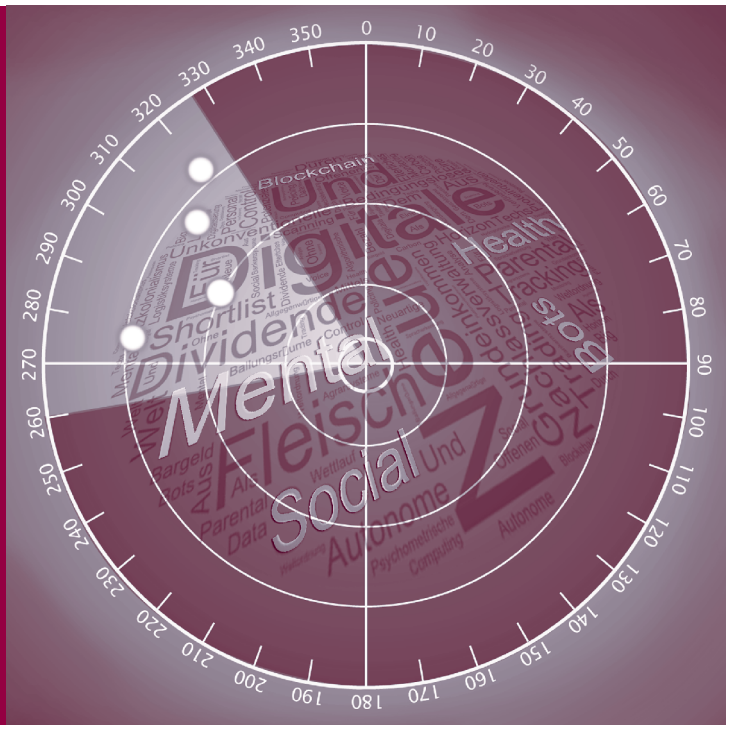
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Kai Enzweiler
Kerstin Goluchowicz
Tobias Jetzke
Sonja Kind
Marc Bovenschulte

Quantencomputer



Themenkurzprofil Nr. 23
September 2018

Quantencomputer

Kurzdarstellung des Themas

Quantencomputer versprechen durch ihre neuartige parallele Ausführung von Rechenoperationen einen innovativen Ansatz zur Lösung rechenintensiver Fragestellungen, bei denen konventionellen Computern physikalische Grenzen gesetzt sind. Das Einsatzpotenzial liegt hierbei in der Verarbeitung sehr großer Datenmengen und bei Echtzeitsimulationen.

Lange Zeit war unklar, ob Quantencomputer überhaupt entwickelt werden können, weil die dafür erforderlichen Systeme an die Grenzen des Machbaren stießen. Aktuellere Erfolge in der Forschung haben zuletzt dazu geführt, dass Quantencomputer den Übergang aus der Grundlagenforschung in die Anwendungsentwicklung finden (Hensinger 2018; Ritter 2018). So haben in den letzten Monaten führende Technologieunternehmen, darunter IBM, Intel und Google, bekanntgegeben, dass sie an der Entwicklung von Quantencomputer arbeiten (Filipp 2018; Kelly 2018).

Nach derzeitiger Einschätzung werden Quantencomputer aufgrund ihrer voraussetzungsvollen technischen Funktionsweise ihre Anwendung bei der Bearbeitung von Spezialproblemen finden und in absehbarer Zeit nicht breit genutzt werden. Eingabedaten müssen zurzeit aufwendig übersetzt werden, damit ein Quantencomputer die Daten verarbeiten kann (Musser 2018). Aufgrund ihrer neuartigen Funktionsweise eignen sie sich speziell zur Untersuchung komplexer Fragestellungen, z. B. zur Berechnung chemischer Reaktionen oder zur Analyse komplexer Prozesse in biologischen Systemen, auf deren Basis neue Materialien oder pharmazeutische Wirkstoffe entwickelt werden könnten. Weitere Anwendungsfelder liegen u. a. in der Kryptografie, der Verkehrssimulation oder im Bereich Machine Learning.

Risiken liegen darin, dass konventionelle Verfahren, z. B. gängige Verschlüsselungstechnologien, durch die Möglichkeit der stark zunehmenden Rechenleistung durch neue Verfahren abgelöst werden müssen (Hensinger 2018).

Konkrete Regulierungsbedarfe bei der Entwicklung der Quantencomputer bestehen aus Expertensicht momentan nicht. Die Entwicklungen sollten jedoch weiter beobachtet werden.

