu bekommen, selbst wenn noch keine Expertise in diesem doch sehr spezifischen und komplexen Themengebiet vorliegt. Beschränkungen finden sich lediglich in der Rechenpower der verfügbaren Hard-

Hier geht es zu weiteren Blogbeiträgen

Jannes Klinck, Entwickler und Data Scientist, bytabo

Qubits	Classical bits required to represent an entangled state
2	512 bits
3	1,024 bits
10	16 kilobytes
16	1 megabyte
20	17 megabytes
30	17 gigabyte
35	550 gigabytes
100	More than all the atoms of planet earth
280	More than all the atoms in the universe

Grafik 1: Informationsgehalt von Qubits und Bits in der Gegenüberstellung. Quelle: IBM Research

ware, welche weit unter den heutigen Standards liegt.

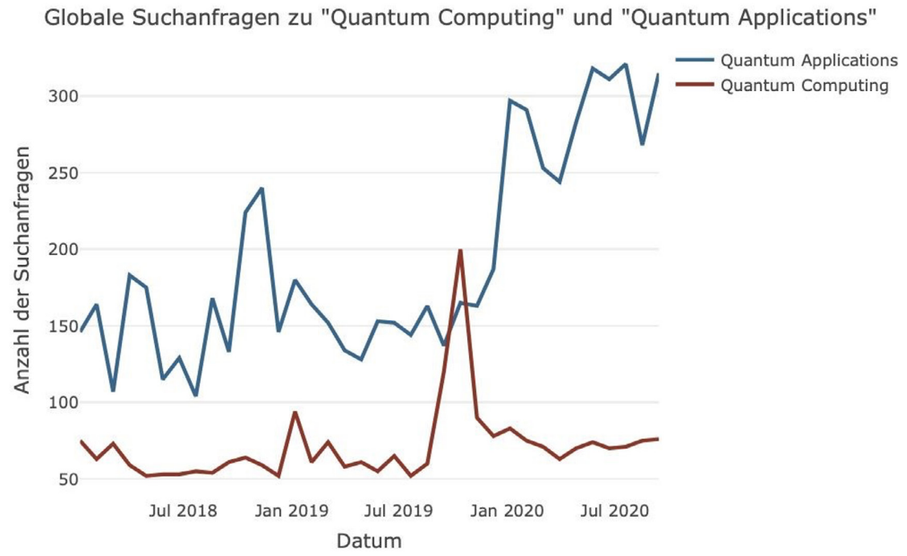
Aber worin liegt der Reiz und Ansporn, eine so vergleichsweise unausgereifte Technologie heute schon zu erkunden? Mit all den verschiedenen Ansätzen, die momentan ausprobiert und erforscht werden, ist es unabdingbar, dass viele von diesen letztendlich im Sande verlaufen werden. Nicht unbedingt eine attraktiver Ausblick, um dort einzusteigen. Doch durch die noch junge und vergleichsweise unerprobte Arbeitsweise gibt es im Quantum Computing noch eine große Freiheit. Genau diese Freiheit erlaubt und verlangt wiederum ein Level an Kreativität und Einfallsreichtum, welches sonst im stringentem Bereich der IT nur noch selten gesehen wird. Der gern verwendete Begriff des Paradigmenwechsels ist beim Quantum Computing also kein Hirngespinst des Marketings, sondern ist direkt zurückführbar auf die grundlegende Weise, in der sich ihre Handhabung und Funktionsweise im Vergleich zu konventionellen PCs unterscheiden. Daher ist das Erlernen der Verwendung von Quantum Computern weniger zu vergleichen mit dem Vertrautwerden mit einer neuen Programmiersprache, sondern erinnert eher an die Pionierarbeit der 1940er und 1950er Jahre, in der die Grundlagen geschaffen werden mussten, um Computer zu dem zu machen, was sie heute sind. Ähnlich wie es damals nötig war, Probleme letztendlich auf Nullen und Einsen herunterzubrechen, so gilt es auch heute beim Quantum Computing, die vorliegenden Problematiken in bestimmte Muster zu transformieren, um die Power der Quantum Computer entfaltbar zu machen. Die dafür nötigen Denkweisen können allerdings nur entstehen, wenn auch jetzt schon das Interesse der zukünftigen Quantum-Entwickler geweckt wird und reges Auseinandersetzen mit der Technologie stattfindet.

2020 als Startschuss für Quantum Applications?

Ein gerne genannter Kritikpunkt des Quantum Computings ist, dass auch wenn große theoretische Potenziale ersichtlich sind, Quantum Computer in der Praxis (noch) keine nützliche Anwendung finden. Begutachtet man zum Beispiel Googles Triumph der Quantum-Supremacy (also das Lösen einer Aufgabe durch einen Quantum Computer viele Größenordnungen schneller als dies ein klassischer Supercomputer könnte) etwas genauer, erscheint die dabei gelöst Aufgabe denkbar nutzlos. Dort ging es nämlich lediglich um das Generieren und Evaluieren von wahllosen Zahlenfolgen (Quelle: Google). Zwar mag dies für die Wissenschaft auch ein Thema von Belangen sein, allerdings ist es wohl kein Feld, das fundamental die Welt verändern könnte. Offen bleibt also die Frage, ob es solche - den Bereich grundlegend revolutionierende - Anwendungsfälle gibt?

Bis dato kann an dieser Steller leider noch keine weltverändernde Erfolgsstory des Quantum Computings erzählt werden. Bedenkt man allerdings, dass diese Technologie momentan noch in den Kinderschuhen steckt, wäre dies auch verwunderlich. Nichtsdestotrotz gibt es schon heute eine Vielzahl von Unternehmen, die praktische Routen erkunden, in welchen Quantum Computing den entscheidenden Vorteil ausmachen könnte:

Mit der stetig steigenden Etablierung der Elektromobilität wird der Fortschritt in Batterietechnologien zunehmend bedeutsamer. An genau diesem Ansatzpunkt forscht Daimler mit dem Einsatz von Quantum Computern. Diese sind nämlich in ihrer quantenmechanischen Funktionsweise nicht ganz unähnlich zu den chemischen Wirkungsweisen einer Batterie und können simulieren, welche Batteriechemie langlebiger, effizienter oder weniger schädlich ist (Quelle: Daimler). Diese Eigenschaft erklärt auch, warum Quantum Computer besonders in der Chemie, Pharmazie und den Materialwissenschaften großes Interesse finden. Andere Firmen greifen hingegen auf die rohe Rechenpower zurück, die durch Quantum Computer ermöglicht wird. Das britische Unternehmen AlgoDynamix, welches Vorhersagen des Finanzmarkts berechnet, konnte mit dem Umstieg auf Quantum Computer



Grafik 2: Suchvolumen der Begriffe „Quantum Computing“ und „Quantum Applications“ im Zeitraum vom Januar 2018 bis September 2020 im Vergleich. Daten auf Monatsebene aggregiert. Quelle: Google-Trends.

einen bis zu 10.000-fachen Geschwindigkeitsanstieg bei der Berechnung ihrer Modelle erreichen. (Quelle: Quantumdaily). Luftfahrtriese Airbus ging sogar noch einen Schritt weiter und arbeitet dieses Jahr an 5 verschiedenen, sehr spezifischen Problemstellungen, die durch die „Airbus Quantum Computing Challenge“ gelöst werden sollen. Diese Aufgabenstellungen spannen von zunächst banal klingenden Problematiken wie das Optimieren des Beladungsprozesses der Flugzeuge bis hin zu abstrakten Konstrukten wie dem Designen eines Quantum neuronalen Netzes zur Lösung von partiellen Differentialgleichungen, welches wiederum zur Berechnung von Aerodynamik eingesetzt werden könnte. (Quelle: Airbus). Projekte wie diese sind dabei nur ein kleiner Ausschnitt des globalen Trends, der sich in Bezug auf Quantum-Anwendungen absehen lässt.

Um den sich anbahnenden Trend noch etwas genauer zu untersuchen, lohnt es sich, das generelle Interesse an Quanten-Technologien präziser zu quantifizieren. Bezieht man sich dafür auf Metriken zum Google-Suchverhalten, wird eine erstaunliche Tendenz ersichtlich (siehe Grafik 2): Während hohe Nachfrage zum Suchterm „Quantum Computing“ allein mit Googles Verkündung der Quantum-Supremacy koinzidierte und für das Jahr 2020 nur geringfügig anstieg, bewegt sich das Interesse an Quantum Applications dieses Jahr auf einem präzedenzlosen, gleichbleibend hohen Level. Dieser Fokus auf Anwendung eröffnet die Frage, ob wir uns aktuell an der Zweigstelle befinden, an der Quanten-Technologien den Weg in die breitere kommerzielle Verwendung finden und infolgedessen ihren Ruf als Zukunfts-Tech-Gimmick allmählich ablegen.

Hindernisse und Risiken

Nach diesem doch sehr optimistischen Einblick in das Quantum Computing, soll allerdings nicht verschwiegen werden, dass es auch deutlich pessimistischere Stimmen gibt. Wirkliche Marktreife ist noch lange nicht erreicht und selbst so fundamentale Fragen wie welcher Ansatz zum Konstruieren eines Quantum Computers sich letztendlich etablieren wird, sind bis dato nicht geklärt. Ferner beruhen die versprochenen Potenziale weitestgehend auf der Annahme der Skalierbarkeit von Quantum Computern. Stellt sich in der Praxis eine Limitation dieser Skalierbarkeit heraus, könnten viele der erhofften Fortschritte unerreichbar bleiben. Dementsprechend kann also nicht ausgeschlossen werden, dass auch Quantum Computing möglicherweise zu jenen Technologien gehört, welche immer 20 Jahre von ihrer Verwirklichung entfernt bleiben. Es bleibt folglich risikobehaftet.

Fazit

Viele der in dem Artikel genannten Informationen sprechen für eine florierende Zukunft des Quantum Computings. Unternehmen sind bereit, zunehmend mehr Kapital in die Hand zu nehmen, um durch die Verwendung von Quantum Computern praxisbezogene Probleme zu lösen. Gleichzeitig sinkt die Eintrittsbarriere stetig durch Entwicklungen wie Cloud-Quantum Computing und macht die Technologie so zugänglich wie nie zuvor. Somit ist es wenig verwunderlich, dass auch das generelle Interesse an Quantum Applications kontinuierlich wächst. Letztendlich wird auch weiterhin genau dieses Interesse und zusätzlicher Enthusiasmus

benötigt, um mit neuem Talent dem Computing zum wortwörtlichen Quantensprung zu verhelfen.

Jannes Klinck

Matthias Ziegler, Managing Director Emerging Technology Innovation ASG, Accenture

Tim Leonhardt, Consultant Technology, Quantum Computing, Accenture

Starting the Quantum Incubation Journey with Business Experiments

Recent developments in quantum hardware for optimization and general purpose quantum computing prototypes as well as application software have propelled quantum computing from a theoretical concept into a tangible computing option for enterprises—one with the potential to deliver business value by solving difficult subsets of problems based on a fundamentally different set of rules.

This year on January 8th 2019 IBM announced the first commercially available universal quantum computer on-premise solution housing 20 qubits[1]. This provides a major step in releasing complex prototype systems, which use chambers as cold as outer space, microwave frequency control electronics and high-tech nano-fabricated chips from their flat-size laboratories, which require extensively trained physicists for maintenance and operation, towards an on-premise solution in your data center. Specific hardware for optimization purposes known as quantum annealers have been announced already in 2011 by D-Wave Systems and reached 2000 qubits today.

At the current stage the gate quantum computer solutions with high quality qubit operations do not provide the capability of solving practical problems but yield the potential of surpassing supercomputers in processing power for a class of sampling problems, that describe the outcomes of random processes in nature. Reaching this milestone is an important step in this era of noisy intermediate scale quantum computation, which is characterized by having access to a few dozen to hundred qubits running hundreds to thousands of operations without errors. This sets the stage for finding approximate solutions to a variety of hard problems. This process is driven by initiatives of global companies and scientific institutes like Google and NASA[2]. Quantum annealers on the other hand trade-off a larger number of qubits at the cost of lower operation quality and a more granular control of the system parameters to solve intermediate scale instances of a specific problem class (so called quadratic binary optimization problems or QUBO) with hundreds to thousands of variables.

These developments raise vast discussions contrasting enormous theoretical potential with uncertainties in predictions of the developments in technology maturity. It is imperative to prepare for different possible outcomes of this Hilbert-space race*.

The first step towards a quantum strategy is a sound introduction to the capabilities, potential advantages and tools in quantum computing. The next step is the identification of business areas, where quantum could yield a business advantage and the assignment of an employee to monitor the trends reporting monthly to hold up with the developments in the field. The quantum potential may only be leveraged, when there is expertise in understanding the structure of the problems that limit business activities in the identified areas and finding quantum approaches that could tackle those limits. Only after this ideation and analysis endeavors the next step of running business experiments enables to build know how in quantum application development and supports predictions on the impact of future hardware developments by using quantum simulators or typical cloud access solutions. With these experiences the strategic roadmap can be funneled into a more specific timeline for how the use cases scale with quantum computing improvements and selecting the most promising.

A large ecosystem has already formed to support this incubation journey in providing hard- and software for quantum computing applications. Quantum computer mainframe providers typically provide an interface including instructions sets that define qubit specific electrical control signals and higher-level programming languages that accumulate operations on qubit registers to subroutines (e.g. addition circuits) as well as high level optimization algorithms like solvers for QUBO problems, while giving cloud access to the quantum hardware backend via web protocols. At the highest level modern web frontends allow for an intuitive user interface that enables the usage by end users without the necessity of understanding the underlying rules of quantum mechanics or programming.

A survey** of more than 5,400 business and IT executives established that 40 percent of respondents are taking proactive steps to prepare for quantum computing, with 36 percent planning to invest in quantum capabilities in the next two years.

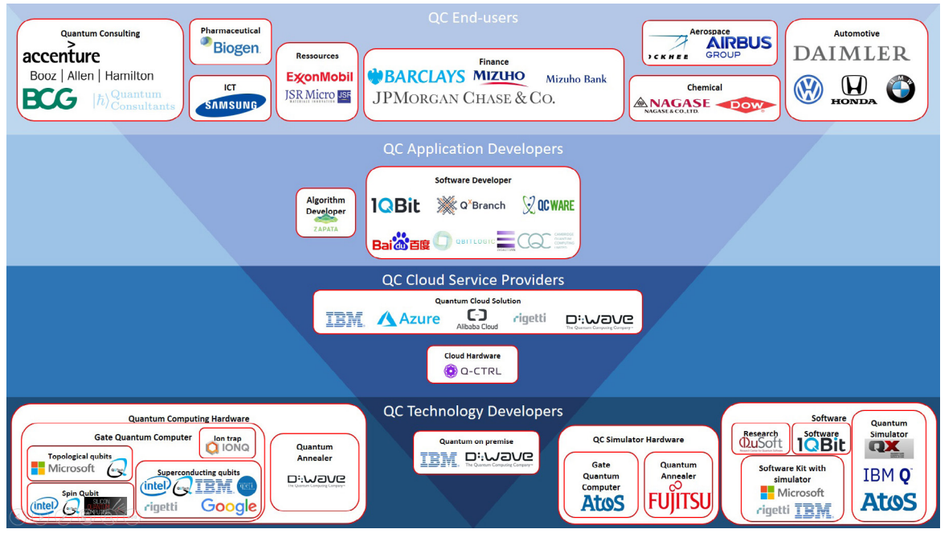
In several fields first proof of concept applications emerge from a sea of use case ideas, that point out promising directions driven by partnership initiatives between business-end-users, hard- and software-providers as well as research institutes. In this article we will focus on the financial services, life sciences and supply chain applications.

Financial services

„Banks and financial institutions like hedge funds now appear to be mostly interested in quantum computing to help minimize risk and maximize gains from dynamic portfolios of instruments," said Dr. Bob Sutor, vice president, IBM Q Strategy and Ecosystem. "The most advanced organizations are looking at how early development of proprietary mixed classical-quantum algorithms will provide competitive advantage."

* The mathematical description of quantum computers relies on matrices with entries that include real and imaginary numbers together with operations like multiplication, which transform these mathematical objects it defines a concept known as Hilbert space within the physics and mathematics community

** Accenture Technology Vision 2017



Examples for businesses with public quantum computing initiatives

Choosing assets from a portfolio of 60 assets already yields a higher number of options than there are atoms in the known universe. Significant competitive advantages could be achieved if the value of those portfolios could be efficiently calculated and the best combination of assets identified. Algorithm concepts exist that predict advantages for portfolio valuation and optimization yielding a competitive advantage, when a larger amount of possible next-day scenarios can be covered to yield precise predictions or intra-day valuations finish before the competitor establishes his numbers. As one example IBM provides software development kits to build algorithms on the quantum register level and functions for the valuation of a series of payments. First movers are the Royal Bank of Scotland, Goldman Sachs, and Citigroup have funded quantum computing startups directly. Barclays and JPMorgan Chase have been experimenting with IBM's quantum computing technology joined the IBM Q Network. Morgan Stanley articulated the bank's hope of speeding up portfolio optimizations like Monte Carlo simulations with the help of quantum computing.

Life sciences

"At Biogen, we're always looking to harness cutting-edge technologies that push the boundaries of traditional pharmaceutical research to discover new treatments and cures for complex neuroinflammatory and neurodegenerative conditions," said Govinda Bhisetti, Head of Computational Chemistry, Biogen. "Collaborating with researchers at Accenture Labs and 1QBit made it possible to rapidly pilot and deploy a quantum-enabled application that has the potential to enable us to bring medicines to people faster."

The idea to build a quantum computer coined by Richard Feynman originally resides on the pain that physicists had with efficiently simulating quantum systems. A prime example is the prediction of material properties be it a slice of silicon or a molecule. Pharma companies invest billions for trials, which would drastically reduce if one could predict the chemical properties in advance and estimate the influence on the human physiology. As a leading biotech company, Biogen is seeking to advance the development of new drugs for neurological and neurodegenerative diseases. With the price reductions chances would increase to find a live saving drug. Biogen has teamed up with Accenture Labs and 1QBit, a quantum software startup, to speed up the discovery of new drugs. The quantum molecular similarity method is a repeatable solution which can be further customized to a specific client's needs. Amgen, a biopharmaceutical company, is using quantum computers for molecular simulations. IBM has recently shown the potential of quantum-based computational chemistry with the simulation of a BeH2 molecule (beryllium hydride)[3] paving the way for simulations of more complex molecules that could help in reducing energy consumption by discovering new catalysts for fertilizer production (3% of the world energy consumption).

Supply chain

The ultimate goal of a driverless supply chain, where all aspects of end-to-end activities – planning, sourcing, production, logistics, services, and the ability to respond to risks with rapid replanning – are optimized for a single global objective across an organization frees disruptive potential to shifts the automotive

industry further towards mobility services and drives innovation initiatives: The Volkswagen Group is the world's first automaker which publicly used quantum computers, further expanding its digital competence for the future. In this context, Volkswagen Group IT is cooperating successfully with leading quantum computing company D-Wave Systems on a research project for traffic flow optimization[4]

VW CIO Martin Hofmann said in a recent interview with automotiveIT that quantum computers have "reached a stage where it becomes interesting to start developing use cases." He cited one project involving publicly available data from Beijing taxis that were used to plot optimal routes. "We were trying to prove that a particular traffic optimization problem could be addressed with a quantum computer," he said.

These are a few examples on building quantum-ready applications, which show how businesses can start innovating now by accessing existing commercial quantum computing capabilities through newly available quantum hardware platforms and software applications by leveraging teams with industry experts, advanced analytics and quantum computing specialists. Several more industry prototypes will be presented at IBM Think (February 12.-15.). In tight cooperation these low fidelity proof of concepts can be established on the time-scale of weeks to months limiting the investment and yielding insights on the execution of further quantum programs. Companies that join these first movers and start their quantum computing incubation journey now will be best positioned when the emerging technology reaches maturity.

Matthias Ziegler, Tim Leonhardt

References: **[1]** https://www.hpcwire.com/2019/01/10/ibm-quantum-update-q-system-one-launch-new-collaborators-and-qc-center-plans/ **[2]** https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/ **[3]** https://arxiv.org/pdf/1704.05018.pdf **[4]** https://guce.oath.com/collectConsent?brandType=nonEu&.done=https%3A%2F%2Fwww.engadget.com%2F2018%2F11%2F05%2Fvolkswagen-quantum-computer-traffic-management%2F%3Fguccounter%3D1&sessionId=3_cc-session_86232d-cc-f07a-450e-ab74-b7e451dbb972&lang=en-US&inline=false

Auf dem Weg zur Quantenindustrie

Einführung

Innovation bleibt nie in erfolgreichen Konzepten verhaftet, sondern bringt ständig neue Ideen hervor: Neben der künstlichen Intelligenz hat in den letzten fünf Jahren die Quanteninformationstheorie, die zur Entwicklung des Quantenbits, kurz Qubits, führte und damit die Grundlage der aktuellen Quantencomputer bildet, eine Menge Aufmerksamkeit auch außerhalb wissenschaftlicher Kreise erregt.