Hintergrund und Entwicklung

Quantencomputer unterscheiden sich in ihrer Funktionsweise fundamental von konventionellen Computern. Die Verwendung quantenmechanischer Effekte

soll es ermöglichen, eine deutlich schnellere Verarbeitung von Rechenoperationen zu erzielen. Ein charakteristisches Merkmal von Quantencomputern sind die kleinsten Einheiten, die Quantenbits oder auch Qubits genannt werden. Während ein normales Bit zwei Zustände »0« oder »1« einnehmen kann (binäre Logik), ist es für das Qubit möglich, nach den Gesetzen der Quantenmechanik Überlagerungszustände bzw. beide Zustände gleichzeitig einzunehmen. Dies wird Superposition (Überlagerung) genannt. Eine zweite wichtige Eigenschaft der Qubits besteht darin, dass sie sich auf eine besondere Weise miteinander verbinden können. Hier wird von einer Quantenverschränkung gesprochen. Das bedeutet vereinfacht, dass diese funktional miteinander verbunden sind, auch wenn sie sehr weit voneinander entfernt sind (auch mehrere Kilometer; Einstein hatte diesen inzwischen experimentell nachgewiesenen Effekt noch als »spukhafte Fernwirkung« bezeichnet). Wird ein Zustand für das eine Teilchen bestimmt, liegt damit auch der Zustand des anderen fest. In einem Quantencomputer sind mehrere Qubits miteinander verschränkt und können so gleichzeitig – statt sequenziell wie beim herkömmlichen Computer – Rechenoperationen ausführen (August 2014; Schughart 2017). Mit der Verschränkung möglichst vieler Qubits versprechen sich die Forscher die angenommene Verstärkung der Rechenleistung.

Bisher waren die Entwicklungen um Quantencomputer eher theoretischer Natur, doch in den letzten Jahren erfuhren diese zunehmend eine praktische Umsetzung. Die ersten Entwicklungen von Quantencomputern reicht bis in die 1980er Jahre zurück: Richard Feynman wies 1982 darauf hin, dass nur Quantencomputer potent genug seien, um quantenphysikalische Systeme und ihre Eigenschaften zu simulieren (Feynman 1982, nach Bleicher 2018). In den 1990er Jahren folgten erste theoretische Arbeiten zur Frage, wie sich mithilfe von Quantencomputern bestimmte Probleme der Informatik lösen lassen: Die Parallelisierung von Rechenschritten, wie sie mit Quantencomputern möglich sein soll, gestattet beispielsweise die Suche in sehr großen Datenbanken, die bei klassischen Computern mit zunehmender Größe der Datenbank immer zeitaufwendiger wird.

Ein wichtiger Schritt war die Entwicklung des Quantenalgorithmus von Peter Shor im Jahr 1994. Mithilfe dieses Algorithmus lassen sich Zahlen exponentiell schneller in Primfaktoren zerlegen als es zuvor möglich war (Shor 1997). Jede natürliche Zahl lässt sich als Produkt von Primzahlen darstellen. Für kleine Zahlen gelingt diese Primfaktorzerlegung leicht, bei großen Zahlen ist sie jedoch extrem aufwendig. Auf dieser Eigenschaft beruhen heute gängige Verschlüsselungsverfahren, wie das weit verbreitete RSA-Verfahren (benannt nach den Urhebern Rivest, Shamir und Adleman), weshalb bislang verwendete Verfahren der Kryptografie durch Quantencomputer angreifbar werden könnten (Monz et al. 2016). Einen weiteren Schub gab die Entwicklung eines Suchalgo-

rithmus durch Lov Grover. Mit diesem lässt sich die Suche in nichtsortierten Datenbanken gegenüber herkömmlichen Verfahren exponentiell beschleunigen (Grover 1996). Seit dem Jahr 2000 wird zunehmend nicht mehr nur an theoretischen Konzepten des Quantencomputers geforscht, sondern auch an deren praktischer Umsetzung.

Die Meinungen, bis wann ein voll funktionsfähiger Quantencomputer verfügbar sein wird, gehen auseinander. Schätzungen zufolge werden noch mindestens 10 bis 20 Jahre benötigt, einen voll funktionsfähigen Quantencomputer zu entwickeln. Derzeit prägen vor allem Universitäten, das US-Militär, die US-Geheimdienste, Technologieunternehmen, wie IBM, Google, Microsoft und Intel, sowie Start-ups, wie D-Wave (Kanada), Rigetti (USA), IonQ (USA) und Alpine Quantum Technologies (Österreich), das Forschungsfeld (Ritter 2018). Aber auch China als ein aufstrebender Akteur hat zuletzt große Investitionen getätigt und in der Forschung beachtliche Fortschritte erreicht, sodass das Land mit großer Wahrscheinlichkeit in den nächsten Jahren zur Spitze im Bereich Quantencomputer aufschließen wird (Wilhelm-Mauch 2018).

Mit Quantencomputern sollen zukünftig komplexe Fragestellungen untersucht werden, z. B. wie chemische Reaktionen oder Prozesse in biologischen Systemen ablaufen. Auf Basis dieses Wissens sollen dann neue Materialien oder pharmazeutische Wirkstoffe entwickelt werden (Hensinger 2018; Wilhelm-Mauch 2018). Insgesamt wird die Entwicklung der Quantencomputer von hoher medialer Aufmerksamkeit begleitet (Bluhm 2018). Die potenziellen Anwendungsfelder von Quantencomputern liegen nach heutiger Einschätzung im Bereich Spezialanwendungen:

- Quantenkryptografie: Gegenwärtige Verschlüsselungsverfahren beruhen auf einer asymmetrischen Kryptografie, d. h., die Verschlüsselung ist weniger aufwendig als die Entschlüsselung. Durch den Einsatz von Quantencomputern wären diese Verfahren in Zukunft nicht mehr sicher (BSI 2018, S. 5). Die Anwendung geht auf die zuvor erwähnten Arbeiten von Shor zurück, mit dessen Algorithmus die Zerlegung großer Zahlen in Primzahlenfaktoren effizienter gelöst werden kann. Allerdings können quantenmechanische Prinzipien auch für neuartige Verschlüsselungsverfahren eingesetzt werden, die die Sicherheit von Datenübertragungen auf ein neues Niveau heben könnten, z. B. durch Erzeugung und sichere Übertragung von Schlüsseln oder digitalen Signaturen (Anton/Ranade 2015, S. 26 f.). Die Kryptografie gehört neben der Simulation von Molekülen zu den am intensivsten verfolgten Anwendungen im Kontext von Quantencomputern (Hensinger 2018).
- Quantensimulation: Mithilfe von Quantencomputern könnten Quantensysteme erforscht werden, deren komplexe Eigenschaften die Rechenkapazitäten konventioneller Computer übersteigen. So ist beispielsweise die Vorher-

sage von Materialeigenschaften unter Einfluss elektrischer und magnetischer Kräfte nicht ohne weiteres möglich. Auch komplexe biologische oder chemische Systeme bzw. Prozesse können durch Reduktion der Modellkomplexität oft nur unzureichend untersucht werden. Auf Quantencomputern hingegen könnten komplexe Systeme besser simuliert werden, um so hoch präzise bzw. neuartige Vorhersagen über Systemeigenschaften zu ermöglichen. Praktische Anwendungen sind beispielsweise in der Weiterentwicklung von Düngemethoden denkbar, wenn es darum geht, komplexe biochemische Reaktionen wie die Umwandlung von elementarem Stickstoff in biologisch verfügbare Form zu verstehen (Reiher et al. 2017). Die Modellierung und Simulation chemischer Prozesse kann zudem die Entwicklung neuer Katalysatoren, die Reaktionen effizienter und unter geringerem Energieeinsatz ablaufen lassen, ermöglichen (Hempel et al. 2018). Auch in der Materialforschung, z. B. bei der Entwicklung neuer Hochtemperatursupraleiter, die Strom verlustfrei über große Distanzen leiten, oder in der pharmazeutischen Forschung, z. B. bei der Simulation von Proteinfaltungen, erhofft man sich große Erkenntnisgewinne (Hensinger 2018).

- Künstliche Intelligenz: Gegenwärtige Erkenntnisse in den Bereichen Machine Learning und Deep Learning (hier speziell Verfahren der Mustererkennung) bieten einen weiteren Anwendungsfall für Quantencomputer (Palmer 2017). Jedoch ist bislang unklar, ob beispiesweise neuronale Netze, die auf Quantencomputern eingerichtet werden, besser sind als solche auf konventionellen Computern.
- Weitere denkbare Anwendungsfälle sind das Lösen von Optimierungsproblemen oder die Suche in unstrukturierten Datenbanken. Optimierungsprobleme finden sich in den Bereichen Logistik, Warenwirtschaft und Verkehrsflusssteuerung (z. B. Flugroutenoptimierung, Routen autonomer Fahrzeuge). Auch die Optimierung von Stromflüssen in komplexen Versorgungsnetzen oder die Portfoliozusammenstellung im Wertpapierhandel werden als potenzielle Anwendungen genannt (Rosenberg et al. 2016; Wilhelm-Mauch 2018).