Fortschritte insbesondere im vergangenen Jahrzehnt haben dazu geführt, dass IBM Stand Oktober 2020 bereits 29 programmierbare Quantencomputer außerhalb von Forschungslaboren ans Netz gebracht hat und deren Rechenleistung über die Cloud bisher mehr als 260.000 Interessenten, Kunden und Partnern zur Verfügung stellt.

Obwohl die Technologie noch in den Kinderschuhen steckt, zeigen bereits diese Systeme und das vielfältige Interesse der Nutzer das Potential von Quantencomputern zur Lösung von Problemen, die selbst die leistungsfähigsten klassischen Computer wahrscheinlich auch in Zukunft nicht werden lösen können.

Um weitere wissenschaftliche Fortschritte auf diesem Gebiet zu erzielen, kommerzielle Anwendungen zu entwickeln und Fachleute in Wirtschaft und Wissenschaft auszubilden, arbeiten wir weltweit mit mehr als 125 Unternehmen und akademischen Institutionen im IBM Q Network zusammen. In Deutschland gehören dazu aktuell die Fraunhofer-Gesellschaft, die Universität des Saarlands, die Bundeswehr-Universität München, Daimler sowie der System-Integrator SVA.

Die Zusammenarbeit mit der Fraunhofer-Gesellschaft ermöglicht beispielsweise anderen Unternehmen und Forschungseinrichtungen den Zugang zu IBM-Quantencomputern in Deutschland und den USA unter dem Dach eines bundesweiten Kompetenznetzwerks. Im Rahmen der Kooperation wird dazu unter anderem ein Quantencomputer in unserem Rechenzentrum in Ehningen bei Stuttgart installiert, der unter vollständiger Datenhoheit nach europäischem Recht operiert. Das System geht im Januar 2021 in Betrieb und wird das erste seiner Art in Europa sein. Davon versprechen wir uns auch eine Initialzündung für das Thema Quantum Computing in ganz Europa, um so den Standort auch technologisch weiter voranzubringen.

Jenseits der klassischen Systeme

Für unsere Quantensysteme werden die Qubits in einem Kryostaten beinah auf den absoluten Nullpunkt abgekühlt und anschließend mit Mikrowellenimpulsen manipuliert. Damit werden sie zu Zuständen der so genannten quantenmechanischen Überlagerung, Verschränkung und Interferenz stimuliert, wie sie in der Quantenmechanik beschrieben werden.

Die Entwicklung solcher Systeme ist heutzutage noch recht aufwändig. Aber die Fortschritte insbesondere in den letzten Jahren rechtfertigen unseren Optimismus hinsichtlich eines breiten Einsatzes von Quantentechnologien. Unser Team hat allein in den letzten drei Jahren das Quantenvolumen – ein Leistungsindikator, der die Anzahl der Qubits und auch die sogenannte Fehlerrate des Systems berücksichtigt - jedes Jahr verdoppelt. Aktuell stehen wir bei einem Quantenvolumen von 64. Allein diese Erfolge kann man als frühes Anzeichen für das Quantenäquivalent des Moore'schen Gesetzes sehen. Wir bezeichnen diesen Trend liebevoll als „Gambetta's Gesetz" - benannt nach dem IBM Fellow und Leiter unseres Quantum-Teams bei IBM Research, Jay Gambetta.

Neben dem Quantenvolumen gewinnen auch sogenannte Quantenschaltkreise als Messgröße für die Leistungsfähigkeit eines Systems an Bedeutung. Sie bilden die grundlegende Arbeitseinheit für einen Quantencomputer. In Zukunft werden Bibliotheken von Quantenschaltkreisen für Programmierer in weit verbreiteten Programmiersprachen wie C++, python oder Java zur Verfügung stehen und optimal auf die Systeme abgestimmt sein.

Quantensysteme mit ein paar Qubits können nur etwa so viel Information verarbeiten wie ein klassischer 512-Bit-Computer. Da sich die Leistungsfähigkeit eines solchen Systems aber unter anderem durch das Hinzufügen von Qubits im Idealfall exponentiell erhöht, verschiebt sich das Kräfteverhältnis sehr schnell zu Ungunsten klassischer Computer. Bei perfekter Stabilität könnten Quantenrechner mit 300 Qubits in der Lage sein, mehr Datenwerte zu repräsentieren als es Atome im beobachtbaren Universum gibt. Das geht weit über die Fähigkeiten einer beliebigen Bit-basierten IT-Architektur hinaus.

Die IBM Quantum Roadmap 2021 – 2023

Wir haben uns für die nächsten drei Jahre eine sehr ehrgeizige Agenda gesetzt, um die notwendigen Technologien für den breiten Einsatz von Quantencomputern zu entwickeln.

Dazu wird sich ein multidisziplinäres Team unserer Forscher der Lösung von Problemen in den Bereichen Herstellung, Kryogenik und Elektronik sowie der Verbesserung von Software-Fähigkeiten, wie beispielsweise der Fehlerkorrekturkodierung, widmen.

Unsere Planungen sehen vor, dass wir 2021 erstmals einen 127-Qubit-Chip mit dem Codenamen „Eagle" einsetzen. „Eagle" wird über mehrere Upgrades zur Reduzierung von Qubit-Fehlern verfügen. Dazu gehört sein einzigartiges Layout, das eine Skalierung der Anzahl der Qubits ermöglicht, die als logische Qubits zusammenarbeiten - die „fehlertoleranten" Qubits, die zum Erreichen der so genannten Quantum Advantage erforderlich sind.

Diese Skalierung werden wir im Jahr 2022 fortsetzen, wenn unser Team den 433-Qubit-"Osprey"-Prozessor vorstellt. „Osprey" wird die Grenzen der Herstellungstechniken und die Möglichkeit, kleinere Chips mit mehr logischen Qubits zu bauen, erweitern, ohne dass die Leistung darunter leidet.

Unser Chip mit dem Codenamen „Condor" wird im Jahr 2023 mit seinen 1121 Qubits ein Meilenstein für die Weiterentwicklung rauschärmerer Qubits sein. Mit ihm werden wir zeigen können, dass Quantencomputer für den Einsatz in der Wirtschaft bereit sind.

Die zusätzlichen Verbesserungen in der Kryogenik und der Qubit-Kontrolle für diesen Chip sowie des dazu gehörigen rund drei Meter hohen und zwei Meter breiten Kühlelements namens „Goldeneye" ermöglichen nach unserer Vorstellung auch die für eine vollständige Fehlertoleranz erforderliche Skalierung für Systeme, die Millionen Qubits ansteuern können.

Wohin wird uns das über das Jahr 2023 hinaus hinführen? Wir können uns vorstellen, dass es Quantenverbindungen zwischen Systemen mit den oben erwähnten Millionen-Prozessor-Chips geben wird – ähnlich den Intranets, die heute bereits in Rechenzentren die Supercomputing-Prozessoren miteinander verbinden. Es wäre die Schaffung eines massiv parallelen, fehlertoleranten Quantencomputers, der in der Lage ist, die Welt zu verändern und die Basis für eine eigenständige Quantenindustrie zu bilden.

Mögliche Anwendungen

Die enorme Rechenleistung von Quantencomputern hat das Potenzial, exponentielle Fortschritte beim Thema künstliche Intelligenz freizusetzen.

KI-Systeme arbeiten umso genauer, je größer die Datenmengen sind, die von den Algorithmen des maschinellen Lernens, die sie trainieren, klassifiziert und analysiert werden können.

Je präziser diese Daten nach bestimmten Charakteristika oder Merkmalen eingeordnet werden können, desto präzisere Ergebnisse werden im Anschluss durch die KI geliefert.

Beim maschinellen Lernen sind vor allem sogenannte Merkmalsräume interessant - mathematische Räume, die ein Objekt durch seine Messwerte in Bezug auf dessen besondere Eigenschaften bestimmen. Quantensysteme bieten alternative Wege, um einen solchen Raum zu betrachten.

Unser Team erforscht auch, wie Qubits mit Neuronen inspirierten Algorithmen für maschinelles Lernen gepaart werden können. Dafür haben sie bereits einen binären Klassifikationsalgorithmus entwickelt, der bis zu 100 Prozent Genauigkeit auf einem künstlichen Datensatz erreicht.

Mit Hilfe von Quantenrechnern werden aber nicht nur bekannte, bisher unlösbar erscheinende Probleme geknackt werden, sondern auch grundlegend neue Entdeckungen möglich sein.

Nehmen wir zum Beispiel die Chemie. Die Simulation selbst einer relativ einfachen Verbindung wie Koffein würde ein klassisches IT-System mit so vielen Bits erfordern, wie es Atome in der Milchstraße gibt.

Wir haben eine Methode entwickelt, bei der Quantensysteme so eingesetzt werden können, dass dort rechnerisch schwierige Aufgaben ablaufen, während die anderen Teile einer Simulation weiterhin auf klassische Rechner ausgelagert und verarbeitet werden.

So kann beispielsweise heute schon das Verhalten von kleinen Molekülen wie Lithiumhydrid simuliert werden. Wenn eines Tages Hunderte oder gar Tausende von Qubits zusammenarbeiten, um Informationen zu verarbeiten, könnten diese Maschinen alle möglichen natürlichen Systeme simulieren, die wir heute bestenfalls annähernd kennen. Wir könnten sofort wissen, wie sich ein bestimmtes Medikament auf unseren Körper auswirkt. Wir könnten effizientere Batterien bauen,

Dr. Mark Mattingley-Scott, IBM Quantum Ambassador Leader for EMEA and Asia-Pacific, IBM

um ein nachhaltigeres Energienetz zu schaffen oder bessere Düngemittel, um die weltweite Nahrungsmittelversorgung zu verbessern.

Quantensysteme könnten auch eingesetzt werden, um effiziente Logistikabläufe zu schaffen, Finanzportfolios dynamisch zu optimieren oder die Materialforschung voranzutreiben.

Gemeinsam Nutzen schaffen

Ein wichtiger Teil des Weges hin zu einer Zukunft mit Quantenrechnern ist der Aufbau einer entsprechenden Interessensgemeinschaft. Wir müssen ein kollektives Gespür und Wissen dafür entwickeln, was Quantum Computing bedeutet und was es kann.

Denn: Ein klassischer, analytischer Algorithmus ist so etwas wie ein Rezept. Er folgt einer Reihe von Schritten, und am Ende erhält der Anwender ein Ergebnis. Ein Quantenalgorithmus ist anders: Hier arbeitet man mit probabilistischen Algorithmen, die keine eindeutigen Ergebnisse, sondern Wahrscheinlichkeiten für bestimmte Ergebnisse liefern.

Hunderttausende von Interessierten haben in den letzten Jahren bereits die IBM Quantum Experience genutzt, um dort erste Erfahrungen zu sammeln. Mehr als 250 wissenschaftliche Arbeiten wurden infolgedessen veröffentlicht. Kurz: Die Interessensgemeinschaft zum Thema wächst.

Und wo Interessierte und Wissenschaftler vorangehen, folgen oft auch Unternehmen: In den letzten zwei Jahren wurden weltweit etwa 100 Startups im Bereich Quantum Computing gegründet. Eine Analyse der Boston Consulting Group sagt voraus, dass Quantencomputing bis 2024 einen Markt von fünf Milliarden Dollar, bis 2029 von 50 Milliarden Dollar und ein Jahrzehnt später von 450 Milliarden Dollar darstellt.

Wir haben unter anderem deshalb den Bereich IBM Quantum aufgebaut, der sich darauf konzentriert, wissenschaftliche und kommerzielle Anwendungen von vielen globalen Unternehmen wie JPMorgan Chase und Daimler auf diesem Gebiet zu unterstützen. Der deutsche Autobauer nutzte einen Quantencomputer, um beispielhaft das Dipolmoment von drei Lithium-haltigen Molekülen zu modellieren. Das kann uns alle einen Schritt näher an die nächste Generation von Lithium-Schwefel-Batterien (Li-S) bringen, die leistungsfähiger, langlebiger und billiger als die heute weit verbreiteten Lithium-Ionen-Batterien für Elektrofahrzeuge sein werden.

Viele unserer Kooperationspartner im oben erwähnten IBM Q Network nutzen die Möglichkeit, mit unseren Forschern zusammenzuarbeiten, um potenzielle Anwendungen für die Technologie auszuloten und mit Hilfe von Qiskit, einer modularen Open-Source-Programmierumgebung, auf unsere Quantensysteme zuzugreifen.

Zusammenfassung

Klassisches, Bit-basiertes Computing hat unsere Welt in den letzten 50 Jahren vollständig verändert. Wir sind überzeugt, dass Quantencomputing Möglichkeiten eröffnen wird, die weit darüber hinaus gehen.

Wir stehen erst am Anfang eines langen Weges. Aber die theoretische Untermauerung und das Fundament der Technologie sind sehr solide. Die Herausforderung besteht jetzt darin, die Leistungsfähigkeit unserer Systeme weiter auszubauen, zu lernen, sie effizient zu programmieren und sie zur Lösung der dringlichsten Herausforderungen in Wissenschaft, Wirtschaft und Gesellschaft einzusetzen.

Mark Mattingley-Scott

Revolutioniert Quantencomputing die Finanzwelt nachhaltig?

In Wissenschaftskreisen wird Quantencomputing schon seit mehr als zwei Jahrzehnten als die Technologie der Zukunft beschworen. Mittlerweile setzt auch die Industrie auf die Revolutionierung der IT durch Qubits. Gerade die Finanzwirtschaft mit immer komplexer werdenden Berechnungen und Prognosen könnte von der erheblich kürzen Berechnungszeit profitieren, die Quantencomputer versprechen. Erstaunlich dabei: Bei einigen Technologien ergeben sich zusätzlich deutliche Energieeinsparungen. Dieser Beitrag beleuchtet das Thema Quantencomputing aus der Perspektive der Finanzwirtschaft, zeigt mögliche Einsatzgebiete und Rechnerarchitekturen und erläutert, auf was es beim Aufbau der Lösungen in Rechenzentren zu achten gilt bzw. wo die Vorteile der Technologie liegen.

Was ist Quantencomputing?

Quantencomputing basiert auf den Gesetzen der Quantenmechanik, die erstmals zu Beginn des 20. Jahrhunderts entdeckt wurden und die die Welt in den mikroskopischen Dimensionen von Atomen und Molekülen beschreiben. Praktisch angewendet werden die quantenmechanischen Effekte heutzutage beispielsweise in Magnetresonanztomographen oder LEDs (light emitting diode). Das Quantencomputing selbst basiert auf individuellen quantenmechanischen Phänomenen. Betrachtet man das Quantencomputing im Vergleich zu der klassischen Digitaltechnik, besteht der größte Unterschied im kleinsten Baustein: dem Bit im Vergleich zum Qubit. Während ein Bit genau einen seiner zwei Basiszustände annimmt – Null oder Eins – kann ein Qubit auch eine Überlagerung der Basiszustände annehmen. Diese bezeichnet man als Superposition. Die Qubits sind zudem in der Lage, sich gemäß den Gesetzen der Quantenmechanik zu verschränken. Diese einzigartige Eigenschaft des Quantencomputing wird genutzt, um komplexe Probleme durch verschränkte Zustände so abzubilden,

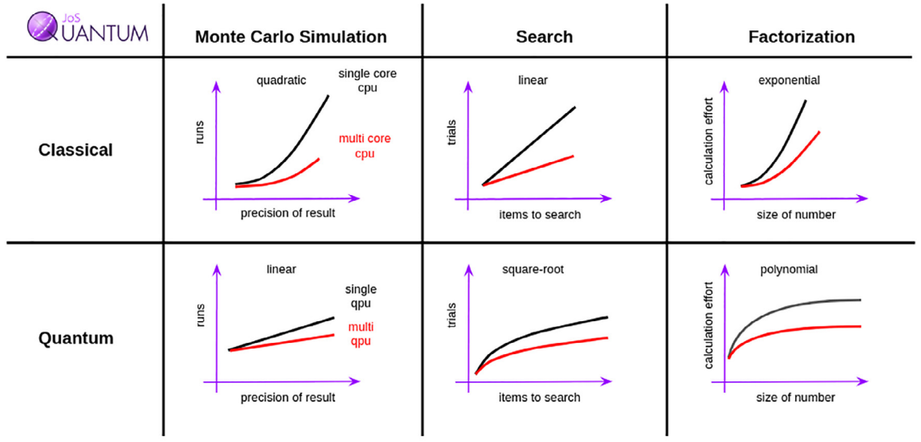


Abb. 1: Wie skaliert die Performance klassischer Algorithmen im Vergleich zur Quantenalgorithmen. Die Darstellung zeigt eine abstrakte Sich der Komplexität und lässt sich auf zahlreiche Anwendungsfälle übertragen (Quelle: JoS Quantum)

dass Information, einfach gesagt, parallel verarbeitet werden kann. Gelingt dies, lassen sich mit Quantenalgorithmen Rechenzeit einsparen und Antworten auf Probleme finden, die sich mit aktuellen Technologien nicht lösen lassen.

Worauf basiert Quantencomputing?

Quantencomputing erfordert einerseits die entsprechende Quanten-Hardware, andererseits spezielle Algorithmen, die individuell entwickelt werden müssen. Nur zehn Jahre nachdem die ersten Ideen zum Quantencomputing ausgetauscht wurden, veröffentlichte Peter Shor 1994 für die AT&T Bell Labs den ersten überlegenen Algorithmus zur Faktorisierung von Integerzahlen. Was auf den ersten Blick nach einer rein wissenschaftlichen Fragestellung aussieht, erweist sich bei näherer Betrachtung als Problem mit praktischer Relevanz: Die Faktorisierung bzw. die Berechnung diskreter Logarithmen bildet die Basis moderner Kryptographie. Allerdings erfordern die Algorithmen fehlerfreie bzw fehler-korrigierte Qubits. Derart „perfekte“ Qubits kann man realisieren, indem man mehrere Qubits mit geringen Fehlern zu sogenannten logischen Qubits zusammenfasst. Mit speziellen Algorithmen kann man dann Fehler in einzelnen Qubits detektieren, und auf Ebene des logischen Qubits Quantenspeicher mit geringerer Fehlerrate schaffen. Als Herausforderung erweist sich jedoch, dass sich damit die Rechenzeit und die erforderliche Anzahl von Qubits erhöhen. Aus diesem Grund setzen Entwickler aktuell verstärkt auf Optimierungs-Algorithmen, die auch auf nicht-fehlerkorrigierten Qubits arbeiten können. Diese Algorithmen nutzen hardwareseitig hybride Computing-Architekturen bestehend aus klassischen IT-Systemen und Quantenrechnern. Quantencomputer werden eingesetzt, um die eigentlichen, sehr komplexen Aufgaben zu lösen, während klassische Computersysteme das Feintuning der Quantenalgorithmen übernehmen. In diesem Setup lassen sich bereits heute Quantenalgorithmen entwickeln und testen, die perspektivisch für Business-Anwendungen genutzt und einfach an die zukünftige Quantencomputer angepasst werden können.

Welche Finanz-Anwendungen lassen sich optimieren?

Die Herausforderungen des Quantencomputing zeigen sich bei einer praktischen Umsetzung: Welche Anwendungsprobleme lassen sich sinnvoll mit Quantencomputern lösen? Was muss bei der Entwicklung des Algorithmus beachtet werden? Welche Hardware ist verfügbar? Um Anwendern diese Fragen beantworten und pragmatische Lösungen an die Hand geben zu können, schlossen sich verschiedene Anbieter (AQT, JoS QUANTUM, SVA System Vertrieb Alexander und NTT GDC) zu einem Pilotprojekt zusammen und erarbeiteten gemeinsam im Technology Experience Lab von NTT Global Data Centers in Frankfurt ein Konzept für Anwendungen des Quantencomputing. Da die Technologie gerade in Hinblick auf komplexe finanzmathematische Berechnungen deutliche Vorteile verspricht, wählte man exemplarisch Finanz-Anwendungen als Ausgangspunkt:

Bei der Optimierung eines Investment Portfolios gilt es eine Vielzahl von Parametern zu berücksichtigen. Eine Investitionssumme soll auf verschiedene Assets so verteilt werden, dass ein hoher Return on Investment erzielt und gleichzeitig das Risiko minimiert wird. Sollen dabei jedoch diskrete Stückzahlen berücksichtigt werden (was näher an der Realität ist),

Dominik Friedel, Business Development Manager, NTT Global Data Centers

Juris Ulmanis, Senior Research Leader, AQT GmbH

Niklas Hegemann, Geschäftsführer, JoS QUANTUM GmbH

Christopher Zachow, System Engineer Quantum Computing, SVA System Vertrieb Alexander GmbH

Abb. 2: Links ein Ionenfallen-Computer von AQT. Ionenfallen Quantenprozessor in einem 19“ Rack (rechts).

liefern klassische Algorithmen trotz langer Laufzeiten meist keine optimalen Ergebnisse. Gilt es nun auch noch stochastische Werte, wie z.B. Zinsentwicklungen, wirtschaftliche Faktoren und Unsicherheiten bei der erwarteten Rendite als Eingangsparameter zu berücksichtigen, wird aus dem gemischt-ganzzahligen ein stochastisches Optimierungsproblem. In diesem Fall können Quantencomputer die Unsicherheiten der Eingangsparamater innerhalb der Optimierung berücksichtigen, um damit die kombinatorische Optimierung effizienter zu lösen und bessere Ergebnisse in kürzerer Zeit zu erzielen.

Das gleiche gilt auch für hochdimensionale Monte-Carlo-Simulationen, wie sie beispielsweise für die Evaluation von Finanzinstrumenten genutzt werden. Dabei müssen Millionen unterschiedlicher Szenarien entwickelt und deren Ergebnisse kalkuliert werden. Daraus ergibt sich eine Verteilung, aus der Risikokennzahlen und Erwartungswerte bestimmt werden. Mittels Quantenalgorithmen kann die Simulation der Szenarien und der damit verbundenen Risiken deutlich beschleunigt bzw. durch die Berücksichtigung einer größeren Anzahl an Möglichkeiten genauer kalkuliert werden. Diese Arten der Simulationen lassen sich nicht nur für die Preisberechnung von Derivaten, sondern für alle Arten von Risiken – beispielsweise von systemischen und Kreditrisiken – verwenden. Generell gibt es eine große Zahl an Anwendungsbereichen für Monte-Carlo Simulationen, auf die zurückgegriffen wird, falls eine analytische Lösung nicht einfach möglich ist. Für alle diese stochastischen Prozesse lassen sich zukünftig Quantencomputer einsetzen.

Wie lassen sich diese Anwendungen mit Quantencomputern umsetzen?

Softwareseitig erfordert die Entwicklung von Algorithmen für das Quantencomputing – ganz gleich ob für Finanzanwendungen oder andere Applikationen – tiefgreifendes Know-how, das bislang in den wenigsten Unternehmen vorhanden ist. Gemeinsam mit externen Experten lässt sich dieses aber mittelfristig aufbauen, und dies sehr kosteneffizient. Stellt sich nun die Frage nach der geeigneten Hardware für das Quantencomputing. Hier gibt es unterschiedliche Ansätze: Schon heute sind cloudbasierte Lösungen verfügbar, die es erlauben, lokale Software-Development-Kits auf einem Laptop mit einem Quantenrechner in der Cloud zu verbinden. Für Anwendungen der Banken- und Versicherungsbranche ist deren Nutzung allerdings kritisch, da hohe sicherheitstechnische Auflagen erfüllt werden müssen. In der Regel benötigen die Algorithmen als Eingangswerte sensible Daten, die es – wie auch die Ergebnisse der Berechnungen – vor unerlaubten Zugriffen zu schützen gilt. Zudem muss auch die Frage nach dem geistigen Eigentum gestellt werden; in einer öffentlichen Cloud für Quantencomputing kann dies in der Regel nur schwierig ausreichend geschützt werden.

Im Rahmen der nachfolgenden Abschnitte beleuchten wir aus diesem Grund Ionenfallen-basierte Quantencomputer. Hier entstehen die Qubits, indem die Ionen in einer mikrostrukturierten Falle gefangen und mit hoch-fokussierten Laserstrahlen kontrolliert werden. Diese Technologie bietet mehrere Vorteile: Sie arbeitet einerseits sehr zuverlässig und lässt sich gleichzeitig sehr gut standardisieren, lokal installieren und auch aus der Ferne warten. Mehr noch: Sie arbeitet nachhaltig und autark.

Warum ist Quantencomputing mit Ionenfallen-Technologie nachhaltig?

Quantencomputer basierend auf der Ionenfallen-Technologie sind schon heute verfügbar und lassen sich in einem klassischen 19“ Rack im Rechenzentrum einbauen. Ein gesamtes System benötigt nur zwei

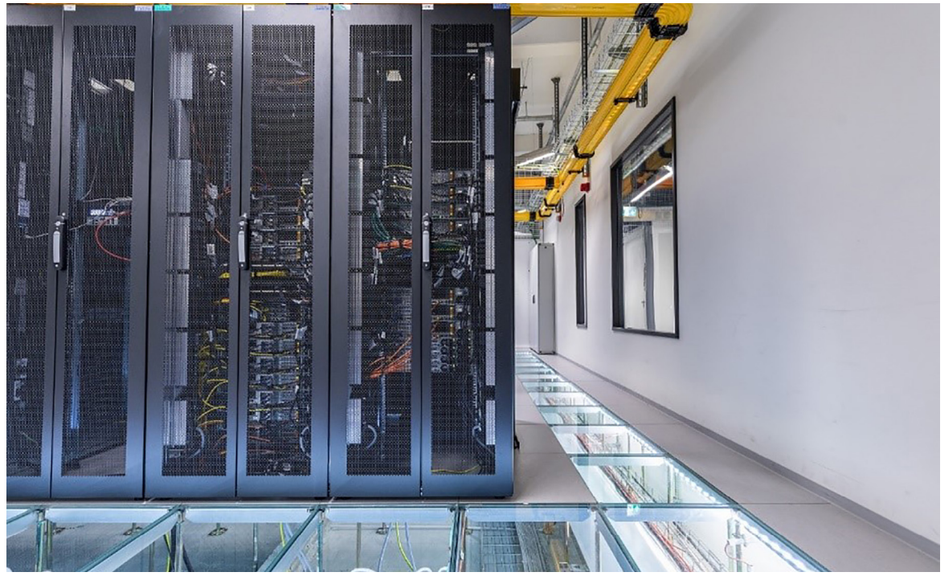


Abb. 3: Im Technology Experience Lab lassen sich Quantencomputer in sicherer Umgebung testen (Quelle: NTT Global Data Centers).

komplette Serverschränke und damit weniger als 4 Quadratmeter Rechenzentrumsfläche. Erstaunlich ist der Energieverbrauch. Er liegt bei dem beschriebenen System bei weniger als 3 kW und steigt auch bei höherer Rechenleistung nicht signifikant an. Damit wird der Dauerbetrieb nicht nur günstiger in Hinblick auf die verbrauchte Leistung für die Recheneinheit, es entsteht insgesamt weniger Abwärme. Auch die Betriebstemperatur erweist sich als vorteilhaft: Während supraleitende Qubits Elektronik erfordern, die typischerweise in einem Temperaturbereich rund um den absoluten Nullpunkt bei etwa 0,1 Kelvin (also Minus 273,1 Grad Celsius) arbeitet, liegt die Betriebstemperatur der ersten Ionenfallen-Quantenrechner im Bereich der normalen Raumtemperatur zwischen 20 und 25 Grad. Energieintensive Kühlungssysteme, z.B. auf Helium-Basis, sind hier nicht erforderlich. Eine Realisierung der oben aufgezeigten Finanz-Applikationen mittels der Ionenfallen-Quantencomputer erweist sich demzufolge in mehrfacher Hinsicht als nachhaltig:

- Geringer Stromverbrauch bei hoher Rechenleistung
- Keine aufwendige Kühlung erforderlich wie bei Supraleitern
- Installation vor Ort möglich

Gibt es spezielle Anforderungen an Rechenzentren?

Unternehmen und Organisationen, die erste Anwendungen mit Quantencomputern testen möchten, können dies mit Ionenfallen-Computern einfach realisieren. Bei der Wahl, wo die Systeme betrieben werden sollen, gilt es allerdings fünf wesentliche Aspekte zu berücksichtigen:

Sicherheit - Finanzinstitute arbeiten mit sensitiven Daten und jede Entscheidung darüber, wo sich diese Daten befinden, muss sicherstellen, dass ein sehr hoher Sicherheitsstandard eingehalten wird. Die Daten müssen auf in einer hochsicheren Umgebung gespeichert und verarbeitet werden, die sowohl gegen Angriffe durch Menschenhand, aber auch vor Naturkatastrophen oder Stromausfällen geschützt ist. Damit wird die konstante Stromversorgung der Systeme gewährleistet.

Compliance – Die Mehrzahl finanztechnischer Anwendungen laufen unter regulatorischer Kontrolle. Sowohl Banken als auch Versicherungen unterliegen Regeln, wie der FISMA, PCI DSS, ISAE3402; etc.; für die Verarbeitung von Zahlungen erfordert es bei IT-Prozessen zudem, dass sie gemäß ISO 27001 BSI funktionieren.

Zugangsprüfungen – Die Daten müssen vor dem Zugriff Unbefugter geschützt werden. Strikte Zugangskontrollen sind dafür unerlässlich. Geht man davon aus, dass hier sensible Finanzdaten verwendet werden, gilt es besondere Vorsicht walten zu lassen.

Stabile Umgebung – Um den kontrollierten und sicheren Betrieb der Quantenrechner zu gewährleisten, sollten die Systeme auf einem Untergrund gestellt werden, der Vibrationen minimiert und andere Einflüsse aus der Umgebung abschirmt. Weiterhin ist eine konstante Temperatur zwischen 20 – 25 Grad Celsius essenziell.

Konnektivität – Noch gibt es nur wenige spezielle Quantenübertragungen (z.B. Quantum Internet) über größere Distanzen. Vielmehr werden die Ergebnisse direkt in klassische IT verständliche Bits umgewandelt

und kommuniziert. Eine schnelle und zuverlässige Netzwerkanbindung sowie – abhängig von der jeweiligen Applikation – eine direkte Anbindung an Internetknoten und Cloud-Services werden empfohlen.

Berücksichtigt man diese fünf wesentlichen Aspekte, bietet sich gerade für eine so neue Technologie wie das Quantencomputing der sichere Betrieb in einem professionell betriebenen Colocation-Rechenzentrum an.

Wie lässt sich Quantencomputing risikolos testen?

Die Chancen des Quantencomputing zu erkennen ist das eine, sie konkret zu ergreifen das andere. Gerade für Finanzinstitute stellt sich auch hier die Frage nach der Sicherheit: Keinesfalls sollen Produktivsysteme durch Testszenarien gefährdet werden. Doch wer die Technologie langfristig nutzen möchte, sollte schon jetzt Erfahrungen sammeln. NTT Global Data Centers bietet aus diesem Grund in mehreren Rechenzentren sogenannte Technology Experience Labs an, in denen mehr als 100 unterschiedliche Soft- und Hardware-Partner eigene Systeme implementieren und anderen Unternehmen für Tests und Innovationsprojekte zur Verfügung stellen. In diesem Beispiel ermöglicht es die Implementation des Testszenarios für Quantenrechner im Technology Experience Lab – direkt in einem sicheren Colocation-Rechenzentrum – Unternehmen, eigene Algorithmen für Quantencomputing zu entwickeln, die entsprechende Hardware und gleichzeitig die Nachhaltigkeit der Technologie zu testen.

Ausblick

Quantencomputer sind längst keine Science-Fiction mehr. Insbesondere die Entwicklung der Quantencomputer basierend auf der hier dargestellten Ionenfallen-Technologie bietet greifbare Chance für viele Unternehmen, darunter auch Finanzinstitute und Versicherungen. Die Hardware lässt sich individuell und autark installieren und betreiben. Wie klassische IT-Systeme ist ein stabiles und sicheres Umfeld erforderlich. Belohnt werden die Unternehmen mit nachhaltigen Rechensystemen, die sich einfach in sicheren Colocation Rechenzentren betreiben lassen, die zukünftigen Anforderungen in Hinblick auf Rechenleistung erfüllen und gleichzeitig den Stromverbrauch reduzieren.

Dominik Friedel, Juris Ulmanis. Niklas Hegemann, Christopher Zachow

Revolution der Computertechnologie und Evolution für die Analyse komplexer Daten

Es ist jetzt an der Zeit, sich intensiv mit Quantencomputern zu beschäftigen. Quantumcomputing könnte für Ihr zukünftiges Geschäft sehr relevant werden.

Quantumcomputing – eine Form der Datenverarbeitung

Quantumcomputing ist eine grundlegend andere Art der Datenverarbeitung.[1,2] Quantencomputer verarbeiten Daten nicht nach einer binären Logik mit Einsen und Nullen. Stattdessen verwenden diese Computer quantenmechanische Objekte, Qubits genannt und gewinnen durch quantenmechanische Effekte, z. B. Superposition und Verschränkung, eine potenziell exponentielle Beschleunigung der Berechnung.

Aber verspricht die exponentielle Natur des Mooreschen Gesetzes nicht eine hinreichende Beschleunigung für rechnerische Aufgaben? Wir sagen nein, da die Standard-Computertechnologie nahe an einigen inhärenten Grenzen liegt. Ein Hauptgrund ist die Miniaturisierung von Schaltkreisen und Komponenten. Die Transistoren auf Siliziumbasis haben eine physikalische Grenze für ihre Strukturgrößen, die bei etwa fünf Nanometern liegt. Bei dieser Größe tritt ein quantenphysikalisches Phänomen namens „Tunneleffekt“ auf. Andere Materialien, wie Molybdändisulfid, können Transistoren mit einer Strukturgröße von bis zu einem Nanometer realisieren.[3]

Zudem stoßen die Herstellungsverfahren an ihre Grenzen, obwohl die Hersteller in neue Materialien und Methoden investieren, um den „Tunneleffekt“ zu umgehen.

Selbst wenn die derzeitigen Computer ihre Leistungsfähigkeit weiter erhöhen, sind bestimmte Rechenoperationen aufgrund ihrer Komplexität durch klassische Verfahren praktisch nicht durzuführen.

Ein aktuelles Schwerpunktthema der Digitalisierung ist die Analyse von komplexen, unstrukturierten Daten. Viele Unternehmen verdienen durch das Sammeln, Analysieren und Bearbeiten von Daten viel Geld. Um die wachsenden Datenmengen schneller verarbeiten zu können, ist ein grundlegender Wandel in der Berechnungstechnik notwendig, der Ihr Unternehmen möglicherweise beeinträchtigen und Ihren Wachstumspfad unterbrechen würde.

Die größten Probleme in den oben genannten Bereichen sind durch die Menge der Daten, ob strukturiert oder unstrukturiert, gegeben. Diese können nicht schnell genug oder gar nicht verarbeitet werden, trotz bestimmter Methoden, wie u. a. Clusterbildung, Strukturerkennung oder die Erstellung von Korrelationen. Ein Hoffnungsträger sind Mechanismen aus dem maschinellen Lernen. Die neue Technologie auf dem Gebiet der Quantencomputer könnten dazu noch einen signifikanten Impuls und sogar eine exponentielle Beschleunigung versprechen.

Beim maschinellen Lernen geht es hauptsächlich um das Klassifizieren und Erkennen von Mustern oder bestimmten Clusterungen solcher Daten ohne Nachahmung der Prozesse, die die Daten erzeugt haben. Durch diese sogenannten „generativen Algorithmen“ wurde ein neues Kapitel für Anwendungen des maschinellen Lernens aufgeschlagen. Damit ist ein großer Schritt getan, damit die Maschinen nicht nur die Daten auswerten, sondern auch neue Ergebnisse generieren, d. h. Daten kreieren. Die Möglichkeit wäre gegeben.

Aktuelle Grenzen für Quantencomputer

Aber warum ist das Quantumcomputing nicht bereits Realität? Und was können Quantencomputer in ihrem derzeitigen Entwicklungsstand leisten?

Wir befinden uns in einer Übergangsphase, in der das Quantumcomputing immer mehr Aufmerksamkeit erregt. Für eine erste Demonstration im Jahr 2019 realisierte Google eine Berechnung von Zufallszahlen mit einem Quantencomputer. Ihre Beispielanwendung sollte zeigen, dass die „Quantum Supremacy“, also die Überlegenheit eines Quantencomputers, keine theoretische Aussage mehr ist. Der Quantencomputer war in der Lage, eine Berechnung in etwa 200 Sekunden durchzuführen, für die ein herkömmlicher Computer 10.000 Jahre gebraucht hätte.[4] Laut Google wären die Kosten um einen Faktor von 1.000 reduziert worden.[5]

Der Fakt, dass ein Quantencomputer schneller arbeitet als ein herkömmlicher Computer, bedingt per se noch keinen Nutzen, ist aber jedoch ein Vorgeschmack auf das, was kommen könnte. Derzeit sind die Hardware-Geräte noch zu klein, und die Anzahl der Qubits und die Anzahl der Operationen sind zu begrenzt, um reale Anwendungsfälle auf Quantencomputern auszuführen.

Werden also Quantencomputer bald die klassischen Computer ersetzen? Die einfache Antwort lautet nein. Google hat mit seinem veröffentlichten Experiment bewiesen, dass es Probleme gibt, die nur mit einem Quantencomputer in angemessener Zeit gelöst werden können. Es geht nicht um die allgemeine Vormachtstellung von Quantencomputern, sondern mehr um die prinzipielle Überlegenheit in einigen Fällen.

Aber mit der Existenz des Quantenvorteils gibt es einen guten Grund, bald weitere bahnbrechende Neuigkeiten auf dem Gebiet der Quantenberechnung zu erwarten.

Wann müssen Sie sich mit dem Thema Quantumcomputing befassen?

Besser früher als später. Es kann Jahre dauern, das Wissen über das Gestalten und Konstruieren von Quantenberechnungen zu erlangen und aufzubauen. Die Implementierung einer Governance, die sich mit der Verfügbarkeit von Quantumcomputing befasst, kann bei den meisten etablierten Unternehmen langwierig sein.

Die Operationen und Berechnungen traditioneller Computer lassen sich mit unserer täglichen Erfahrung mit physikalischen Prozessen beschreiben. Quantencomputer nutzen jedoch quantenmechanische Phänomene. Die Gesetze der Quantenphysik stehen oft im Widerspruch zu unseren täglichen Beobachtungen, was diese Prozesse nicht intuitiv und nur schwer nachvollziehbar macht. Weitere Forschung ist notwendig, um die Grenzen und Möglichkeiten vollständig fehlerkorrigierter Quantencomputer zu entdecken.

Die derzeitige Quantencomputer-Hardware ist nicht umfangreich und nicht fehlerresistent. Im Gegenteil, die aktuellen Geräte sind eher klein dimensioniert und fehleranfällig bei der Ausführung von Algorithmen. Dennoch, in den kommenden Jahren sollten und werden Unternehmen beginnen „quantentauglich“ zu werden und sollten Schritte zur Einbeziehung von Quantencomputern in ihre Geschäftsprozesse gehen. In vielen Bereichen werden Quantencomputer entscheidende Anwendungen und Upgrades für derzeit unlösbare Probleme finden. Sie sollten in jeder Strategy Roadmap 2030 eines größeren Unternehmens thematisch enthalten sein.

Eine Zukunft ohne Quantumcomputing ist kaum vorstellbar

Zusammenfassend ist zu sagen, dass diese neue Form der Datenverarbeitung Möglichkeiten schafft, Themen wie Risikomodellierung, Modellierung finanzieller Zeitreihen oder die Erforschung von Krankheiten effektiv und effizient mit Methoden des maschinellen Lernens zu bearbeiten. Wie schnell diese Technologie sich etabliert, bleibt abzuwarten. Es hängt von Faktoren, wie der Stabilität und Größe des Quantencomputers ab. Derzeit rechnen große Computerhersteller damit, dass bis 2025 (Honeywell) bzw. 2030 (IBM) die Quantum Supremacy erreicht wird.[6] Es könnte wettbewerbsentscheidend für Unternehmen sein, sich frühzeitig mit Anwendungsfällen zu beschäftigen, die betroffenen Themenfelder in ihren Geschäftsmodellen zu analysieren, Anwendungsfälle zu erarbeiten und eine Strategie zu entwickeln, wie das Quantumcomputing genutzt werden kann. Diese Strategie muss Richtlinien und Maßnahmen beinhalten, wie z. B. der Wissensaufbau zum Quantumcomputing in der Organisation umzusetzen ist oder wie die Berechnungen durchzuführen sind (On-Premises vs. Cloud Lösungen). Fakt ist, Unternehmen sollten sich mit dieser Technologie beschäftigen, besser jetzt als zu spät.