Bei der Entwicklung anwendungsreifer Quantencomputer ist allerdings noch eine Reihe von Herausforderungen zu lösen:

- Eine technische Herausforderung ist die Instabilität der Qubits. Damit ein Quantencomputer Berechnungen durchführen kann, müssen möglichst viele Qubits miteinander verschränkt bleiben. Die Qubits verlieren jedoch schon bei geringsten Umwelteinflüssen ihren Superpositionszustand und es kommt zur sogenannten Dekohärenz und damit zur Störung der quantenmechanischen Überlagerung möglichst vieler Zustände über einen hinreichend langen Zeitraum (Kusche 2016). Durch eine aufwendige Isolierung

müssen die Einflüsse aus der Umgebung entsprechend reduziert und außerdem die aus den Umwelteinflüssen resultierende hohe Rechenfehleranfälligkeit mittels einer Quantenfehlerkorrektur ausgeglichen werden. Hierzu benötigt man zusätzlich zu den eigentlichen Qubits, die zur Ausführungen der Berechnungen genutzt werden, eine signifikant höhere Anzahl von Qubits zur Überprüfung der Berechnungen und zur Fehlerkorrektur. Diesen hohen Anforderungen an die Hardware versuchen Forscher mithilfe neuer Algorithmen zur Quantenfehlerkorrektur zu begegnen (Palmer 2017; Ritter 2018). Die Minderung der Fehlerrate ist langfristig wahrscheinlich umsetzbar, erfordert aber noch große Forschungs- und Entwicklungsanstrengungen (Bluhm 2018).

- Die Gestaltung geeigneter physikalischer Systeme in Form von Bauteilen für Qubits und deren Skalierbarkeit ist eine weitere große Herausforderung. Qubits können mittels Ionen, Atomen oder supraleitender Schaltkreise realisiert werden. Supraleitende Qubits und Ionen-Qubits (auch Ionenfalle; Rohde/Eschner 2011) haben sich bislang als vielversprechend erwiesen (Bluhm 2018, S. 7; Hensinger 2018, S. 6). Der apparative Aufwand für ihre Herstellung ist jedoch immens. Supraleitende Systeme müssen fast auf den absoluten Nullpunkt (-273 °C) heruntergekühlt und auch Ionen-Qubits müssen in der Regel stark gekühlt werden (-200 °C). Dies begrenzt insbesondere deren Skalierung, denn die Anforderungen an Kühlsysteme und der damit verbundene Energieaufwand sind sehr groß (Anton/Ranade 2015, S. 29 f.; Hensinger 2017, S. 1; Matting 2012). Sowohl die Notwendigkeit der Kühlung als auch die der Isolierung von der Umwelt machen einen Einsatz von Quantencomputern in mobilen Endgeräten sehr unwahrscheinlich (August 2014). Eine Gruppe um den Physiker Winfried Hensinger an der Universität von Sussex, die an der Entwicklung eines voll funktionsfähigen Quantencomputers arbeitet, rechnet zudem damit, dass ein solches Gerät die Größe eines Gebäudes haben würde (Hensinger 2017). Eine weitere Problematik besteht darin, dass es bis jetzt noch kein modulares Design für Quantencomputer mit supraleitenden Qubits gibt. Der Trend geht deshalb in Richtung Ionen-Qubits-basierter Quantencomputer (Hensinger 2018).

Der Einsatz von Quantencomputern erfordert aufgrund der grundlegend unterschiedlichen Datenverarbeitung neue Softwarelösungen. Deshalb gewinnt neben der Hardwareentwicklung zunehmend auch die Schaffung geeigneter Software an Bedeutung. Dies umfasst sowohl die Entwicklung von Programmiersprachen und Benutzeroberflächen als auch die Entwicklung von Algorithmen, die auf Quantencomputern umgesetzt werden können (Palmer 2017).[1] Dabei steht die Entwicklung von Algorithmen für Quantencomputer mittlerweile in

1 Eine Übersicht der bislang entwickelten Algorithmen findet sich bei Jordan 2018.

einem Wettbewerb mit der Entwicklung konventioneller Algorithmen. Die Frage, ob bzw. wann und für welche Anwendungen Quantenalgorithmen leistungsfähiger sein werden als Algorithmen auf binären Computern, ist bisher jedoch noch ungeklärt (Bleicher 2018).

Die Forschung und Entwicklung wird weltweit von Unternehmen und Forschungsinstitutionen vorangetrieben. Mit Blick auf Veröffentlichungen zählt Deutschland im Bereich Quantencomputer nach den USA und China zu einem der publikationsstärksten Länder, gefolgt von Großbritannien, Japan und Kanada (Palmer 2017).

Auf europäischer Ebene läuft seit Ende 2017 das Quantum-Technology-Flagship-Programm (»H2020-FETFLAG-2018-2020«), das mit ca. 140 Mio. Euro in einer 3-Jahres-Periode unterstützt wird (EC 2017). In diesem Zusammenhang steht die erste Ausschreibung »QuantERA ERA-NET Cofund in Quantum Technologies« Ende 2017 mit rund 36 Mio. Euro ebenfalls für eine 3-Jahres-Periode (Quantera 2017). Nach Angaben der Europäischen Kommission (EC 2016) soll das Budget für das Quantum-Technology-Flagship-Programm innerhalb der nächsten 5 Jahre auf insgesamt 1 Mrd. Euro anwachsen (Wicht et al. 2018). Das Budget fällt gegenüber der von China verlautbarten Summe von 10 Mrd. US-Dollar allein für ein Nationales Zentrum für Quanteninformationswissenschaft, das bis 2020 fertiggestellt sein soll, eher gering aus (South China Morning Post 2018). Das Forschungsbudget für Quantentechnologien der USA liegt im Vergleich bei ca. 200 bis 360 Mio. Euro pro Jahr (South China Morning Post 2018; Wicht et al. 2018).

Zur Förderung der Quantentechnologien in Deutschland und als Vorbereitung auf das europäische Flaggschiffprogramm hatte das Bundesministerium für Bildung und Forschung (BMBF) die nationale Initiative »Quantentechnologie – Grundlagen und Anwendungen (QUTEGA)« eingerichtet, die ihre Arbeit mittlerweile abgeschlossen hat.[2] Anfang 2017 veröffentlichte diese Arbeitsgruppe ein Konzeptpapier, dessen Ergebnisse in die Gestaltung von Fördermaßnahmen einflossen (QUTEGA 2017). Die Erforschung von Quantentechnologien findet auf Bundesebene innerhalb von drei Fördermaßnahmen statt. Dabei handelt es sich um das Programm »Schlüsselkomponenten für Quantentechnologien«, den Nachwuchswettbewerb »Quantum Futur« im Rahmen des Förderprogramms »Photonik Forschung Deutschland« sowie die Förderung von Forschungsinitiativen zu »Anwendungsszenarien der Quantenkommunikation« im Rahmen des Forschungsrahmenprogramms zur IT-Sicherheit »Selbstbestimmt und sicher in der digitalen Welt«.

Auf Seiten unternehmerischer Forschung und Entwicklung arbeiten mittlerweile viele führende Technologieunternehmen an Quantencomputern und

2 www.qutega.de

tätigen beträchtliche Investitionen. Neben Intel, Hewlett-Packard und Microsoft haben vor allem Google und IBM in den letzten Monaten öffentlichkeitswirksam ihre erreichten Ergebnisse präsentiert: Im März 2018 stellte Google mit »Bristlecone« den ersten Quantencomputer mit 72 Qubits vor. Ein Jahr zuvor lag der Rekord noch bei 50 Qubits und wurde von IBM gehalten.[3]

Gesellschaftliche und politische Relevanz

Die Anwendungs- und Marktpotenziale von Quantencomputern und -algorithmen sind heute noch nicht vorauszusagen. Erste praktische Anwendungen werden derzeit erforscht. Mittelbar können die Fortschritte im Bereich der Quantencomputer auch andere Quantentechnologien oder Teilkomponenten, wie beispielsweise Sensorsysteme, die ebenfalls in der Medizintechnik oder Navigation genutzt werden können, hervorbringen. Anbieter von relevanten Technologien, wie spezifischen Elektronikkomponenten, Bauelementen, Kryo- und Lasertechnik etc., sind in der Mehrzahl kleine und mittlere Unternehmen (Ritter 2018). Der Umsatzanteil deutscher Firmen an den weltweit in der Entwicklung befindlichen Quantentechnologien (Laboranwendungen) wird auf rund 10 % geschätzt (Palmer 2017).

Nach jetziger Einschätzung ist nicht davon auszugehen, dass Quantencomputer auf absehbare Zeit eine breite gesellschaftliche Anwendung finden, sondern nur durch etwaige Nutzung mittels Clouddiensten das Anwendungsspektrum für PCs und mobile Endgeräte erweitern könnten. Die technischen Herausforderungen für ein Funktionieren von Quantenprozessoren (Kühlung, Vakuum, etc.) sind zu anspruchsvoll, als dass sie im privaten Kontext einsetzbar wären (Bluhm 2018; Wilhelm-Mauch 2018). Auch werden Quantencomputer klassische Computer nicht ablösen, sondern eher ergänzen, weil die herkömmlichen Computer eine deutlich geringere Störanfälligkeit haben und in vielen Anwendungsbereichen überlegen sind (Ritter 2018). Wahrscheinlich werden für Quantencomputer Rechenzentren entstehen, auf die – wie heute schon bei Supercomputern üblich – von extern über ein Netzwerk zugegriffen werden kann. Diese Entwicklung entspricht im Prinzip der Situation der Entwicklungsanfänge der klassischen Computer (Ritter 2018; Wilhelm-Mauch 2018), eine Abschätzung des zukünftigen Entwicklungspotenzials ist jedoch zum jetzigen Zeitpunkt eher spekulativ.