Stefan Pechardscheck, Kai Baumann

Referenzen: **[1]** Rieffel, Eleanor / Polak, Wolfgang: Quantum Computing: A Gentle Introduction, MIT Press, 2011 **[2]** Chuang, Isaac L. / Nielsen, Michael: Quantum Computation and Quantum Information, Cambridge University Press, 2011. **[3]** Desai, Sujay B. / Madhvapathy, Surabhi R. / Sachid, Angada B. / Llinas, Juan Pablo / Wang, Qingxiao / Ahn, Geun Ho / Pitner, Gregory / Kim, Moon J. / Bokor, Jeffrey / Hu, Chenming / Wong, H.-S. Philip / Javey, Ali: MoS2 transistors with 1-nanometer gate lengths, Science, Volume 354, 2016. **[4]** Arute, Frank / Arya, Kunal / Babbush, Ryan / Bacon, David / Neven, Hartmut / Martinis, John M.: Quantum supremacy using a programmable superconducting processor, Nature, Issue 574, 2019. **[5]** Arute, Frank / Arya, Kunal / Babbush, Ryan / Bacon, David / Neven, Hartmut / Martinis, John M.: Quantum supremacy using a programmable superconducting processor, Nature, Issue 574, 2019. **[6]** Wang, Brian: Quantum Volume is Not Over 9000 Yet, https://www.nextbigfuture.com/2020/06/quantum-volume-is-not-over-9000-yet.html, 22.07.2020.

Stefan Pechardscheck, Globaler Leiter Technologie, BearingPoint

Kai Baumann, Senior Business Consultant, BearingPoint

1.2 CYBER SECURITY

So bereitet sich die Kryptografie auf Quantencomputer vor

Das Zeitalter der Quantencomputer dämmert herauf und verspricht eine enorme Schubkraft für Wissenschaft und Forschung ebenso wie für innovative Geschäftsmodelle. Die Möglichkeiten, die Qbits eröffnen, bringen aber auch Gefahren mit sich. Malte Pollmann, Chief Strategy Officer von Utimaco, erklärt, wie sich die Fähigkeiten von Quantencomputern auf den Bereich Kryptografie auswirken und warum Unternehmen sich schon jetzt krypto-agil aufstellen sollten.

Glaubt man der Google-Forschungsgruppe um den US-amerikanischen Physiker John M. Martinis, so hat der Quantencomputer Sycamore des Suchmaschinenkonzerns Ende 2019 erstmals Quantenüberlegenheit („Quantum Supremacy“) erreicht und ist damit jedem konventionellen Rechner überlegen. Einem Problem, für das ein Supercomputer auf Basis herkömmlicher Bits 10.000 Jahre benötigen würde, werde Sycamore in nur 200 Sekunden Herr, so die Forscher in einem Beitrag im Wissenschaftsjournal Nature. Nicht zuletzt IBM-Experten stellen diese Zahlen in Frage. Doch selbst wenn die (konventionelle) Rechenzeit für das betreffende Problem nur wenige Tage betragen würde – Sycamore bleibt um den Faktor 1.000 schneller. Das ist beachtlich, denn die Technologie steckt noch immer in der Experimentierphase. Es ist nur eine Frage der Zeit, dass marktreife Quantencomputer flächendeckend reale Probleme in Angriff nehmen. Und das betrifft in besonderem Maße auch die Kryptografie.

Malte Pollmann, Chief Strategy Officer, Utimaco

Was macht Quantencomputer so schnell?

Die unvorstellbaren Geschwindigkeiten, die Quantencomputer zumindest theoretisch erreichen können, sind auf Eigenschaften der Quantenbits (Qbits) zurückzuführen, die mit unserer alltäglichen Wahrnehmung kaum nachvollziehbar sind. Zum einen offenbaren Quantenobjekte ihren Zustand prinzipiell erst bei Beobachtung – im Fall der Qbits bei einer Messung. Anders als die Bits mit dem Zustand „0“ oder „1“, auf denen die bisher bekannte Computer-Technologie basiert, haben Quantenbits also per se keinen festgelegten Zustand. Das bedeutet: Qbits können gleichzeitig 1 und 0 sein – für ihren Zustand lassen sich zunächst nur Wahrscheinlichkeiten angeben. Erst im Augenblick der Messung definiert sich der Zustand eines Qbits.

Etwas greifbarer wird dies durch ein Gedankenexperiment, bekannt als „Schrödingers Katze“: Dem Beobachter ist in diesem Beispiel nicht bekannt, in welchem Zustand sich die Katze in einer Kiste befindet. Erst, wenn er die Kiste öffnet, definiert sich für ihn ihr Zustand als „tot“ oder „lebendig“.

Zum anderen kennt die Quantenwelt das Phänomen der Verschränkung von zwei Teilchen, die in Wechselwirkung miteinander stehen. Wo diese sich dabei befinden, ist egal. Zudem entfällt die Zustandswahrscheinlichkeit für die einzelnen Teilchen – die Verschränkung erlaubt nur noch eine komplexe Wahrscheinlichkeitsbeziehung des Gesamtsystems. Sobald der Zustand von einem der verschränkten Teilchen gemessen wird, zerstört dies ihre Wechselwirkung.

Kryptografische Gewissheiten auf den Kopf gestellt

Was bedeuten die enormen Geschwindigkeiten, die sich mit Quantencomputern erreichen lassen, für die Kryptografie? Kurz gesagt: Sie haben das Potenzial, bisherige Gewissheiten, was die Sicherheit von Passwörtern und kryptografischen Schlüsseln angeht, auf den Kopf zu stellen. Bislang galten in der Kryptologie Schlüssel für sicher, die so komplex waren, dass selbst leistungsstärkste Supercomputer für deren Entschlüsselung per Brute-Force-Methode Jahrtausende benötigen würden. Dabei werden alle möglichen Problemlösungen durchprobiert, bis die richtige Lösung – also das Passwort oder der Schlüssel – „erraten“ ist. Um Passwörter gegen Brute-Force-Angreifer zu schützen, begrenzt man in der Regel die Zahl der möglichen Eingaben.

Quantenrechner lassen allein durch ihre enorme Geschwindigkeit die von konventionellen Computern für solche Problemlösungen benötigten Jahrtausende rasant dahinschmelzen – man bedenke nur den Beschleunigungsfaktor 1.000 im Falle von Sycamore. Hinzukommt, dass mit dem Grover-Algorithmus für Quantencomputer bereits ein Verfahren bekannt ist, das Suchen im Quadrat beschleunigt. Würde ein herkömmlicher Rechner bei einer Suche in einer Datenbank mit n Einträgen n Rechenschritte benötigen, dann verkürzt der Grover-Algorithmus die entsprechende Suche auf einem Quantencomputer auf √n Schritte. Bei einer linearen Suche bräuchte es etwa 2128 Rechenschritte, um eine AES-128 Verschlüsselung zu knacken – mit dem Grover-Algorithmus dagegen gerade mal 264. Auch wenn sich die Gefahr eines auf diese Weise geknackten Schlüssels eingrenzen lässt, indem man seine Länge schlicht und einfach verdoppelt, gibt es nur eine Sicherheit: Jede Verschlüsselungsmethode, die auf mathematischen Problemen beruht – so komplex diese auch sein mögen –, ist potenziell durch Quantencomputer gefährdet. Um auch in Zukunft Sicherheit zu gewährleisten, bedarf es also neuer kryptografischer Verfahren als Bollwerk gegen die weiter steigende Rechenleistung und Effizienz von Quantenrechnern.

Die fünf Ansätze der Post-Quanten-Kryptografie

Die Post-Quanten-Kryptografie arbeitet im Wesentlichen mit fünf Ansätzen, die zwar ebenfalls auf mathematischen Problemen basieren, deren Lösung aber nicht nur herkömmliche, sondern auch Quantenrechner vor echte Probleme stellt. Entsprechende Algorithmen sind längst im Einsatz, zumal einige der Verfahren für die Post-Quanten-Kryptografie – etwa Code- und Hash-basierte Schemata – schon seit mehr als 40 Jahren diskutiert und erforscht werden. Als entsprechend sicher gelten diese Verfahren. In den 1980er Jahren wurde dann die sogenannte multivariate Kryptografie entwickelt, bei der beispielsweise quadratische Gleichungssysteme mit mehreren Variablen zum Einsatz kommen. Allerdings sind nur wenige Schemata der multivariaten Kryptografie als sicher zu betrachten, was ein Hemmschuh für die Entwicklung eines effizienten Public-Key-Systems ist. Seit Ende der 1990er Jahre nutzt die gitterbasierte Kryptografie die Komplexität von hochdimensionalen Gittern, in denen es den kürzesten Vektor aufzuspüren gilt. Das jüngste Gebiet der Post-Quanten-Kryptografie ist die isogeniebasierte Kryptografie – eingeführt 2006 und verfeinert 2011: Zwischen elliptischen Kurven im Sinn von strukturerhaltenden Abbildungen sollen zur Entschlüsselung dabei Isogenien gefunden werden.

Erschwert wird die Entwicklung neuer kryptografischer Verfahren für den Alltagsgebrauch insbesondere dadurch, dass diese effizient sein müssen. Verglichen mit klassischer Kryptografie brauchen alle quantensicheren Verfahren mehr Rechenleistung, sollen potenziell aber auch auf schlankeren Geräten mit begrenzten Ressourcen wie Mobiltelefonen zum Einsatz kommen können, ohne diese in ihrer Anwendbarkeit zu sehr einzuschränken.

So sollten Unternehmen sich schon heute vorbereiten

Es ist eine Frage der Zeit, dass Quantencomputer auch jenseits von Forschungslaboren eingesetzt werden – und das nicht immer mit guten Absichten. Auch wenn stellenweise noch viel Forschungsbedarf besteht, sollten Unternehmen im Sinne eines angemessenen Risikomanagements schon jetzt entsprechende Vorbereitungen für die „Post-Quanten-Zeit“ treffen und ihre Systeme krypto-agil aufstellen. Denn eine vollständige Ad-hoc-Umstellung auf quantensichere Algorithmen wird in den wenigsten Fällen möglich sein. Daher empfiehlt es sich bereits heute, auf einen hybriden Betrieb zu setzen, in dem konventionelle und moderne Post-Quanten-Algorithmen nebeneinander laufen. Dieser erleichtert den späteren Umstieg auf quantensichere Kryptografie.

Gleichzeitig sollte die Elektronik von Produkten mit langen Lebenszyklen quantensicher „by design“ entworfen werden – etwa beim Bau von Maschinen für smarte Fabriken oder auch bei der Konstruktion vernetzter Autos. Eine Nutzungsdauer von zehn Jahren und länger setzt im Sinne des Anwenders Quantensicherheit voraus. Das gilt natürlich auch für Signaturzertifikate mit langer Laufzeit. Schon heute können und sollten an vielen Stellen quantensichere Algorithmen genutzt werden. Unternehmen, die herausfinden wollen, wie sich Post-Quanten-Algorithmen auf ihre bestehende Infrastruktur auswirken, können dies anhand von entsprechenden Werkzeugen testen.

Malte Pollmann

Quantum Computing - Quantensprung für digitale Zahlungen?

Erinnern Sie sich an den Nanotech-Hype? Zu Beginn dieses Millenniums schien die Nanotechnologie, also das Knowhow und die Produktion der Technik im Maßstab von Atomen und Molekülen, der Schlüssel zu den Problemen in der Fertigungs- und IT-Industrie. Infolgedessen verdoppelten und vervierfachten sich die Aktien von Nanotech-Firmen.

Quantum Computing basiert auf der Nanotechnologie hat so heutzutage die Rolle des Lieblingskindes bei Tech- Startups und IT-Giganten eingenommen. Für Anbieter digitaler und kontaktloser Zahlungssysteme könnten Quantencomputer einen Quantensprung bei der Abrechnung von Rechnungen ohne Bargeld bedeuten. Gerade jetzt, nachdem China im Dezember 2020 behauptete, einen Quantencomputer gebaut zu haben, der 10 Milliarden Mal (!) schneller sei als der von Google. Sollte der Geschwindigkeitsvorsprung stimmen, so lässt sich ausmalen, dass verspätete elektronische Zahlungen, die heute ausgeführt werden, aber erst einen Tag später ausgeführt werden oder verzögert auf dem Kontoauszug erschienen, bald der Vergangenheit angehören können.

Keine Alchemie

Kurz gesagt, basieren herkömmliche Computer auf dem binären Schema, das die Welt in „Einsen“ und „Nullen“ aufteilt. Quantencomputer dagegen sind imstande, die beiden Größen „1“ und “0“ als Ja/Nein-Parameter zu mischen. Diese Art der Durchmischung wurde notwendig, weil PC-Chips immer kleiner wurden, während die Bytes auf Mega-Giga-Terra wuchsen. Daher haben die kleinen Helfer in unseren Laptops und Smartphones fast ihre physischen Grenzen erreicht - wir können sie nicht einfach kleiner als Atome bauen. Dadurch sind die Quanten-Computer agiler und schneller, viel schneller als ihre herkömmlichen Kollegen. Denn das Grundprinzip hat sich bei den heutigen PCs nicht geändert, seit der deutsche IT-Pionier Konrad Zuse vor 80 Jahren den ersten programmierbaren Computer Z3 baute.

Die Experten sind sich einig, dass Quantum Computing Auswirkungen auf alle Branchen haben wird, und nicht nur auf Technologie und Fertigung, sondern von A wie Agrarwirtschaft bis Z wie zollfreier Handel. Dies schließt die Finanzindustrie und damit einen Bereich ein, der uns alle betrifft: den elektronischen Zahlungsverkehr.

Quantum Computing kann die Kryptografie, also die Verschlüsselungstechnologie von Zugangsdaten, auf die nächste Stufe heben und somit kontaktlose Zahlungen per Debit- oder Kreditkarte oder über das Smartphone ausführen. Diese Form des digitalen Geldtransfers hat seit Ausbruch der Pandemie enorm zugenommen, und er wird sich inmitten einer wachsenden Zahl von technisch versierten Millennials, die in die Arbeitswelt eintreten, weltweit fortsetzen.

Global und verschlüsselt

Laut Oscar Covers, Cybersecurity Analyst bei der Dutch Payments Association, müssen „aktuelle Programmprotokolle höchstwahrscheinlich neu gestaltet werden, um die Post-Quanten-Kryptographie optimal nutzen zu können." In einem Artikel von CyberSec Asia heißt es jedoch, dass Quantum-Computer noch einige Jahre von der Massenzugänglichkeit und -nutzung entfernt sind und dass „mit Sicherheit das Risiko besteht, dass Hacker mit irgendeiner Form der Technologie versuchen werden, einen Vorsprung erlangen."

In dem Artikel heißt es weiter: „Bereits im dritten Quartal 2020 machte die Durchdringung kontaktloser Zahlungssysteme 41% der weltweiten Kauftransaktionen weltweit aus, laut Quellen 30% mehr als vor einem Jahr."

Doch es gibt Hoffnung, denn die Bezahlanbieter haben die Initiative ergriffen. Der Kreditkartenanbieter Mastercard hat angekündigt, die „nächste Generation kontaktloser Zahlungen" zu entwickeln, damit die Verbraucher auch in den kommenden Jahrzehnten ein hohes Maß an Sicherheit und Komfort genießen können". Ajay Bhalla, Präsident der Cyber- und Intelligence-Division bei Mastercard, wurde in besagtem Artikel wie folgt zitiert: „Während sich das IT-Ökosystem weiterentwickelt, werden mehr vernetzte Geräte und das Internet der Dinge zu einer höheren Nachfrage unter den Benutzern und einen größeren Bedarf an konstanten Innovationen führen. " Er fügt hinzu, dass ein als branchenweit erstes und neues verbessertes kontaktloses Vergütungssystem dazu beitragen wird, dass sich die kontaktlose Technologie mit neuen disruptiven Technologien wie dem Quantencomputer weiterentwickelt.

Fabio Carvalho, Digital Marketing Specialist, CCV Schweiz

Einen Schritt voraus

Diese Technologien nutzen die neue „quantenresistente Technologie" durch die Implementierung von Algorithmen der nächsten Generation und kryptografischen Schlüsselstärken, während die kontaktlose Interaktion „unter einer halben Sekunde" bleibt. „Der Begriff quantenresistent könnte zunächst irritieren. Hacker versuchen jedoch, sich an neue Technologien anzupassen. Daher sind Kartenanbieter bestrebt, auf Quantenprozessoren zu setzen, während sie gleichzeitig chinesische Mauern entwickeln, um Phishing- Versuchen und Cyber-Attacken im Keim zu ersticken.

Die Mitbewerberin American Express, auch unter dem Namen Amex bekannt, stellt auf ihrer Website fest, dass diese neuen, leistungsstärkeren Quantum-Helfer viel leichter „Daten erstellen können, um Ausgabenmuster zu analysieren und neue Effizienzmaßnahmen vorzuschlagen, Anomalien zu erkennen und Einsparpotenziale zu ermitteln".

Deshalb hat der Aufstieg von Quantencomputern kontaktlose Kartenanbieter motiviert ihre Bemühungen zu beschleunigen, um eine schnelle UND sichere Anwendung der unsichtbaren Zahlung zwischen der Karte oder dem Smartphone des Kunden und dem festen oder mobilen Bezahlungsterminal zu gewährleisten. Für den Kunden hingegen ändert sich scheinbar nichts, aber die Geschwindigkeit der elektronischen Zahlungen wird die heutige Funktionsweise in den Schatten stellen.

„Die Konsumenten werden von allen Vorteilen beeinflusst, die Firmenkartenunternehmen bieten, auch wenn sie diese nicht unbedingt nutzen", zitiert Amex auf seiner Website Richard Koch, Leiter der Abteilung für Kartenzahlungsrichtlinien bei der UK Cards Association, dem britischen Verband für Bezahlkartenanbieter. „Es geht um Wettbewerbsunterscheidungsmerkmale", sagt Koch.

Der Wettbewerb um die nächste Generation von Datenprozessoren, die mehr als nur Einsen und Nullen kennen, ist derart intensive, dass die chinesische Regierung Ende 2020 ein neues Exportkontrollgesetz erlassen hat, das den Export von Verschlüsselungstechnologie und Kryptoanalyse-Tools verbietet. Dieses Verbot umfasst quantenkryptografische Hardware und Software.

Der Wettlauf wird weitergehen, weil Quantum Computing effektiv einen Quantensprung für den digitalen Zahlungsverkehr darstellt.

Fabio Carvalho

Security in the Quantum Age

The world of security and cryptography has been in relative peace until it became clear that Quantum Computing development will eventually result in usable devices. Both symmetric cryptography, for which two or more parties trust each other and possess the same key to accomplish security tasks, and that of asymmetric (or public key) cryptography have been relatively well understood. Security had been based on assumptions on the maximal power of an adversary that appeared more than reasonable. Many tools have been designed, found to be convenient and even certified from a practical security perspective and have relied on "provable" public key methods. These proofs have been based on an assumptions on complexity of specific tasks and from there the infeasibility of breaking the crypto methods in polynomial time has been deduced. Incidentally most of the wide spread public key methods have selected factoring big numbers into prime factors as the source of complexity. However, already in the ninety-nineties Peter Shor had put forward the "Shor-algorithm" that can solve in polynomial time the factorization problem on a sufficiently powerful Quantum Computer. Starting at the latest in 2013 the big security agencies, even NSA, have called for developing new methods that are "Quantum Safe", i.e. secure against adversaries equipped with Quantum Computers.

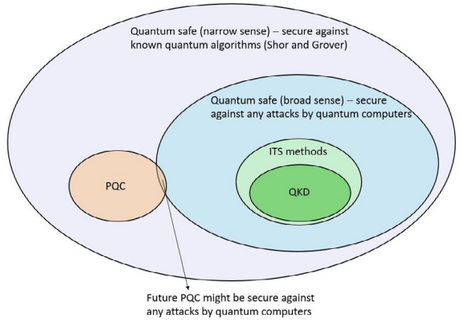
Let us try to analyze the concept of Quantum Safety. There are two abstract possibilities (see Figure):

1. Quantum Safety in the narrow sense (i.e. secure to the best of our present knowledge on the computing efficiency of prospective Quantum computers). This is a Cryptography that is secure against known, cryptographically relevant, algorithms for Quantum Computers. At present these include the Shor algorithm and the Grover algorithm. The latter is a specific search algorithm. It essentially does not affect block-encryption schemes, such as AES, except for doubling of the key space, and these are therefore automatically Quantum Safe in the narrow sense.
2. Quantum Safety in a broad sense. It should not be breakable by a Quantum Computer at any future time. Naturally, this is not a well-defined category as:

   a. the algorithms that can efficiently be executed on a Quantum Computer are principally unknown. It is often conjectured that the so called "NP hard problems" (at least as hard as any NP problem, the latter being a problem, unknown whether it can be solved in polynomial time, as function of its input, on a deterministic Turing machine) are also not solvable by a Quantum Computers in a polynomial time. In the end, however, this is only a conjecture and is based on what we do not know today;

and

   b. the method of application of a "Quantum Computer" is undefined. The "narrow sense" interpretation of a Quantum Computer implicitly assumes a kind of non-physical adversarial activity (although chosen plain attacks are not excluded), in which the communication, quantum and classical, data are supplied to a distant Quantum Computer that does calculations and provides the adversary with conclusions, e.g. the key generated in a Diffie-Hellman based protocol for subsequent direct decryption of any cipher text that is produced by a block–cipher encryption algorithm. Note, however, that this is not the only possibility, especially the attacks considered in physics-based crypto methods. More generally an adversary can possess a distributed quantum computer integrated in the user's infrastructure that also steers physical attacks.