Durch die Entwicklung von Quantencomputern können sich sowohl positive als auch kritisch zu bewertende Technikfolgen ergeben:

3 www.qubitcounter.com

- Quantencomputer bzw. die Schaffung der für sie geeigneten Rahmenbedingungen (insbesondere tiefe Temperaturen, Ultrahochvakuum) benötigen sehr viel Energie, auch wenn der Energiebedarf im Vergleich zu herkömmlichen Supercomputern geringer auszufallen scheint (Wilhelm-Mauch 2018). Effiziente Nutzungsalgorithmen bieten hier Ansatzpunkte für Energieeinsparungen (Ritter 2018).
- Die Anwendung der Quantencomputer kann aber auch zu Energie- und Ressourceneinsparung führen. Potenziale bestehen beispielsweise in der Simulation effizienterer chemischer Prozesse oder der Lösung von Optimierungsproblemen der Logistik. Beispielsweise könnte die Simulation der Ammoniaksynthese für die Düngemittelproduktion weltweit zu Energie- und Ressourceneinsparungen führen, wenn es gelingt, effizientere Syntheseverfahren zu entwickeln (Ritter 2018) als den bisherigen Haber-Bosch-Prozess, der für ca. 3 % des weltweiten CO_2-Ausstoßes verantwortlich ist (Wilhelm-Mauch 2018). Auch die Lösung logistischer Problemstellungen könnte zu mehr Energieeffizienz und CO_2-Einsparung führen (Bluhm 2018).
- Chancen und Risiken liegen zudem darin, dass die gängigen Verschlüsselungstechnologien in der IT-Sicherheit angreifbar werden (Bluhm 2018; Ritter 2018; Wilhelm-Mauch 2018). Derzeit noch sichere Informationen könnten bereits heute gespeichert und zu einem späteren Zeitpunkt mittels Quantencomputern entschlüsselt werden (Ritter 2018). Daneben bietet die Quantenkryptografie selbst neue Möglichkeiten der Verschlüsselung, d. h., es werden quantenkryptografische Verfahren, also Verschlüsselungsmethoden, entwickelt, die auf den quantenmechanischen Prinzipien basieren (Bluhm 2018; BSI 2018; Ritter 2018).

Konkrete Regulierungsbedarfe bei der Entwicklung der Quantencomputer bestehen aus Expertensicht momentan nicht (Hensinger 2018). Die Entwicklungen sollten vergleichbar mit denen im Bereich Supercomputer beobachtet werden (Bluhm 2018). Um jedoch eine offene Zugänglichkeit der Wissenschaft weiterhin zu gewährleisten, die durch die Entstehung von Oligopolen im Bereich amerikanischer Hardwareentwicklung behindert werden könnte, wird von den Experten als europäisches Gegengewicht eine offene Kooperations- und Entwicklungsplattform für den Bereich Quantencomputing vorgeschlagen (Wilhelm-Mauch 2018, S. 3).

Mögliche Bearbeitung des Themas

In jüngster Zeit hat eine intensivere Beschäftigung mit dem Thema Quantencomputer eingesetzt, im Bundestag zuletzt in Form der Befragung von Experten

aus Wissenschaft und Wirtschaft im Rahmen der Öffentlichen Anhörung am 6. Juni 2018 zum Thema »Quantencomputer« des Ausschusses Digitale Agenda des Deutschen Bundestages.[4] Bereits 2015 wurde von Leopoldina, acatech und der Union der deutschen Akademien der Wissenschaften ein Positionspapier mit dem Titel »Perspektiven der Quantentechnologien« veröffentlicht (Anton/Ranade 2015). 2017 wurde ein Positionspapier der Deutschen Industrie »Förderung von Quantentechnologie« (Förtsch et al. 2017) publiziert, in dem auch auf Technikfolgen eingegangen wird. Kürzlich wurde vom Bundesamt für Sicherheit (BSI) eine Studie zum Entwicklungsstand von kryptografisch relevanten Quantencomputern vorgestellt (BSI 2018), um im BSI selbst auf dieser Basis den Einsatz von Post-Quanten-Kryptografie (Kryptografieverfahren, die selbst unter Nutzung von Quantencomputern praktisch nicht zu entschlüsseln sind) besser antizipieren bzw. planen zu können (Wilhelm-Mauch 2018).

Vor diesem Hintergrund und angesichts des insgesamt nach wie vor frühen Entwicklungsstands erscheint eine Behandlung im Rahmen einer Technikfolgenabschätzung derzeit nicht vordringlich. Da sich das Thema aber mit hoher Dynamik weiterentwickeln wird, sollte es beobachtet werden, um es ggf. zu einem späteren Zeitpunkt, wenn sich die Anwendungsszenarien deutlicher abzeichnen sollten, vertiefend zu bearbeiten.

Literatur

Anton, C.; Ranade, K. (2015): Perspektiven der Quantentechnologien. Stellungnahme Juni 2015. Nationale Akademie der Wissenschaften Leopoldina e. V. (Leopoldina); Deutsche Akademie der Technikwissenschaften e. V. (acatech); Union der deutschen Akademien der Wissenschaften (Akademieunion). Halle (Saale)

August, K. (2014): Nachgefragt! Was ist eigentlich ein Quantencomputer? Hermann von Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V., 7.4.2014, www.helmholtz.de/technologie/was-ist-eigentlich-ein-quantencomputer/ (25.7.2018)

Bleicher, A. (2018): Quantum Algorithms Struggle Against Old Foe: Clever Computers. Quanta Magazine, 1.2.2018, www.quantamagazine.org/quantum-computers-struggle-against-classical-algorithms-20180201/ (28.5.2018)

Bluhm, H. (2018): Stellungnahme zum Thema Quantencomputer für die Anhörung im Ausschuss Digitale Agenda des Deutschen Bundestages am 06.06.2018. Deutscher Bundestag, Drucksache 19(23)14, www.bundestag.de/blob/558196/c18430f92a54f4c4743e18d84b64c00f/a-drs-19-23-14-data.pdf (24.7.2018)

4 Dokumente verfügbar unter www.bundestag.de/ausschuesse/a23_digital/anhoerungen/anhoerung/557930

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2018): Entwicklungsstand Quantencomputer. Deutsche Zusammenfassung. BSI-Projektnummer 283. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Zusammenfassung.pdf?__blob=publicationFile&v=4 (19.7.2018)

EC (European Commission) (2016): European Commission will launch €1 billion quantum technologies flagship. 17.5.2016, https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship (29.8.2018)

EC (European Commission) (2017): FET Flagship on Quantum Technologies. 27.10.2017, http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/fetflag-03-2018.html (7.8.2018)

Feynman, R. (1982): Simulating Physics with Computers. In: International Journal of Theoretical Physics 21(6/7), S. 467–488

Filipp, S. (2018): Quantencomputer: Der Beginn der kommerziellen Quanten-Ära. IBM, 23.2.2018, www.ibm.com/de-de/blogs/think/2018/02/23/quantencomputer/ (31.5.2018)

Förtsch, M.; Kaenders, W.; Riedel, M.; Strohm, T.; Totzeck, M. (2017): Förderung von Quantentechnologien. Positionspapier der Deutschen Industrie. VDI Technologiezentrum GmbH. Düsseldorf

Grover, L. (1996): A fast quantum mechanical algorithm for database search. Cornell University, 29.5.1996, https://arxiv.org/abs/quant-ph/9605043 (25.7.2018)

Hempel, C.; Maier, C.; Romero, J.; McClean, J.; Monz, T.; Shen, H.; Jurcevic, P.; Lanyon, B.; Love, P.; Babbush, R.; Aspuru-Guzik, A. et al. (2018): Quantum Chemistry Calculations on a Trapped-Ion Quantum Simulator. In: Phys. Rev. X 8, S. 1–22

Hensinger, W. (2017): Quantum computing. In: Al-Khalili, J. (Hg.): Whats next? Even Scientists Can't Predict the Future - or Can They? London, S. 129–139

Hensinger, W. (2018): Stellungnahme zum Fragenkatalog zur öffentlichen Anhörung »Quantencomputer« des Ausschusses Digitale Agenda am Mittwoch den 6. Juni 2018. Deutscher Bundestag, Drucksache 19(23)11, www.bundestag.de/blob/558022/b24a891d2915213a085e373a175a953f/a-drs-19-23-11-data.pdf (24.7.2018)