The presently known Quantum safe methods include:

1. **Post-Quantum Cryptography (PQC).**
   Post Quantum Cryptography as presently evaluated at NIST is a set of public key algorithms. All these algorithms are related to different classes of problems, which are different from the factoring problem as well as the related discrete logarithms and elliptic curves which .are "easily solvable" by the Shor algorithm for universal Quantum Computers in the above sense. The post-quantum public key algorithms therefore are Shor-secure. It is not known publicly, whether these other fundamental problems suggested as foundational for different post-quantum versions may be susceptible to yet unknown algorithms for Quantum Computers.

However, there is a sentiment that the problems lying at the heart of present day post-quantum cryptography might have been too exotic to be addressed by a sufficient amount of researchers developing Quantum Computing algorithms up to now. This is of course a speculation. The fact is that post-quantum public key cryptography is designed to be Shor-safe and is thus Quantum Safe in the narrow sense.

2. **Quantum Key Distribution (QKD).**
   QKD is a key generation method that uses quantum mechanical effects to establish security. There are different possibilities to address
   a. In the most traditional sense QKD (put forward already in 1983 with some intuitions existing before) is considered as an Information Theoretically Secure (ITS) primitive (i.e. secure forever against any completely unlimited eavesdropper except for a negligible probability ε that can be reduced at will) with potential implementation imperfections. This is a very appealing interpretation as in theory implementation imperfections are nothing special – any crypto primitive has some qualities that are "spoiled" by implementation imperfections. Clearly an ITS scheme cannot be thwarted by any algorithm whatsoever, and not by any attack, irrespective of its specific realization (distributed or not). So clearly, in this inter-

PhD Momtchil Peev, Group Leader, Huawei Technologies Duesseldorf GmbH

PhD Fred Fung, Researcher, Huawei Technologies Duesseldorf GmbH

pretation, QKD is Quantum Safe in a broad sense. Note: This property is restricted to key generation alone.

b. QKD as a Quantum Safe Implementation in a narrow sense. It can be argued (see box) that from a security point of view, QKD is not worse than any narrow-sense Quantum Safe method. QKD is also forward secure (as most physical methods), sometimes called everlasting secure, i.e. that if it is not broken in real time, it cannot be broken later in any way. This feature is a significant improvement to all present day and Post-Quantum methods, as the output of these can be passively eavesdropped, stored and, potentially, broken later. However, we should seriously address also the practical side of QKD. On security-management levels there is the prejudice that QKD is difficult to operate, needs parallel communication infrastructures (optical fiber networks) and mainly therefore (OPEX) but also as of itself (CAPEX) is inherently and forbiddingly expensive. Some people believe: "If QKD is not ITS, it cannot be sold to the management." This is sort of skepticism is confirmed by existing products on the market. However, it is clear that this is a result of extreme narrow proliferation in niche markets and lack of sufficient R&D investment with practical orientation. Moreover, there exist examples of QKD technology that are much more convenient to use, do not require a parallel infrastructure and are significantly cheaper already now. It is also arguable, although not everyone agrees, that leaving aside some traditional ITS requirements that non-ITS QKD variants can get even more efficient and less expensive. On the positive "popular side" there are arguments by security practitioners: "We do not want something ideal (ITS). We do want something that is dauntingly difficult (practically unrealistic) to crack and we want to use such a method jointly with Post-Quantum methods. In this way we would have a 'software' backed and a 'hardware' backed security, sort of 'unbeatable' two factor crypto as of today."

Real Security and real security of QKD

Security of traditional crypto devices

Core Crypto Primitives: There are two types of crypto primitives – those based on provable security (as is e.g. public key crypto or QKD) and others based on the lack of knowledge of feasible attacks (as are block cyphers, e.g. AES). We shall review in more detail the first class here: as in any theorem there are assumptions and then a proof that is a mathematical derivation, the result of course being an implicit but direct consequence of the assumptions. In the case of public key cryptography, as already mentioned, the assumption is the complexity of a problem i.e. that for known algorithms, the inverse of an "easy" problem is of higher than polynomial complexity (as function of the length of the input). Meanwhile experts in the field have shown that there is a lot of progress in this domain (different for the specific different crypto primitives) and while the conjecture still holds it is greatly eroded even in the domain of traditional mathematical algorithms.

Implementation: It can be argued that in the case of mathematical cryptographic algorithms the core primitive is not affected by implementation as the assumptions are not. No doubt, implementation opens side channels but these can be independently tackled, by methods that do not affect the core primitive. Unfortunately this does not hold for QKD as it is a physics-based primitive. Indeed implementation affects the assumptions (particularly the first one) and then there is no easy way to prove security with unstable assumptions on system models, especially in the case of system models of increasing complexity.

QKD security

Core Primitive of QKD: The security of QKD is rooted in assumptions, most notably knowledge of the model of the QKD system, authentic message communication, availability of true random number generators, and absolute security isolation. Derivations of security proofs follow the rules of Quantum Information Theory (i.e. the hidden assumption is that Quantum theory is "correct" something that we are not going to doubt here).

The Security of QKD implementations:

There are two problems of QKD implementations. First, there are problems related to the model that in contrast to traditional security devices IS NOT unrelated to the implementation – i.e. the core primitive and the implementation are intertwined. Irrespectively of how much effort is put here (closing the obvious side channels or attempting a Security Proof to the best of our knowledge on an extended model and at the expense of decreased performance) QKD will not become secure "by the laws of nature" but rather will be a function of our description of the system. However, no matter what a QKD system cannot be broken by a distant (physically passive) computing machine running any algorithms. The machine cannot use side channels at all even if they are not closed! (This already goes at least partially in the broad sense Quantum Safety.) To break QKD one needs an elaborate and advanced, quantum attacks with direct access to the quantum channel.

Second, the isolation assumption is not reasonable as in a strict sense it would render the QKD system unusable. This problem can be avoided by using additionally post-quantum only methods and/or adequate additional isolation by organizational measures. In any case QKD will remain Quantum Safe at least in the narrow sense.

What higher security can QKD aim at beyond Quantum Safety in the narrow sense?

This is a really difficult point.

In this connection it should be considered whether cheaper and more efficient devices that are only quantum safe in the narrow sense are not worth addressing.

Moreover, it can aim at "everlasting security" if methods used that are not everlasting secure are ensured not to have an impact on key generation (possibly with organizational methods).

If we close all known side channels we shall render QKD Quantum Safe in the broader sense to the best of our knowledge. We can go even for something as ITS "to the best of our knowledge" attempting a model that captures all known side channels at any given point of time. Might be such security is not worth the effort from a practical point of view. However, this is a very interesting research line that might bring us to new insights.

At the same time the struggle for low cost, increased efficiency and applicability must continue. Last but not least we would mention that security design of QKD networks is critical as this is an essential part of realistic, non-niche applicability.

3. **Quantum Cryptography beyond QKD**

QKD is just a key generation method - nothing more. It is an essential building block in symmetric cryptography. We know, however, that it is asymmetric cryptography (in terms of use cases not methodology) that is needed to solve many of the real security problems in the modern world. Asymmetric tasks can be efficiently solved by means of public key cryptography, for which reason PQC is indispensable.

However, asymmetric Quantum Cryptography is a field of research that exists, is viable, although it is little known as of today.

All started with an early observation / proof of H.-K. Lo in the 90s that ITS asymmetric cryptography is impossible by quantum means. This led to complete disinterest to the subject among Quantum Information scientists. However, around 2005 L. Salvail came with an ingenious scheme. If one uses QKD hardware, changes the post-processing and assumes an eavesdropper with limited quantum resources (limited quantum storage or noisy quantum memory) then he/she can realize bit-commitment and oblivious transfer – the sufficient building blocks for realizing any asymmetric crypto primitives. Later preliminary experimental tests of these protocols and extensions to identification (C. Schaffner et al.) have been carried out. Unfortunately, hitherto these themes have remained very little studied.

The bottom-line is that there is a significant but not sufficiently studied potential for QKD hardware to be used for classes of cryptography other than key generation. It appears that the resulting schemes, even if not ITS would probably turn out to be Quantum Safe.

PhD Momtchil Peev, PhD Fred Fung

Kryptoagilität zum Schutz vor Quantencomputing: Bedrohung oder Chance?

Jede Veränderung bringt zunächst eine Störung der aktuellen Ökosysteme und Vorgehensweisen mit sich, bietet gleichzeitig aber die Möglichkeit zur Verbesserung. Die Lösung liegt in der Fähigkeit, die zukünftigen Veränderungen frühzeitig zu erkennen und sich auf diese vorzubereiten.

Dasselbe gilt für Quanten-Computing. Dieses soll in der Theorie eine exponentielle Rechenleistung erbringen, die nicht nur Vorteile mit sich bringt. Vielmehr stellt es den aktuellen Stand der Kryptografie in Frage, welche das Fundament der heutigen Informationssicherheit bildet. Daher ist es wichtig, Daten, welche auch in Zukunft verschlüsselt sein sollen, bereits heute gegen Quantencomputer abzusichern.

Was ist Quanten-Computing und welche Veränderungen beinhaltet es?

Während klassische Computer „0" und „1" (also den Zustand „an" und „aus") verwenden, um zwei unterschiedliche Zustände eines Informationsbits zu repräsentieren, nutzen Quantencomputer die Eigenschaften der „Unschärferelation", „Überlagerung" und „Verschränkung" von Quantenbits (Qbit), sodass ihre jeweilige „0" und „1" gleichzeitig, mit einer unterschiedlichen Wahrscheinlichkeit und in einer korrelierten Weise existieren können. Wenn mehrere Qbits miteinander wechselwirken, kann die Wahrscheinlichkeit, dass jedes Bit eine „0" oder „1" ist, als Vektor ausgedrückt werden. Wenn eine Messung durchgeführt wird, kollabiert die Funktion entsprechend der angewendeten programmierten Bedingung und man erhält das wahrscheinlichste Ergebnis. (Man würde die Berechnung wahrscheinlich ein paar Mal durchführen, ergänzt durch eine weitere Überprüfung mit einem klassischen Computer, um sicherzugehen, dass man zum selben Ergebnis kommt). Zum Vergleich: Ein klassischer 3-Bit-Computer kann einen Wert aus acht Kombinationen ausdrücken. Ein 3-Qbit-Quantencomputer hingegen kann acht verschiedene mögliche Kombinationen auf einmal ausdrücken. Bei einem 300-Qbit-Quantencomputer, hätte man am Ende eine

Markus Hofbauer, Pre-Sales Consultant, DACH, Thales

Anzahl von Möglichkeiten, die größer ist als die Anzahl der Atome im beobachtbaren Universum (schätzungsweise 1078 bis 1082 Atome).

Diese enorme Menge an neuer Rechenleistung ist für viele Anwendungen nützlich. Die Modellerstellung der Interaktion von Molekülen, um die Entwicklung neuer Medikamente und Materialien zu beschleunigen, bis hin zur Vorhersage von Verkehr, Wetter und Erdbeben. Dies sind jedoch nur einige wenige Beispiele. Eine besondere Anwendung des Quanten-Computings ist die Lösung einiger schwieriger mathematischer Probleme, wie z. B. das Ermitteln der Primfaktoren großer Zahlen. Wenn sie beispielsweise die Faktoren des aktuellen Jahres „2021“ berechnen sollen, dann können Sie 2021 durch die Primzahlen 2, dann 3, ... teilen, bis Sie die Zahl 43 erreichen, was ihnen das Ergebnis 43 x 47 = 2021 liefert. Eine vierstellige Zahl „2021“ mag für einen klassischen Computer nicht allzu schwierig zu faktorisieren sein, jedoch stoßen die meisten klassischen Computer an ihre Grenzen, wenn die zu faktorisierende Zahl so groß wie 1,3 x 10154 ist (was eine 512-Bit-Zahl darstellt). Diese Art von schwerem mathematischem Problem ist genau das, worauf die traditionelle Public-Key-Kryptografie wie RSA (die mit Primfaktoren arbeitet) und DSA, Diffie-Hellman und Elliptic-Curve (die mit diskreten Logarithmus-Problemen arbeiten) basiert. Darin liegt die Sicherheitsgrundlage des heutigen e-Commerce, der digitalen Identitäten usw. Mit einem ausreichend leistungsfähigen Quantencomputer, auf dem die nach dem Mathematiker Shor benannten Algorithmen laufen, können diese traditionell schwierigen mathematischen Probleme in wenigen Tagen oder sogar Stunden gelöst werden. Mit dem Aufkommen des Quantencomputers wird somit die Sicherheit, welche die digitalen Identitäten und die Internetkommunikation (SSL/TLS) unserer modernen Gesellschaft schützt, erheblich geschwächt.

Welche Risiken bringt das mit sich?

Wenn der Zugang zu dieser Rechenleistung in die falschen Hände fällt, werden für uns selbstverständliche Dinge, wie Mobile Banking, Onlineshopping, IoT, Ampelsteuerung und Stromverteilung anfällig für die Übernahme durch Geräte, da sie nicht stark genug geschützt sind, um einen Quantenangriff zu überstehen.

- Wenn die Kommunikation im elektronischen Bankwesen kompromittiert wird und somit die Transaktionen der Kunden an die Öffentlichkeit gelangen, kann dies zum Verlust von Bankkunden führen, da diese ihr Geld keiner Bank anvertrauen wollen, die ihre Geheimnisse nicht wahren kann.
- Lebensbedrohliche Situationen könnten eintreten, wenn die Identitäten einiger medizinischer IoT-Geräte kompromittiert werden und Malware die Kontrolle über die Geräte übernehmen kann. Ein Angriff durch Ransomware auf seinen Herzschrittmacher, ist sicherlich das Letzte, was sich ein Patient wünscht.
- Vor allem den Regierungs- und Verteidigungssektor sollte diese Bedrohung alarmieren. Auch wenn ein Angreifer derzeit nicht in der Lage ist, die kryptografischen Codes zu knacken, die zum Schutz der Kommunikation verwendet werden, können diese Akteure die Informationen jetzt horten und die verschlüsselten Daten analysieren, sobald die Mittel zur Entschlüsselung der Kryptografie verfügbar sind. Die Kompromittierung solcher Geheimnisse wird die nationale Sicherheit in der Zukunft gefährden.

Wie viel Zeit bleibt uns?

Der derzeitige Fortschritt im Quanten-Computing wird durch die spezielle Betriebsumgebung des empfindlichen Quantengeräts begrenzt. Um das Rauschen des Geräts zu reduzieren, erfordert die Inbetriebnahme spezielle Umgebungen, die auf -273,1 °C gekühlt werden (kälter als der Weltraum) und das Gerät muss in einem Hochvakuum platziert werden, das 10 Milliarden Mal niedriger ist als der atmosphärische Druck. Wenn man also einen Computer mit 1.000 logischen Qbits in einem stabilen Zustand betreiben will, muss man einen Quantencomputer mit einer Million physikalischen Qbits bauen. Experten auf diesem Gebiet sagen voraus, dass es noch 5 bis20 Jahre dauern kann, bis Quantencomputer praktisch nutzbar werden. Es besteht jedoch kein Grund zur Panik – der richtige Weg ist nicht, den Fortschritt im Quanten-Computing zu stoppen, sondern die Grenzen der Kryptografie und Informationssicherheit, wie wir sie heute kennen, infrage zu stellen und die richtigen Schritte einzuleiten.

Wie können wir uns vorbereiten?

Es gibt drei Bereiche, mit denen sich Risikoeigner, CISOs und Systemarchitekten befassen sollten:

1. **Krypto-agile Implementierung mit quantensicherem Algorithmus:** Komponenten, die auf digitale Zertifikate angewiesen sind und deren Lebensdauer bis ins Quantenzeitalter reicht, sollten sicher von der aktuellen Kryptografie auf die Verwendung quantensicherer Algorithmen migrieren. Im Hinblick auf den bevorstehenden Einsatz des Quantencomputers sollten sie in der Lage sein, schnelle Änderungen vorzunehmen, welche die Anwendungen dazu zwingen, entweder auf quantensichere Algorithmen oder größere Sicherheitsschlüssel umzustellen (dies entspricht den Anforderungen an die Kryptoagilität, wie sie im Cybersecurity Labelling Scheme der Cyber Security Agency of Singapore festgelegt sind). Ein Drop-in replacement für RSA, ECDSA, ECDH und ECIES ist eine zu berücksichtigende Option.
   Empfehlungen von Thales: Kryptoagil zu werden ist entscheidend für den Schutz und die Sicherung von Daten sowie die Abwehr neuer Bedrohungen. Das Luna HSM Post Quantum Crypto Functionality Module (FM) nutzt das ISARA Radiate™ Quantum-safe Toolkit und ermöglicht es, quantensichere Signaturen für die heutige Code-Signierung zu verwenden. Diese Implementierung beinhaltet Mechanismen zur Schlüsselkomprimierung, die entweder auf Geschwindigkeit oder auf Größe optimiert sind, um sicherzustellen, dass der private Schlüssel optimal gespeichert und in einer Betriebsumgebung mit unterschiedlichen Anforderungen verwendet wird. Zertifizierungsstellen, Dokumentensignatur und Firmware-Codesignatur, die eine längere Lebensdauer als fünf Jahre haben (untere Grenze der quantum arrival), sollten mit der Migration beginnen.
2. **Quanten-Zufallszahlengenerierung:** Es muss betont werden, dass Zufallszahlengeneratoren, die auf einem Quantenprozess basieren, normalerweise nicht allein verwendet werden, unter anderem weil nur wenige Zertifizierungssysteme die Ausgabe eines QRNG-Geräts zur direkten Verwendung akzeptieren. Vielmehr ist die resultierende hohe Entropie der von einer Quantenquelle erzeugten Zufallszahl geeignet, um einen zertifizierten Deterministic Random Bit Generator-Algorithmus häufig neu zu besetzen.
   Empfehlungen von Thales: Luna HSM bietet eine API, die externe Entropie einmischen kann. Zudem gibt es eine gebrauchsfertige Integration, bei der ein iDQ-Gerät verwendet werden kann, um dem HSM zusätzliche Entropie zu liefern, die mit internen Entropiequellen gemischt wird.
   Quantenschlüssel-Verteilung: Es wird davon ausgegangen, dass die Einführung von Quantencomputern einen viel größeren Einfluss auf die Public-Key-Kryptografie haben wird als die symmetrische Kryptografie. Erstere wird hauptsächlich für die Schlüsselverteilung verwendet und daher sollte die Sicherung der Schlüsselverteilungsmechanismen als oberste Priorität angesehen werden. Es besteht die Möglichkeit, dass die verschlüsselten Datenströme aufgezeichnet und gespeichert werden, um sie zu interpretieren, sobald die Leistung des Quantencomputers verfügbar ist, um die Daten in der Zukunft zu entschlüsseln. Dies kann in Szenarien, in denen die Informationen 20 Jahre oder länger vertraulich bleiben müssen, höchst problematisch sein.
   Empfehlungen von Thales: Die Thales High-Speed Encryptoren für Netzwerke beinhalten sowohl die Quantenzufallszahlengenerierung als auch die Quantenschlüsselverteilung. Diese quantenfähigen Verschlüsseler sollten für den Einsatz in allen Netzwerken spezifiziert werden, in denen hochsensible Daten übertragen werden.

Fazit: Vorbereitung ist bereits heute wichtig

Obwohl die Post-Quanten-Kryptografie noch einige Jahre entfernt ist, müssen Unternehmen und Behörden, die auf digitales Vertrauen angewiesen sind, schon heute planen, wie sie ihre Informationssicherheit in der Zukunft gewährleisten können. Einige Unternehmen bieten eine kostenlose Risikobewertung an, um herauszufinden, ob das eigene Unternehmen dem Risiko einer Sicherheitsverletzung durch Post-Quanten- Kryptografie ausgesetzt ist. Mit dem gewonnenen Situationsbewusstsein können Anwender dann eine Strategie erarbeiten, um sich vor Post-Quantum-Kryptografie zu schützen.