Jordan, S. (2018): Quantum Algorithm Zoo. A comprehensive catalog of quantum algorithms. Microsoft Quantum. https://math.nist.gov/quantum/zoo/ (13.7.2018)

Kelly, J. (2018): A Preview of Bristlecone, Google's New Quantum Processor. Google Al B,log, 5.3.2018, https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (31.5.2018)

Kusche, N. (2016): Wie funktioniert ein Quantencomputer? Welt der Physik, 26.2.2016, www.weltderphysik.de/gebiet/technik/quanten-technik/einfuehrung-quantencomputer/ (25.7.2018)

Matting, M. (2012): Wie der Quanten-Computer funktioniert. Heise Online, 13.7.2012, https://heise.de/-3394901 (25.7.2018)

Monz, T.; Nigg, D.; Martinez, E.; Brandl, M.; Schindler, P.; Rines, R.; Wang, S.; Chuang, I.; Blatt, R. (2016): Realization of a scalable Shor algorithm. In: Science 351(6277), S. 1068–1070

Musser, G. (2018): Job One for Quantum Computers: Boost Artificial Intelligence. Quanta Magazine, 29.1.2018, www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/(28.5.2018)

Palmer, J. (2017): Quantum technology is beginning to come into its own. The Economist, www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own (19.7.2018)
Quantera (2017): QuantERA Call 2017. www.quantera.eu/co-funded-call/call-2017 (29.8.2018)
QUTEGA (Quantentechnologie von Grundlagen bis Anwendungen) (2017): Quantentechnologie. Grundlagen und Anwendungen. Konzeptpapier der Nationalen Initiative zur Förderung der Quantentechnologie von Grundlagen bis Anwendungen (QUTEGA). www.qutega.de/fileadmin/qutega/Qutega_Grundlagenpapier.pdf (8.8.2018)
Reiher, M.; Wiebe, N.; Svore, K.; Wecker, D.; Troyer, M. (2017): Elucidating reaction mechanisms on quantum computers. In: Proceedings of the National Academy of Sciences of the United States of America 114(29), S. 7555–7560
Ritter, S. (2018): Stellungnahme zum Thema Quantencomputer für die Anhörung im Ausschuss Digitale Agenda des Deutschen Bundestages am 6.6.2018. Deutscher Bundestag, Drucksache 19(23)10, www.bundestag.de/blob/558018/3fc6bad8412a3bfeabc64b96e146f2a3/a-drs--19-23-10-data.pdf (24.7.2018)
Rohde, F.; Eschner, J. (2011): Quantum computation with trapped ions and atoms. In: Miniatura, C.; Kwek, L.-C.; Ducloy, M.; Grémaud, B.; Englert, B.-G.; Cugliandolo, L.; Ekert, A.; Phua, K. (Hg.): Ultracold Gases and Quantum Information, S. 218
Rosenberg, G.; Haghnegahdar, P.; Goddard, P.; Carr, P.; Wu, K.; de Prado, M. (2016): Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer. In: IEEE Journal of Selected Topics Signal Processing 10(6), S. 1053–1060
Schughart, A. (2017): Was genau sind Quantencomputer – und was können sie? Wired, 13.11.2017, www.wired.de/collection/science/was-genau-sind-quantencomputer-und-was-koennen-sie (7.8.2018)
Shor, P. (1997): Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: SIAM Journal on Computing 26(5), S. 1484–1509
South China Morning Post (2018): Is China winning race with US to develop quantum computers? South China Morning Post, 9.4.2018, www.scmp.com/news/china/economy/article/2140860/china-winning-race-us-develop-quantum-computers (8.8.2018)
Wicht, A.; Krutzik, M.; Thoss, A. (2018): Quantum Technology: Quantum sensing is gaining (s)pace. LaserFocusWorld, 18.1.2018, www.laserfocusworld.com/articles/print/volume-54/issue-01/features/quantum-technology-quantum-sensing-is-gaining-s-pace.html (8.8.2018)
Wilhelm-Mauch, F. (2018): Antworten zum Fragenkatalog zur öffentlichen Anhörung »Quantencomputer« des Ausschusses Digitale Agenda am Mittwoch den 6. Juni 2018. Deutscher Bundestag, Drucksache 19(23)009, www.bundestag.de/blob/557952/9bbe5fbf00627b43ba08137f38e52d25/a-drs--19-23-09-data.pdf (24.7.2018)

TAB

**BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG**

KARLSRUHER INSTITUT FÜR TECHNOLOGIE

Neue Schönhauser Straße 10
10178 Berlin

Tel.: +49 30 28491-0
Fax: +49 30 28491-119

buero@tab-beim-bundestag.de
www.tab-beim-bundestag.de