Markus Hofbauer

Post-Quantum-Kryptographie: Sichere Verschlüsselung trotz Quantencomputer

Kryptographie ist so alt wie die Welt selbst. Stets gab es einen Wettlauf zwischen der Verschlüsselung und der Entschlüsselung. Nun aber stehen Quanten-Computer mit bisher ungekannten Rechengeschwindigkeiten in den Startlöchern und könnten sämtliche der etablierten Kryptographie-Verfahren wirkungslos machen.

Wenn es um Verschlüsselung in der Informationstechnologie (IT) geht lässt sich zusammenfassen: Es existieren viele sehr sichere Schlüssel, deren Entschlüsselung in annehmbarer Zeit mehr Rechenleistung erfordert, als derzeit den weitaus meisten Hackern zur Verfügung steht. Hier kommen nun die Fortschritte im Bereich der Quanten-Computer ins Spiel. Es ist nicht eindeutig, wie weit die Forschung und Konstruktion tatsächlich gekommen ist, doch offensichtlich wird es nicht mehr lange dauern, bis die ersten Quanten-Computer im Einsatz sind. Greift ein Angreifer über diese Art von Rechner ein Bankkonto an, dauert es nur wenige Augenblicke, bis sämtliche Verschlüsselung geknackt wurde und alle Informationen in seiner Hand sind. Ein Quanten-Computer kann sogar im Nachhinein jeden aufgezeichneten Datenfluss entschlüsseln.

Das potenzielle Ausmaß des Schadens sprengt jede bekannte Grenze und lässt die Kosten für die Bereinigung einer derartigen Attacke explodieren. Einrichtungen ließen sich vollständig stilllegen – in wenigen Minuten.

Aus diesem Grund wird weltweit von allen Sicherheitsexperten, die sich Gedanken um die Zukunft machen, an Maßnahmen gearbeitet, um Daten und Informationen weiterhin zu schützen. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt: „Um im Sinne eines angemessenen Risikomanagements vorbereitet zu sein, muss bereits heute mit den Vorbereitungen für die ‚Post-Quanten-Zeit‘ begonnen werden.“ Das Schlagwort lautet also: Post-Quantum-Kryptographie. Darunter wird

die Forschung verstanden, die Algorithmen sucht, welche einem Angriff durch einen Quanten-Computer standhalten könnten. Die Schwierigkeit besteht dabei in der Spekulation, denn aktuelle Modelle von Quanten-Computern besitzen nicht die Kraft, um jede Verschlüsselung zu brechen, doch es ist davon auszugehen, dass dies in absehbarer Zeit möglich sein wird. Es müssen daher völlig neue Algorithmen erfunden werden.

Was ist Quanten-Computing?
Wer die Gefahr verstehen möchte, die von Quanten-Computern für die IT-Sicherheit ausgeht, muss zunächst einmal wissen, was Quanten-Computing eigentlich ist.

Der klassische Computer bedient sich zur Entschlüsselung von Informationen der Bits. Jedes davon hat einen speziellen Wert: entweder 0 oder 1. Quanten-Computer würden nun mit Qubits arbeiten, die ursprünglich aus der Quanten-Mechanik stammen. Qubits können nicht nur die Werte 0 oder 1 annehmen, sondern ebenfalls die Superposition der beiden Zahlen, oder Überlagerung. Dieser Begriff stammt aus der Physik und meint eine Überlagerung gleicher physikalischer Größen, die sich nicht behindern. Hier liegt die Stärke des Quanten-Computers: Wird eine Operation an das Quanten-Register des Rechners übertragen, wird sie an jeden Qubit-Wert der Superposition übertragen – sie wird also von mehreren Qubits parallel durchgeführt. Hinzu kommt, dass die Anzahl der mathematischen Zustände im Quanten-Register, welches die Summe n von Qubits beinhaltet, 2n ist. Das bedeutet, dass eine Operation, die auf einem Quanten-Computer durchgeführt wird, einer exponentiellen Anzahl von Operationen, nämlich 2n, auf einem klassischen Computer entspricht. Jedoch gilt es eine Hürde zu nehmen, um von der Quanten-Geschwindigkeit zu profitieren: Das Ergebnis einer Operation, die auf einem Quanten-Computer durchgeführt wurde, ist natürlich ein Qubit-Wert, kein Bit-Wert, also möglicherweise eine Superposition. Um dieses auslesen zu können braucht es daher neue Algorithmen, da bisher bekannte nur mit Bits arbeiten.

Auswirkung auf die bekannte Kryptographie und daraus abgeleitete Produkte
Bereits in den Jahren 1994 und 1996 schafften es zwei Algorithmen, vorgestellt von Peter Shor und Lov Grover, die Quantum-Parallelität zu nutzen. Der Algorithmus von Shor kann verwendet werden, um jedes Verschlüsselungsverfahren mit öffentlichem Schlüssel zu brechen, dessen Sicherheit auf der Stärke der Integer-Faktorisierung oder des Diskreten-Logarithmus-Problems in polynomieller Zeit beruht. Das umfasst die meisten der weitverbreiteten Verschlüsselungsverfahren mit öffentlichem Schlüssel, darunter: RSA, ECDSA, ECDHE.

Grovers Algorithmus dagegen kann die Brute-Force-Angriffszeit auf ihre Quadratwurzel reduzieren. Für die symmetrischen Schlüssel-Algorithmen, wie AES (Advanced Encryption Standard) und TDES (Triple Data Encryption Standard), bedeutet dies: Sobald ein Quanten-Computer verfügbar wird, ist die Stärke eines 256-Bit-Schlüssels identisch zu der eines 128-Bit-Schlüssels. Der Algorithmus von Grover ermöglicht es auch, die Zeit eines sogenannten Kollisionsangriffs (Collision Attack) zu reduzieren, wodurch die Stärke von Hash-Funktionen verringert wird. Die Stärke der SHA256 verringert sich von 128 Bit auf 80 Bit, die Stärke der SHA384 von 192 Bit auf 128 Bit.

Folgen für die IT-Sicherheit
Quanten-Computer würden nicht nur das Knacken der zukünftigen verschlüsselten Kommunikation ermöglichen, sondern auch die nachträgliche Entschlüsselung der gegenwärtig sicher verschlüsselten Daten. Aus diesem Grund müssen Vorbereitung getroffen werden:
- Krypto-Schemata, die für Authentifizierung, Vertraulichkeit und Schlüsselaustausch verwendet werden, müssen ersetzt werden.
- Die symmetrische Kryptographie benötigt nicht nur einen vertraulichen Weg, um private Schlüssel auszutauschen, sondern um die Größe des symmetrischen Schlüssels und des Hash-Werts zu erhöhen.

Das National Institute of Standards and Technology (NIST) der Vereinigten Staaten von Amerika leitet seit einiger Zeit ein Post-Quantum-Standardisierungsprogramm (PQS), welches versucht, neue Algorithmen zu definieren, die quantensicher sind. Das heißt, sie können nicht mit bekannten Techniken von Quanten-Computer und deren erwarteter Rechenleistung gebrochen werden. Das Projekt ist in seine letzte Phase eingetreten und soll in den nächsten zwei Jahren abgeschlossen werden.

Umstellung auf sicheres Quanten-Computing
Zur Verwirklichung der Vorstellung eines sicheren Betriebs trotz Quanten-Computern müssen die bestehenden Sicherheitsprotokolle – darunter SSH, VPN/IPSec, SSL/TLS – so verbessert werden, dass sie hybrid arbeiten können. So bliebe die Kompatibilität zu derzeitigen Verschlüsselungen erhalten, während mit der Quanten-Verschlüsselung bereits gearbeitet werden kann.

Diese Änderung wirkt sich auf asymmetrische Kryptografie und die Schlüsselgenerierung aus. Sie erfordert außerdem eine vergrößerte Schlüsselgröße in symmetrischen Algorithmen. Alles zusammen wirkt sich stark auf die nötige Rechenleistung und Internet-Bandbreite aus. Es lohnt sich daher, die Umstellung auf die Quanten-Sicherheit mit Hardware-Upgrades, wie Quanten-Gateways, abzustimmen und zusammen durchzuführen. Auf diese Weise können sofort nach der Freigabe neue Algorithmen, die erforscht wurde, in das System integriert werden, damit Unternehmen umgehend bereit sind für die neue IT-Welt des Quanten-Computing.

Christine Schönig

Christine Schönig, Regional Director Security Engineering CER, Office of the CTO, Check Point Software Technologies GmbH

1.3 TECHNOLOGIE

Ist durch Quantum Computing eine „Artificial general intelligence“ in absehbarer Zeit realistisch?

Quantencomputer sind eine relativ neue Technologie, die wegweisende Wissenschaftler, Forscher und Unternehmer auf der ganzen Welt versuchen zu kommerzialisieren. Im Januar 2019 stellte IBM zum Beispiel mit dem „Q System One“ den ersten eigenständigen Quantencomputer für wissenschaftliche und kommerzielle Zwecke vor. Durch die Quantencomputer beschleunigt sich der Fortschritt in der Entwicklung der künstlichen Intelligenz (KI). Quantencomputer verbessern nicht nur die Leistung der Informationsverarbeitung, sie machen auch KI-Techniken wie „Deep Learning“ und „Machine Learning“ erst möglich.

Quantencomputer, künstliche Intelligenz und Big Data
Quantencomputer verwenden eine Technologie, die auf den Prinzipien der Quantentheorie basiert, welche die Natur von Energie und Materie auf atomarer und subatomarer Ebene erklärt. Es beruht auf der Existenz quantenmechanischer Phänomene wie Überlagerung und Verschränkung. Erwin Schrödingers berühmtes Gedankenexperiment aus den 1930er Jahren, bei dem eine Katze gleichzeitig tot und lebend war, sollte die scheinbare Absurdität der Überlagerung hervorheben. Nach diesem Prinzip können Quantensysteme gleichzeitig in mehreren Zuständen existieren, bis sie beobachtet oder gemessen werden.

Heutzutage enthalten Quantencomputer Dutzende von Qubits (Quantenbits), die genau dieses Prinzip nutzen. Jedes Qubit existiert in einer Überlagerung von Null und Eins. Das heißt, die Wahrscheinlichkeiten haben eine Null oder Eins, bis das Qubit gemessen wird. Die Entwicklung von Qubits hat Auswirkungen auf den Umgang mit riesigen Datenmengen und das Erreichen eines bislang unerreichten Recheneffizienzniveaus, das das verlockende Potenzial des Quantencomputers darstellt.

Während Schrödinger über Zombie-Katzen nachdachte, beobachtete Albert Einstein ein Phänomen, das er als „spukhafte Fernwirkung“ bezeichnete: Partikel, die scheinbar schneller als mit Lichtgeschwindigkeit kommunizieren. Was er sah, waren verschränkte Elektronen in Aktion. Verschränkung bezieht sich auf die Beobachtung, dass der Zustand von Partikeln aus demselben Quantensystem nicht unabhängig voneinander beschrieben werden kann. Auch wenn sie weit voneinander entfernt sind, sind sie immer noch Teil desselben Systems. Wird ein Teilchen gemessen, scheint der Rest diese sofort zu wissen.

Der Fortschritt im Bereich der Informatik hängt entscheidend von der Rechenleistung ab. Die rechnerischen Anforderungen der Big-Data-Analyse belasten Computersysteme derzeit erheblich. Seit 2005 wurde der Fokus auf die Parallelität mit mehreren Kernen anstelle eines einzigen schnellen Prozessors verlagert. Viele Big-Data-Probleme können jedoch nicht einfach durch die Verwendung von immer mehr „Cores“ gelöst werden. Zur Aufteilung der Arbeit werden mehrere Prozessorkerne verwendet, die Implementierung ist jedoch komplex. Die Probleme müssen nacheinander gelöst werden, wenn der vorangehende Schritt ebenso wichtig ist.

Der Unterschied zwischen klassischen Computern und Quantencomputern
Klassische Computer sind binär. Das heißt, bei ihnen kann ein Bit nur zwei Zustände annehmen: 0 oder 1. Nimmt man das Beispiel mit Schrödingers Katze, können subatomare Teilchen gleichzeitig unzählige Zustände aufweisen. Stellt man sich eine Kugel im binären Zustand vor, wäre der obere Pol zum Beispiel eine 1, während der untere Pol durch eine 0 dargestellt wird. In einem Qubit kann die gesamte Kugel unzählige andere Zustände enthalten. Die Zuordnung dieser Zustände auf verschiedene Qubits machen Quantencomputer für eine Vielzahl spezifischer Aufgaben geeignet, die mit klassische Computern nicht möglich sind.

Beim Large Hadron Collider (LHC) am CERN in Genf werden Teilchen beschleunigt und bewegen sich mit fast Lichtgeschwindigkeit innerhalb eines 27-km-Rings. Dabei finden in einer Sekunde 600 Millionen Kollisionen stattfinden, bei denen nur eine der 1 Millionen Kollisionen für die Vorauswahl ausgewählt wird. Bei der Vorauswahl wird nur 1 von 10.000 Ereignissen an ein Raster von Prozessorkernen weitergeleitet, die weiterhin 1 von 100 möglichen Ereignissen auswählen, wodurch der Datenprozess bei 10 GB/s erfolgt. Bei LHC werden pro Sekunde 5 Billionen Datenbits erfasst. Nachdem 99% der Daten verworfen wurden, werden immer noch 25 Petabyte Daten pro Jahr analysiert.

Zu den Stärken der Quantencomputer gehört die Verarbeitung riesiger Datenmengen, doch bei den derzeitigen Ressourcen steckt die Anwendung von Big Data noch in den Kinderschuhen. Wenn es technisch möglich ist, wären Quantencomputer für die Berechnung für bestimmte Aufgaben sehr nützlich, zum Beispiel beim:
- Factoring großer Zahlen

Alexander Eser, Co-Founder & Managing Director, Kaufberater.io

- Kryptographie
- Wettervorhersagen
- Künstliche Intelligenz
- Schnelles Durchsuchen großer unstrukturierter Datensätze
- Finden und identifizieren von Mustern und Anomalien

Die Entwicklungen bei Quantencomputern könnte die Verschlüsselung im Handumdrehen überflüssig machen. Mit der Rechenleistung eines Quantencomputers wäre es möglich, große Datensätze zu erstellen, die wahrscheinlich vollständige Informationen enthalten, wie zum Beispiel die genetische Daten eines jeden Menschen, die existieren. Algorithmen für maschinelles Lernen können Muster in den Eigenschaften dieser Menschen finden und gleichzeitig die Identität von Menschen schützen. Auch das Clustering und die Klassifizierung von Daten wäre eine sehr schnell zu lösende Aufgabe.

Quantum Computer lösen komplexe Probleme sehr schnell

Führende Technologie-Firmen sind kurz davor kommerziell einsetzbare Quantencomputer herzustellen. Mit diesen Quantencomputern ist es möglich, Berechnungen in Sekundenschnelle durchführen, für die heutige Computer tausende von Jahren benötigen würden. Bereits jetzt entwickelt Google einen Quantencomputer, der angeblich 100 Millionen Mal schneller ist als alle heutigen Systeme. Dies wird entscheidend sein, wenn wir die enorme Datenmenge verarbeiten und sehr komplexe Probleme lösen können.

Der Schlüssel zum Erfolg ist die Umsetzung unserer Probleme in die Quanten-Sprache. Künstliche Intelligenz und besonders maschinelles Lernen werden von den Fortschritten der Quanten-Technologie und die schnelle Analyse riesiger Datenmengen enorm profitieren. Während heute Programmierer den Code anpassen muss, um optimale Ergebnisse zu erzielen, entscheiden KI-Algorithmen selbst, ob ein Ergebnis richtig oder falsch ist.

Quantencomputer und künstliche Intelligenz

Fast täglich erreichen uns Meldungen über Fortschritte bei der Entwicklung von Quantencomputern. Es gibt kaum ein wichtiges IT-Unternehmen, das nicht auf diesem Gebiet forscht. Dieses Geschäft werden sich die Technologie-Giganten nicht entgehen lassen. Nach acht Jahren Arbeit hat eine 25-köpfige Gruppe von Google-Ingenieuren einen neuen Quantenchip hergestellt, deren Leistungsfähigkeit sie bis Ende 2019 demonstrieren wollen. Bei Erfolg wird dies ein Benchmark für alle anderen Quantencomputer sein. Seit mehr als 10 Jahren arbeiten Ingenieure bei Microsoft und Intel an einem Quantencomputer auf Silizium-Basis.

Auf dem Quantencomputer IBM Q System One werden bereits erste Quanten-Algorithmen getestet. Das kanadische Unternehmen D-Wave hat bereits erste Quantencomputer an Industrie-Unternehmen verkauft. Auch in Deutschland gibt es zahlreiche IT-Firmen, Universitäten und Forschungsinstitute mit einer hohen Kompetenz im Bereich Quanten-Computing.

Mit einem Quantencomputer, der 100 Millionen Mal leistungsfähiger ist als herkömmliche Computer, könnten wir beispielsweise den gesamten Körper eines Menschen digital simulieren und maßgeschneiderte Medikamente für spezielle Erkrankungen erstellen. Noch wichtiger ist jedoch, dass Forscher einige KI-Agenten auf diesen Quantencomputern erstellen und sie dazu veranlassen, bessere Instanzen ihrer selbst zu schaffen. Quantencomputer öffnen die Tür zur künstlichen Intelligenz.

Der D-Wave Quantencomputer basiert auf einem 512 Qubit-System. Der Chipsatz für die KI muss jedoch nicht von einer großen oder bekannten IT-Firma stammen. Startups versuchen, KI-Chips zu entwickeln, die für künstliche Intelligenz optimiert sind, um ein Stück von diesem Kuchen zu bekommen.

Die Komplexität und Größe unserer Datensätze wächst schneller als unsere Computerressourcen und stellt daher eine erhebliche Belastung für unsere Computerstruktur dar. Während die heutigen Computer Schwierigkeiten haben oder nicht in der Lage sind, bestimmte Probleme zu lösen, können dieselben Probleme durch leistungsfähige Quantencomputer in Sekundenschnelle gelöst werden. Die Quanten-Technologie bewegt sich mit einer unglaublichen Geschwindigkeit und es ist realistisch, dass in naher Zukunft Technologie-Giganten noch leistungsfähigere Quantencomputer auf den Markt bringen werden. Diese könnten dann ihrerseits zur Verbesserung dieser Systeme eingesetzt werden. Das würde die gesamte KI-Landschaft nachhaltig verändern.

Alexander Eser

Nicht mehr Science-Fiction, sondern schon Wirklichkeit: Quantencomputer wird durch Verbindung mit Hochleistungsrechner für die Anwendung nutzbar gemacht

In der Quanten-Welt bewegt sich derzeit einiges: Das hochdynamische Technologiefeld ist nicht nur durch neueste, bundesweite Initiativen in aller Munde, sondern beschäftigt sich auch zunehmend mit kommerziellen Anwendungsfällen. Das Forschungsprojekt IQuAn ermöglich jetzt auch Anwendungsfälle mit High-Performance Computing für externe Nutzer. Dabei ist Mainz mit der Forschungsgruppe um Prof. Schmidt-Kaler in der Entwicklung von Ionen-Quantenprozessoren ein wichtiger Punkt auf der Quantencomputing-Landkarte geworden. Zu Beginn des Jahres startete das neue Forschungsprojekt IQuAn, welches vom BMBF gefördert wird.

Was ist der Gegenstand des IQuAn Projekts?

Im Projekt IQuAn, das für Ionen-Quantenprozessor mit HPC-Anbindung steht, forschen Unternehmen, Universitäten und Forschungsinstitute an der Entwicklung einer robusten Quantenprozessorplattform. Das Vorhaben konzentriert sich dabei auf die technologische Entwicklung von essenziellen Komponenten eines skalierbaren Quantenprozessors von bis zu 100 Qubits. Im Fokus steht dabei die Neuentwicklung eines Vielkanal-Radiofrequenzpulsgenerators zur Darstellung von Quantengattern mit hoher Güte sowie die Implementierung von Softwaremodulen zur skalierbaren und effizienten Generierung von Kontrollsequenzen auf Hardwareebene. Dabei geht es unter anderem um die Modularisierung von Soft- und Hardware. Dies ist notwendig, um eine skalierbare Architektur von Quantencomputern auf den Weg zu bringen.

Der Quantenprozessor soll latenzarm an den Mainzer MOGON II High Performance Computer angebunden und für hybrides Quantencomputing auch extern nicht forschenden Nutzern zur Verfügung gestellt werden. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt IQuAn umfasst ein Projektvolumen von 12 Millionen Euro über einen vierjährigen Zeitraum. Die Projektkoordination liegt beim Institut für Physik der Johannes Gutenberg-Universität Mainz. Weitere Teilnehmer des Projektkonsortiums sind AKKA Technologies, das Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF, das Fraunhofer-Institut für Lasertechnik ILT, das Forschungszentrum Jülich und die TOPTICA Photonics AG.

Wo stehen wir gerade in der Entwicklung von Quantentechnologien?

Wir befinden uns auf dem Weg in die dritte Quantenrevolution. Nach der Entwicklung der theoretischen Grundlagen um 1900, und der erfolgreichen Umsetzung von Technologien, wie beispielsweise dem Laser um 1960, stehen wir nun vor der Herausforderung unser Systemverständnis soweit zu vergrößern, dass wir die Quantenmechanik auf Fragestellungen aus unserem industriellen und kommerziellen Alltag anwenden können. Unter der dritten Quantenrevolution versteht man Technologien auf Basis von Quantenmechanik in makroskopischen Systemen, die den Bereich kommerzieller Anwendungen erreichen. Dies betrifft Quanten-Sensorik, -Computer, -Simulation und –Kommunikation. Die Entwicklungen sind rasant; die Idee von Ionenfallen-Quantencomputern ist gerade einmal 25 Jahre alt. Im Jahr 1995 beschrieben Ignacio Cirac und Peter Zoller erstmals in den Physical Review Letters den konkreten Aufbau eines Quantencomputers.

Welche Vorteile bringt ein vollautomatisierte Inonenfallen Quantencomputer?

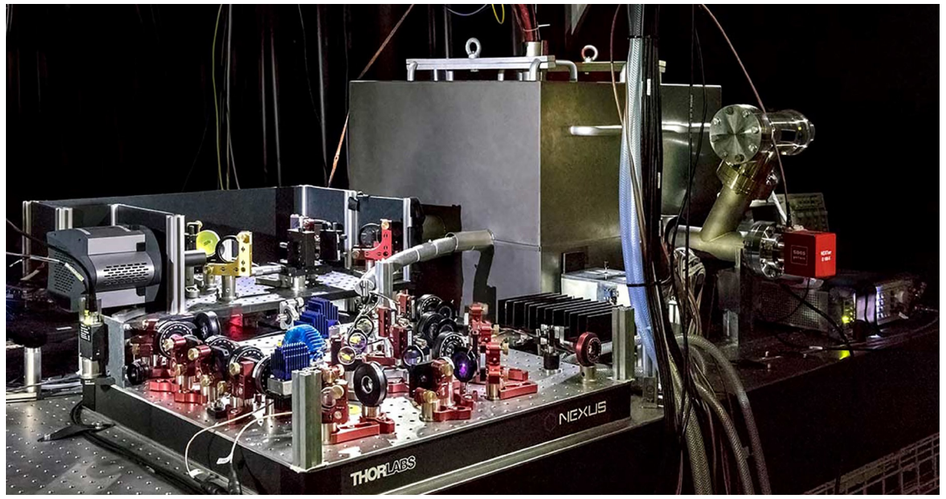
Es gibt mehrere aussichtsreiche Systeme für die Realisierung eines Quantencomputers: Zum einen erfolgt die Umsetzung mithilfe von supraleitenden Schaltkreisen, wie sie zum Beispiel von IBM und Google eingesetzt werden. Die supraleitenden Schaltkreise weisen ein Gatter-zu-Kohärenzzeit-Verhältnis auf, also wie viele Rechenoperationen ausgeführt werden können, das 8 bis 1000-mal kleiner ist als bei dem weiteren aussichtsreichen Ionenfallen-System [Chang et al. 2020, AAPPS Bulletin]. Hier erfolgt die Realisierung über gefangene atomare Ionen. Im Rahmen der Quantum-Flagship-Initiative der Europäischen Kommission arbeiten wir mit Forschern der Universität Mainz und Innsbruck an einem vollautomatisierten Ionenfallen-Quantencomputer mit Kalzium-Ionen-Ketten. Ionenfallen mit mikroskopisch dimensionierten Elektroden sind ein Kernelement bei der Skalierung von Quantenprozessoren. Obwohl supraleitende Quantenprozessoren aktuell über mehr Recheneinheiten verfügen, ist bei gefangenen Ionen die Qualität der Rechenoperationen erheblich besser. Ionenfallen-Quantencomputer mit Rechenoperationen hoher Qualität werden in dem Projekt mit hoher algorithmischer Flexibilität kombiniert und bieten damit vielversprechende neuartige Anwendungsmöglichkeiten. Die Anwenderorientierung in Verbindung mit dem Hochleistungsrechner ist also ein Meilenstein in der Entwicklung der Technologie.

Welche Anwendungsfälle für die industrielle und kommerzielle Nutzung kann man sich bei Quantencomputern vorstellen?

Ein leistungsstarker Quantencomputer kann einen entscheidenden Beitrag zur Lösung komplexer Probleme leisten. Ein Beispiel aus dem Alltag sind Navigationssysteme, bei denen gleichzeitig mehrere Routenoptionen unter bestimmten Bedingungen berechnet werden. Derzeit werden die Optionen alle einzeln berechnet. Ein Quantencomputer könnte die Optionen in einem Bruchteil der Zeit alle gleichzeitig berechnen und somit schneller und effizienter den optimalen Weg finden. Große Potenziale ergeben sich auch in den Bereichen der Materialforschung sowie in der Medizintechnik und dem Finanzwesen. Hier sind schon jetzt Algorithmen bekannt, die selbst für den größten aktuellen Supercomputer zu rechenintensiv sind, deren Fragestellungen aber mit genügend Quantenbits gelöst werden könnten. Der hybride Einsatz von Quantencomputern und HPC bietet auch einen vielversprechenden Hebel im Bereich des maschinellen Lernens, bei dem die Teile der Programme, die von einem klassischen Computer nur schwer verarbeitet werden können, einem Quantensystem zugewiesen werden. In diesem Subsystem können die Berechnungen dann effizient durchgeführt werden und dann die Ergebnisse an das Gesamtsystem zurück geliefert werden, vergleichbar dem Einsatz von Grafikkarten. Auch der Bereich der Kryptographie kann von Quantencomputern stark profitieren: Die Quantenkryptographie kann die Lebensdauer heutiger kryptographischer Systeme deutlich verlängern und

Stefan Ulm, Senior Project Manager Embedded System Development, AKKA Technologies

Nicolas Bonnotte, Digital Tech Line Leader, AKKA Technologies



Experimenteller Aufbau eines Ionenfallen-Quantenprozessors der JGU Mainz Bildrechte: Thomas Klink

findet z.B. im Banken- und Krankenversicherungsbereich sehr gute Anwendungen. Dabei kann der Quantencomputer als Quelle echter Zufallszahlen eingesetzt werden, oder bei der Erzeugung sicherer Schlüssel mit Hilfe der Verschränkung der Qubits in verteilten Systemen verwendet werden.

Auf welche innovativen Ansätze stützt sich das Forschungsprojekt?

Im IQuAn-Verbund wird ein neuer, skalierbarer Ansatz mit hoher Qubit-Konnektivität verfolgt. Dieser fordert auch im Bereich der Steuerungselektronik die Entwicklung von neuen Soft- und Hardwarekomponenten für die elektronischen Kontrolleinheiten für Quantenprozessoren.

Im Projekt wird beispielsweise daran gearbeitet, die bestehende Kontrollelektronik auf die Anforderungen eines solch skalierbaren Systems zu erweitern. Dies betrifft nicht nur die Vernetzung und Modularisierung der Soft- und Hardware-Komponenten untereinander, sondern auch die Anpassung der Prozesse an die wachsenden Anforderungen immer größerer Systeme. So versetzen wir die Kontrollelektronik auch in die Lage, auf der Zeitskala der Experimente Entscheidungen im Programmablauf zu treffen, um bei der steigenden Komplexität der Berechnungen im Quantencomputer Leerlauf-Zeiten zu minimieren.

Die Zusammenarbeit mit Universitäten und Forschungsinstituten im IQuAn Projekt ist ein wichtiger Schritt in der Realisierung neuer Technologiefelder wie Quantentechnologien und High Performance Computing.

Welches Potenzial hat das IQuAn Projekt, beispielsweise für die Mobilitätsindustrie?

Die Skalierbarkeit und Qualität der Rechenleistung von Ionenfallen-Quantencomputern ist der Schlüssel zum Erfolg. Durch die Zusammenarbeit von Forschung und Industriepartnern werden konkrete Anwendungsfälle aus dem industriellen und kommerziellen Alltag, zum Beispiel bezüglich der Entwicklung von Steuerungselektronik für quantenoptische Experimente mit segmentierten Ionenfallen, in das Projekt mit eingebracht und garantieren so den Wissenstransfer in den industriellen Alltag. Aufgrund dieser Neuerungen und der Entwicklung nach Industriestandards bieten sich Perspektiven zur Kommerzialisierung des Systems, auch über auf gefangenen Ionen basierenden Quantencomputer-Plattformen hinaus.

Stefan Ulm, Nicolas Bonnotte

The Quantum GHZ game: a playful introduction to entanglement and error mitigation on real Quantum computers

Quantum computers are promised to dramatically change how we think about computing, what problems we can solve and to which depth we understand our environment. With unparalleled implications for applications in physics, optimization, or machine learning, it is no surprise that this exciting field attracts more and more interest not only in research but also in industry and among individuals.

Thus, it is important to understand the differences and the additional potential Quantum computers can provide. However, Quantum computing and especially Quantum entanglement, one of the key properties underpinning its power, is difficult to understand as

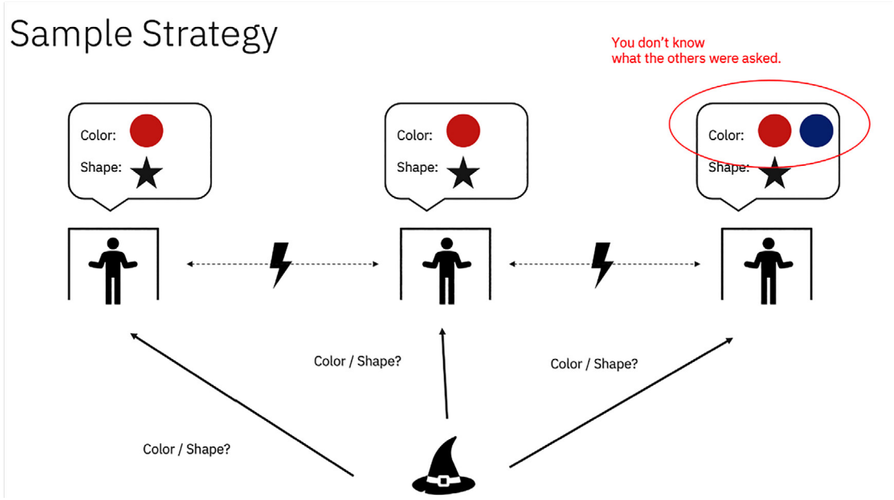


Figure 1 Dilemma of a sample classical strategy for the GHZ game

it contradicts our everyday experiences and intuition.

To learn about complicated topics like these and to develop a basic understanding of the ideas that conflict with the way that we perceive the world around us, Serious Games – games designed for a primary purpose other than pure entertainment – can be used with the objective to explain the fundamental concepts of Quantum computing such as entanglement.

The GHZ game

Imagine that you and your two friends, Alice and Bob, have been caught by an evil wizard. As he likes to play games, he gives the three of you a riddle and promises that you are free to go if you give the correct answer. The rules for this game are as follows:

- The three players are locked in different rooms.
- Each of you is given a piece of paper asking either for a color or for a shape.
- If asked for a color you can write red or blue on the paper, if asked for a shape you can chose either a star or a rectangle.
- The wizard will either ask all three of you for a color or two for a shape and one for a color.
- If all three are asked for a color, you win if red was answered an even number of times.
- If two players are asked for a shape and one for a color, you win if combined an uneven number of players answered with red or star depending on the question they were asked.
- You do not know what your friends were asked and what they answered and have no possibility to communicate.

Shortly before the wizard captured you, you had the chance to formulate a strategy on how to proceed. You and your friends agreed that if asked for a shape, all of you will answer with star, and if asked for a color, all of you will answer with red. However, after a while you realize that this solution only works in three out of four possible cases, as illustrated below.

In fact, classically, it is impossible to find a perfect solution using pre-agreed values. The highest winning probability that can be achieved this way is 75%.

However, when using Quantum entanglement, it becomes possible to develop a perfect solution for this hopeless situation. If you want to learn more about this and find the solution yourself, you can play the GHZ game using the interactive notebook "GHZ game" on https://github.com/JanLahmann/Fun-with-Quantum. Here, we will provide a short summary.

Quantum entanglement results in a strong dependency between qubits, allowing to store information that could not be stored on three independent qubits. If you and your friends each have one of three entangled qubits, it enables you to give coordinated answers without the need to communicate. Whether the wizard asks you for a shape or a color translates into reading the qubit in a different measurement base for each case. To retrieve information in a specific measurement base, we add additional gates to the target qubit before the quantum measurement operation.

Below you find an example. In the first part of the Quantum circuit, the three qubits are being entangled, resulting in the so-called GHZ state. Then, after the grey barrier, a measurement follows according to the question asked. In this example, the first person (top wire) is asked for a color and the other two are asked for a shape. Using the appropriate Quantum circuit, you will always receive one of the correct answers, no matter which question the wizard asked to whom. This

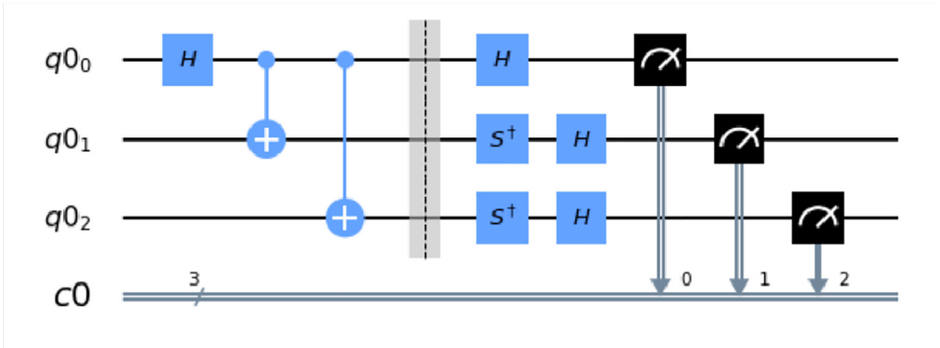


Figure 2 Quantum circuit for the GHZ game where the top player is asked for a color and the lower two are asked for a shape

Lennart Schulze, IBM Quantum Ambassador and Qiskit Advocate, IBM Germany

Isabell Heider B.Sc., IT consultant and Qiskit Advocate, IBM Germany

Dr. Jan-Rainer Lahmann, IBM CTO for Lufthansa, IBM Quantum Ambassador, Member IBM Academy of Technology, Board Member of IBM TEC, IBM Germany

means that on an ideal quantum computer, we will win the game with 100% probability.

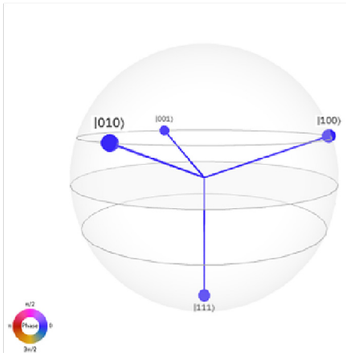


Figure 3 – Q-sphere visualization showing the possible outcomes of the sample GHZ game circuit, each of which corresponds to victory

Playing the GHZ game on real Quantum computers

Does that mean you have outsmarted the evil wizard? Unfortunately, not yet. For the above solution to work reliably, we would need a perfect Quantum computer, which currently does not exist.

Today's Quantum computers are imperfect, meaning that they are subject to a number of error sources and noise that render the outcomes of a Quantum algorithm partially incorrect. For this reason, we play the GHZ game mainly on a simulator.

However, there are some tricks to beat the wizard on a noisy Quantum computer too!

First of all, let us identify the reasons why the results on a real system are different from those on a simulator. Remember that a Quantum algorithm consists of a Quantum circuit like the one above, where on multiple qubits different gates are applied over time.

Mainly, we can distinguish two groups of issues. First, there are imperfections and errors that occur at different stages of executing a Quantum circuit. In some cases, the system can fail to accurately prepare qubits in their ground state before the algorithm starts. Similarly, gates, which manipulate the Quantum state of a qubit, can perform inaccurate transformations leading to accumulating errors. Ultimately, errors might occur when measuring the state of a qubit at the end of an algorithm, an operation which forces them to collapse into either of its two basis states. When instead of the expected classical state another one is randomly returned, we refer to it as measurement error.

Second, there are independent physical effects that corrupt the state of a Quantum system over time. Since Quantum states are very fragile, they would require outer-space conditions to persist. Even though current devices, such as the IBM Q System One, operate close to absolute zero temperature, we cannot yet isolate the systems to the extent that would be necessary. Due to small interactions with the environment and between qubits, the Quantum states held in the system slowly lose their Quantum properties, which is what we refer to as decoherence.

To quantify these effects, we introduce a metric that tells us how reliably we can win the game. In an ideal Quantum world, this value would be 100%, indicating all of the returned results are correct so that we always solve the riddle. Due to the present errors, we found that on average, the fidelity achieved on selected IBM Q real Quantum devices only is 84.3%, 15.7 percent points less than on the ideal simulator. Even though this does not sound too much, imagine being locked by the wizard and failing to escape – or even worse, imagine trying to reliably decode chemical properties of a molecule in order to develop a new drug!

Data retrieved from IBM Q Experience. On each system the game was executed with 8000 shots for 10 times oneach system. Luckily, plenty of methods are being researched and developed that can help us to improve the accuracy of our results.

Think about the second category of error sources. In principle, the longer an algorithm runs on a system the greater will be the effect of decoherence.

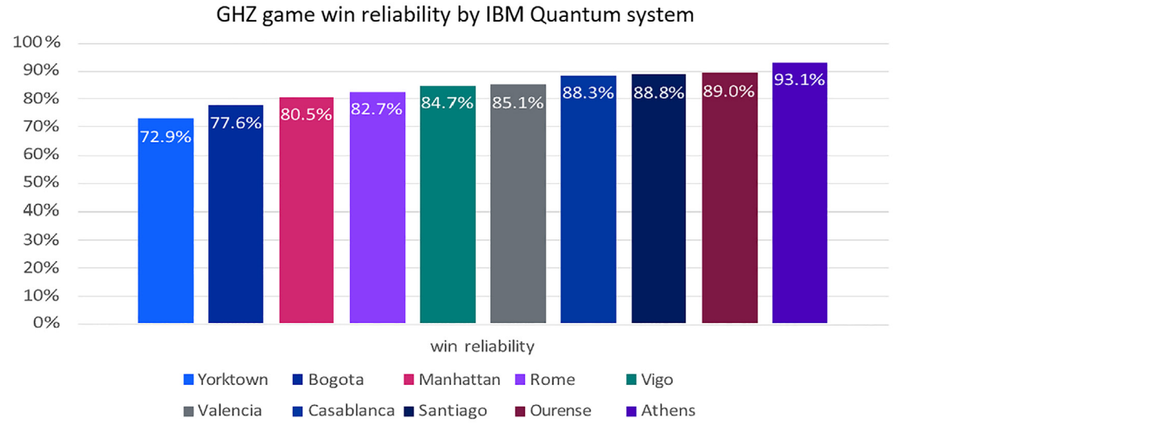


Figure 4 – Average reliability to win the GHZ game on ten selected IBM Q Quantum computers. (CC BY-NC-ND)

Furthermore, each additional gate introduces additional error due to its unprecise transformation. Thus, reducing the number of gates is key.

Now, if we wish to run the GHZ game circuit on a real device, we need to consider the physical layout of the qubits of the Quantum computer. If it does not match how we connect the qubits through the gates in our circuit, additional gates are added before the execution that maintain the semantics of the circuit while transforming it to correspond to the device's properties on the hardware level. Hence, if we pick the qubits in our circuit in a way that matches the alignment of the physical qubits, we can omit this overhead. In fact, this coupling map-adaptive optimization returned a win reliability of 85.3% on the four devices tested, an improvement of one percent point.

Furthermore, consider that the gate and measurement errors can greatly vary from one qubit to another even within the same machine. In a similar way to above, let us, thus, try to pick qubits for our circuit that fit the physical layout of the device and among these have the lowest gate and readout error rates. Using this error map-adaptive approach we win with 87.3% certainty; another two percent points up.

Both of these steps can be done automatically in Qiskit, the software that we use to execute Quantum algorithms, applying the so-called transpiler optimization. The transpiler is the engine that translates our logical Quantum circuits into those that are executable on our target Quantum computer. Its strongest configuration considers aspects far beyond the aforementioned two. And indeed, using this feature we receive a win reliability of 88.0%.

Now, the reliability is still not there where we need in order to defeat the wizard with confidence. Let us therefore use a more advanced technique, which is called measurement error mitigation. By experimentally examining the behavior of our Quantum computer, we can statistically deduce how strong the influence of measurement errors is in our results – and can calculate them out after we retrieved them! Applying this technique on our results from the error map-optimized circuit and the one optimized by our transpiler, we achieve a tremendous reliability of more than 97% and almost certainly win the game.

If you wish to try these methods on a real quantum computer yourself, you can do so by visiting the notebook "GHZ game on real devices" on https://github.com/JanLahmann/Fun-with-Quantum.

Besides the discussed techniques, which represent only a few examples under the large umbrella of Quantum error mitigation, there is even a fully developed theory that can ensure algorithms to reliably produce results that are completely accurate, referred to as Quantum error correction. Even though this is not feasible to implement on current devices, it gives you a glimpse of the future power of Quantum computers. Using entanglement and our mitigation strategies, the wizard better be prepared!

Lennart Schulze, Isabell Heider B.Sc.,
Dr. Jan-Rainer Lahmann

References and further reading: **[1]** Hands-on interactive notebooks for the GHZ game and Quantum error mitigation: https://github.com/JanLahmann/Fun-with-Quantum **[2]** IBM Quantum Experience: https://quantum-computing.ibm.com **[3]** Theoretical foundations of the GHZ state: Greenberger, D. M.; Horne, M. A.; Zeilinger, A. (1989): Going Beyond Bell's Theorem. Fundamental Theories of Physics, Vol.37, pp.69-72. **[4]** Introduction to Quantum measurement error mitigation in the Qiskit Textbook: https://qiskit.org/textbook/ch-quantum-hardware/measurement-error-mitigation.html **[5]** Hands-on journey to Quantum computing with IBM https://medium.com/@jan.lahmann/hands-on-journey-to-quantum-computing-with-ibm- 2487f0b2e10b **[6]** Playful introduction to the concepts of superposition and entanglement https://digitaleweltmagazin.de/2020/03/06/ein-spielerischer-einstieg-in-quantum-computing/ (German) **[7]** Exploring Quantum capabilities using a Raspberry Pi and a 3D printer https://digitaleweltmagazin.de/2021/01/08/rasqberry-oder-was-hat-ein-raspberry-pi-mit-einem- quantencomputer-zu-tun/ (German) http://rasqberry.org/ (English)

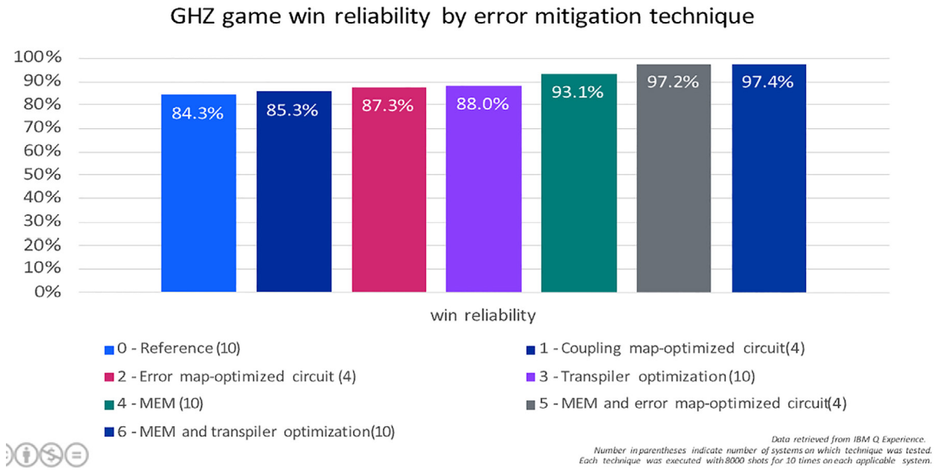


Figure 5 – Average reliability to win the GHZ game using different error mitigation techniques on IBM Q Quantum computers. Numbers in parentheses indicate the number of systems on which the technique was tested. MEM is the abbreviation for measurement error mitigation. (CC BY-NC-ND)

Digital Annealing – a bridge technology for quantum computing

Quantum computing is at the forefront of the digital world's attention right now, following Google's claim to have solved a random sampling task using its Sycamore quantum processor much faster than would be possible using even the fastest supercomputer.

The case is still contentious, but there is no doubt anymore that prototype quantum devices that exploit quantum phenomena actually exist. Many of the world's leading organizations have already moved beyond investigation and experimentation and are standing up proofs of concept and business cases. Major auto OEMs have announced quantum computing programs. Pharmaceutical companies and chemical companies are looking at areas such as molecular matching for new drug and material discoveries. Utility companies are aiming to optimize ROI from new asset investment, while banks and insurance companies are seeking to optimize portfolio and credit risks. Governments, too, are fascinated by the potential to achieve climate change targets faster, through optimization of transport systems to reduce pollution from traffic jams.

Quantum annealing and digital annealing

Among other things, quantum computing promises the ability to improve business processes by solving a class of 'combinatorial optimization' problems. This means identifying the optimal solution from a finite but extremely large set of options by evaluating each possibility. 'Annealing' is a probabilistic technique for achieving this by approximating the overall optimum result of a given function. Until now, by using annealing to tackle any combinatorial optimization process there has been a trade-off between precision and risk. In the past, seeking high precision implied the need for more time to calculate the answer – often more time than was available – while accepting a 'good enough' answer introduced an increasing amount of risk and the need for a security buffer. The more precise the calculation you can achieve the more cost-efficient the final process will be.

The limitations of true quantum computing

Quantum annealing solves the speed side of this equation however, despite recent breakthrough announcements, it is unlikely to be available for solving real world scenarios or ready for practical use in enterprises in the near future.

When it comes to algorithms, experimentation on quantum computing means that we are now seeing the maturity of quantum algorithms. However, the very early quantum computers available today are still unable to take advantage of these quantum algorithm advances. In quantum annealers, the problem is called 'chain break' – essentially the problem breaks as the scale increases resulting in sub-optimal solutions or errors.

In order to produce the correct output for a problem, quantum bits (qubits) must remain in a quantum state at near absolute-zero temperatures, free from any outside interference including cosmic or magnetic rays. Without all this, the qubits collapse out of their delicate entangled state losing all quantum acceleration and of course also rendering any calculation impossible.

The fragility of these quantum states makes quantum computing prone to error and creates a corresponding need for error correction. This consumes a sizable proportion of an already sparse pool of qubits, making it practically impossible to solve large scale problems. Therefore, quantum computing has largely been restricted to research purposes only. There is also a frequent misconception in quantum computing about the difference between physical and logical qubits. Today, based on the systems available in the market, the required error correction depends on the problem and the algorithm being used. For quantum gate computers (e.g. IBM, Google), the estimates range between 100 and 1,000 physical qubits representing an error-corrected logical qubit, in some cases even more. For quantum annealers, noise is less problematic due to their adiabatic 'analog' process. However, the sparse connectivity between physical qubits makes it necessary to represent logical qubits by sets of physical qubits. A fully-connected logical qubit typically requires a factor of approximately 30 to 80 physical qubits.

To put this in perspective, at the TCS Quantum Symposium held in Bombay on April 7, 2019, the quantum algorithms performed much better on classical computing systems in test results intended to showcase real world quantum computers– re-establishing the fact that quantum computers are simply not ready yet and we are still trying to find the best way to create a less error-prone quantum computer.

Fujitsu's scientists were keen on finding how to solve these critical quantum optimization problems and were among the first to realize that the software being developed for quantum computers could be applied to digital architectures. Based on this insight, they created the Digital Annealer, a new circuit design inspired by quantum phenomena.

Digital annealing is more precise, more robust than quantum annealing – and available today

Today's quantum annealers suffer from limitations in solving large scale problems due to the limited number of connections between qubits. On the other hand, the Digital Annealer architecture has a fully-connected architecture. It can, therefore, solve large-scale combinatorial optimization problems very quickly and – hugely important – more accurately today than quantum annealing with its limited qubit connections. The technology also has none of the cost, energy and deployment hurdles being experienced by quantum devices today.

Digital Annealing has been described by independent industry analysts as a unique opportunity to preempt quantum computing and achieve the first stage benefits of optimization today, working within current data center constraints. They talk about creating a 'bridge' to the quantum future – getting the benefits of combinatorial optimization today while also learning how true quantum computing can be applied to operations in the future.

How quantum-inspired optimization is being used today

There are tangible benefits in almost all areas of industry, ranging from the optimization of logistics and manufacturing processes, to materials research in the chemical and pharmaceutical industries, to significantly improved portfolio and risk calculation in the financial industry.

In automotive manufacturing, the Digital Annealer has been applied in job-shop scheduling, engineering design and just-in-time manufacturing optimization for robot positioning for chassis welding, which has a significant impact on manufacturing efficiency and cost. For the automotive manufacturer BMW, Digital Annealer is calculating the best assignment of welds (or seams) to PVC sealing robots as well as the optimal path for the robots in setting out from and returning to their base positions. Currently, prototype quantum computing solutions addressing this challenge are able to compute optimization for about seven seams. Working with the Fujitsu Digital Annealer, a trip of 64 seams can be calculated. This increase from seven to 64 seams is not just 9x the number of seams. The number of possible combinations to choose from increases by a factor of 10100, a total far beyond the assumed number of atoms in the whole universe.

For the car maker, this has resulted in production of more vehicles without investment in additional resources and has led to a reduction in paint-shop costs – which account for 30 to 50 percent of automotive OEM's manufacturing costs.

In financial services, main incubator GmbH, Commerzbank's research and development unit has successfully concluded a loan portfolio management Proof of Concept (PoC) , leveraging the Digital Annealer. Focusing on receivables from vehicle leasing contracts, the PoC optimized the selection of several thousand vehicle leasing assets for a securitization portfolio. Critical factors taken into simultaneous consideration included regulatory requirements, absolute volume limits and percentage limits for specific asset characteristics needed to achieve greater risk diversification.

The Port of Hamburg is one of the largest seaports in the world, with an annual throughput of 136.5 million tons and up to 12,000 trucks calling at the port every day. It is also located in the heart of a busy city and has been prone to congestion causing delays to freight transfers. The Port of Hamburg Authority is working with the Fujitsu Digital Annealer team on a PoC to find a new approach to traffic management in the port area. Together they developed a combinatorial optimization model with excellent evaluation performance and scalability for realistic street and traffic simulations that can be used to optimize traffic flow at traffic lights in the port area.

As these examples show, Digital Annealing makes it possible to solve complex combinatorial optimization problems under real-time conditions – even before practically usable real quantum computers are available for companies.

Carsten Meurer

Carsten Meurer, Head of Sales Financial Services Central Europe, Fujitsu

DIGITALISIERUNG *in Zahlen*

Der chinesische Quantum Supercomputer „Zuchongzhi“ unterstützt **66** *Qubits.*

Das Unternehmen **PsiQuantum** *investiert* **450 Mio.** *Dollar, um den ersten kommerziell brauchbaren Quantencomputer zu bauen.*

Laut Amy Leong, Senior Vice President von **FormFactor**, *wurden Investitionen von über* **20 Mrd.** *Dollar von 15 Ländern angekündigt.*

IBM *plant den Debut eines* **1121**-*Qubit Quantumprozessors namens IBM Quantum Condor.*

Der globale Quantum Computing-Software-Markt wird voraussichtlich bis 2026 auf **430 Mio.** *US-Dollar wachsen.*

Die **DARPA** *und* **Honeywell** *haben im Rahmen des Quantum Apertures-Projekts einen Vertrag in Höhe von* **5,5 Mio.** *Dollar beschlossen.*

In Großbritannien erhöhen mehr als **80 %** *der großen Unternehmen ihre Quantum Computing-Kapazitäten und -Ressourcen.*

Die Quantum Networking-Firma Aliro Quantum wird von der **U.S. Air Force** *mit* **100.000** *Dollar gefördert, um „Quantum Entanglement as-a-Service“ zu realisieren.*

Laut Dr. Ilana Wisby, CEO von **Oxford Quantum Circuits**, *gibt es rund* **20** *Unternehmen im UK, die auf „Quantum Computing as-a-Service“ fokussiert sind.*

Es existieren rund **15 Mio.** *bekannte chemische Strukturen, womit mittels Quantum Computing verbesserte Materialien und Medikamente hergestellt werden können.*

Foto: 123RF

Marcus Raitner ist überzeugt, dass Elefanten tanzen können. Als Agile Coach begleitet er deshalb Unternehmen auf ihrer Reise zu mehr Agilität und menschlicher Lebendigkeit. In seinem Blog „Führung erfahren!“ schreibt er seit 2010 über die Themen Führung, Agilität, Digitalisierung und vieles mehr.

Die Kunst des Weglassens

Was passiert mit der Verwaltung, wenn die Arbeit weniger wird? Diese Frage stellte sich Cyril Northcote Parkinson und sein Gegenstand der Untersuchung war das britische Kolonialamt, das von 1854 bis 1966 für die Verwaltung der britischen Kolonien zuständig war. Parkinson stellte fest, dass die Anzahl der Beamten unabhängig von der vorhandenen Arbeit stetig wuchs. Die meisten Beamten hatte das Kolonialamt im Jahr 1966, als es mangels zu verwaltender Kolonien in das Außenministerium integriert wurde. Die Organisation war beschäftigt – vor allem mit sich selbst.

Weglassen ist eine Kunst, die Verwaltungen offenbar weniger gut beherrschen. Weniger ist mehr. Mit diesem Motto beschrieb der Bauhaus-Architekt Ludwig Mies van der Rohe diese Kunst. Sein Kollege Richard Buckminster Fuller sah das ganz ähnlich, wenngleich er damit eher die funktionalen Aspekte meinte: „Doing more with less.“

Weniger ist mehr – und macht mehr Arbeit. Nicht nur in der Architektur, auch der französische Mathematiker Blaise Pascal entschuldigte sich 1656 für seine sprachlichen Ausschweifungen: „Ich habe den gegenwärtigen Brief aus keiner andern Ursach so lang gemacht, als weil ich nicht Zeit hatte, ihn kürzer zu machen.“ Und sein ungarischer Kollege Paul Erdős glaubte an „The Book“, ein Buch Gottes, das seiner Meinung nach all die eleganten und perfekten mathematischen Beweise enthält.

Wenn sich also nun diese großen Denker und Künstler einig sind, dass Einfachheit die höchste Form der Vollendung ist, wie es Leonardo da Vinci so treffend formulierte, wie kommt es dann zu diesem krebsartigen Wachstum von öffentlichen Verwaltungen wie des britischen Kolonialamts und damit einhergehend ihrer exzessiven Bürokratie? Ein Phänomen, das in großen und über Jahrzehnten gewachsenen Konzernen in fast identischer Weise zu beobachten ist und in schöner Regelmäßigkeit recht erfolglose Vorhaben zur Entbürokratisierung hervorbringt.

Sicher geht es uns viel beschäftigten Wissensarbeitern wie Blaise Pascal und wir haben einfach keine Zeit unsere Prozesse zu verschlanken. Hinzu kommt eine interessante soziologische Dynamik, die Cyril Northcote Parkinson als Ursache für das von ihm beobachtete Phänomen beschreibt. Einerseits versucht jeder Angestellte, die Anzahl seiner Untergebenen zu vergrößern, nicht aber die Anzahl seiner Rivalen. Und andererseits machen sich Angestellte gegenseitig Arbeit. Eine nach wie vor treffende Zusammenfassung der Gründe für die massiven Reibungsverluste in großen Organisationen.

Vielleicht liegt die Ursache aber auch viel tiefer in unserer menschlichen Psyche und unseren Neigungen, wie ein jüngst im Magazin Nature erschienener Artikel (Adams, G.S., Converse, B.A., Hales, A.H. et al. People systematically overlook subtractive changes. Nature 592, 258–261 (2021)) feststellte. Bei der Suche nach Lösungen bevorzugen wir in der Regel solche, die durch Hinzufügen von neuen Elementen entstehen gegenüber solchen, die durch Weglassen von bereits vorhandenen Elementen entstehen, selbst wenn letztere deutlich effizienter oder günstiger wären.

In einem Experiment hatten die Teilnehmer die Aufgabe, die Stabilität einer Lego-Struktur so zu verbessern, dass am Ende das Dach einen Ziegelstein tragen würde. Die Teilnehmer sollten bei Erfolg einen Dollar bekommen, aber jeder zusätzlich verwendete Legostein kostete 10 Cent. Da das Dach anfangs auf einem einzelnen kleinen Stein weit außerhalb des Schwerpunkts ruhte, fügten die meisten Teilnehmer einfach weitere Steine hinzu, um das Dach zu stabilisieren. Viel einfacher und gewinnbringender wäre es allerdings gewesen, den einzelnen Stein am Rand des Dachs einfach zu entfernen und das Dach dann stabil auf den Rest der Struktur aufzusetzen.

Das Weglassen scheint uns nicht zu liegen. Lieber machen wir mehr desselben, und wenn das nicht hilft, dann eben noch mehr. Diese universelle menschliche Neigung kombiniert mit deutscher Gründlichkeit erklärt dann vielleicht auch die umfangreiche deutsche Steuergesetzgebung sowie fein ziselierte Reisekostenrichtlinien in DAX-Konzernen.

Foto: Privat

Das Buch zum Manifest für menschliche Führung. Erhältlich als Taschenbuch und E-Book bei Amazon

FACHBEIRAT

IMPRESSUM

REDAKTION
Chefredaktion Claudia Linnhoff-Popien (V. i. S. d. P.)
Chef vom Dienst Robert Müller
Fachbeirat Patric Fedlmeier, Dr. Norbert Gaus, Dr. Sandro Gaycken, Dr. Michaela Harlander, Dr. Markus Heyn, Dr. Markus Hoffmann, Manfred Klaus, Andrea Martin, Dr. Niko Mohr, Dr. Christian Plenge, Frank Rosenberger, Dr. Ralf Schneider, Stephan Schneider, Michael Zaddach
Redaktion Steffen Illium, Hannes Mittermaier, Claudia Huber
Redaktionsassistenz Katja Grenner, Catarina Ilg
Mitarbeiter dieser Ausgabe Thomy Phan
Schlussredaktion Barbara Haber

ANFRAGEN AN DIE REDAKTION
redaktion@digitaleweltmagazin.de

GRAFIK
Layout Stefan Stockinger, www.stefanstockinger.com

ANZEIGEN
Ansprechpartner
redaktion@digitaleweltmagazin.de
Es gilt die gültige Preisliste, Informationen hierzu unter www.digitaleweltmagazin.de/mediadaten

KOSTENLOS ERHÄLTLICH
www.digitaleweltmagazin.de/magazin/
Ebenfalls online über SpringerLink (Berlin, Heidelberg, New York) erhältlich.
Alle Artikel werden von GoogleScholar indexiert.

HERAUSGEBER
Prof. Dr. Claudia Linnhoff-Popien, Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München, Tel. +49 89 2180-9153, www.digitaleweltmagazin.de

Digitale Stadt München e.V.

Jetzt Mitglied werden!

Stand: Sept. 2019

Digitale Stadt München e.V.:

Der Verein „Digitale Stadt München e.V.“ ist ein branchenübergreifendes Netzwerk im Umkreis der Digitalmetropole München. Als lebendige Plattform vernetzt er seine Mitglieder im Rahmen von drei Formaten:

DigiTalk

DigiTalks sind unsere regelmäßigen Themenabende. Unsere Mitglieder öffnen ihre Türen und laden zu einem aktuellen Thema der digitalen Transformation ein. Lernen Sie das Unternehmen kennen und erfahren Sie dessen Herausforderungen und Lösungsansätze.

AGs

Die Arbeitsgruppe „Smart City“ hat beispielsweise das Ziel, die Stadt München zu einer intelligenten Metropole zu entwickeln. Zu diesem Zweck werden Potenziale aus Wissenschaft und Wirtschaft identifiziert, um sie in das urbane Leben zu integrieren.

DIGICON

Die DIGICON ist großer Treffpunkt, wenn jährlich 350 namhafte Experten und Entscheider zusammenkommen, um sich über aktuelle Themen der Digitalisierung auszutauschen.

Kontakt: Geschäftsstelle des Vereins „Digitale Stadt München e.V.“, Oettingenstraße 67, 80538 München
geschaeftsstelle@digitalestadtmuenchen.de 089/ 2180-9259 oder -9171
Mitglied werden unter: https://digitalestadtmuenchen.de/mitglied-werden/