Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)10

TOPTICA Photonics AG · Lochhamer Schlag 19 · D-82166 Gräfelfing

Deutscher Bundestag
Ausschuss Digitale Agenda
11011 Berlin

per E-Mail an:
ada@bundestag.de

TOPTICA Photonics AG
Lochhamer Schlag 19
D - 82166 Gräfelfing
Telefon: +49 89 85837-217
Telefax: +49 89 85837-200
Email: stephan.ritter@toptica.com
Internet: http://www.toptica.com
Sitz: Gräfelfing
HRB-München: 137368
VAT-Nr.: DE 192124378
Deutsche Bank München
SWIFT/BIC: DEUTDEMM
Konto: 2104297
DE 20 7007 0010 0210 4297 00
Bayerische Landesbank München
SWIFT/BIC: BYLADEMMXXX
Konto: 4191096
DE 81 7005 0000 0004 1910 96

Gräfelfing, 3. Juni 2018

Fragenkatalog zur öffentlichen Anhörung „Quantencomputer“ des Ausschusses Digitale Agenda am Mittwoch den 6. Juni 2018 – beantwortet von Stephan Ritter

1) Wie ist der Stand von Forschung und Technik auf dem Gebiet des Quantencomputing?

Die Idee zum Quantencomputing entstand in den Achtzigerjahren und ist eng mit der Idee der Quantensimulation verknüpft. Größere Bedeutung und Aufmerksamkeit bekam dieses Thema mit den ersten Arbeiten zu Quantenalgorithmen, insbesondere dem von Peter Shor 1997 vorgestellten Faktorisierungsalgorithmus, weil hierdurch die breite Relevanz des Themas evident wurde. So könnten, die notwendige Quantencomputerhardware vorausgesetzt, mit dem Shor-Algorithmus gängige Kryptographieverfahren erfolgreich angegriffen werden. Derzeit erlebt die Entwicklung von Quantencomputern einen Übergang aus der Grundlagenforschung hin zu ersten kommerziellen Angeboten. Für ein größeres öffentliches Interesse hat eine breite Berichterstattung in den Medien gesorgt, ausgelöst oder verstärkt auch dadurch, dass die kanadische Firma D-Wave Systems Inc. im Jahre 2011 den ersten kommerziellen Quantencomputer ankündigte.

Begleitet wurde deren Marktauftritt von berechtigter Kritik, dass die angebotene Maschine keinen universellen (*general purpose*) Quantencomputer im engeren Sinne darstellt. Stattdessen handelt es sich um einen adiabatischer Quantencomputer oder *quantum annealer*, der den minimalen Energiezustand eines vorher definierten quantenmechanischen Systems findet. Universelle Quantencomputer arbeiten typischerweise nach dem Quantengattermodell, das auf einer Verkettung diskreter Logikgatter basiert. Beide Ansätze sind prinzipiell gleich effizient.

Quantenbits (Qubits) sind das Analogon zum Bit eines klassischen Computers, und als quantenmechanisches Zweizustandssystem die kleinste Speichereinheit für Quanteninformation. D-Wave bietet derzeit ein System mit 2000 supraleitenden, jedoch nicht vollständig kohärenten Quantenbits an. Mittlerweile gibt es auch einige Firmen, die universelle Quantencomputer entwickeln. Hier sind insbesondere die Aktivitäten von Alphabet (Google; derzeit 72 supraleitende Quantenbits), IBM Q (derzeit 50 Quantenbits), Intel (in Zusammenarbeit mit QuTech in Delft, Niederlande; derzeit 49 Quantenbits) und Microsoft Station Q (unter anderem in Zusammenarbeit mit Forschern in Delft, Kopenhagen und Zürich; topologisches Quantencomputing) zu nennen. Eine Fokussierung allein auf die Anzahl der Quantenbits zur Beurteilung der Leistungsfähigkeit eines Quantencomputers würde zu kurz greifen. Kohärenzzeiten, die Qualität von Logikgatteroperationen und deren Dauer sowie viele weitere Aspekte sind nicht weniger relevante Kriterien für die Gesamtperformance.

Noch lässt sich nicht mit Sicherheit sagen, auf welcher Technologie zukünftige Quantencomputer beruhen werden. Derzeit sind supraleitende Systeme, die in Kryostaten knapp über dem absoluten Temperaturnullpunkt betrieben werden müssen, vorherrschend. Ein anderes physikalisches System, das nicht nur sehr gut erforscht ist, sondern für dessen Skalierbarkeit interessante Vorschläge existieren, sind gefangene Ionen. Einen darauf basierenden Quantencomputer entwickelt derzeit die Firma IonQ Inc. in der Nähe von Washington. Die kürzlich gegründete Alpine Quantum Technologies GmbH, ein Spin-off der Universität Innsbruck, hat dasselbe Ziel. Auch neutrale Atome, etwa gefangen in optischen Gittern, werden bezüglich Ihrer Eignung für die Realisierung eines Quantencomputers erforscht. Des Weiteren gibt es Konzepte für optisches Quantencomputing. Insbesondere für die Übertragung von Quantenzuständen in Quantennetzwerken, die zur Vernetzung von Quantencomputern, für die Quantenkryptographie und vieles mehr verwendet werden können, sind photonische Quantenbits essentiell.

Es muss betont werden, dass ein Quantencomputer völlig unabhängig von der Hardware nur für sehr spezielle Problemstellungen einen auch nur prinzipiellen Vorteil gegenüber einem klassischen Computer bietet. Ein Vorteil ist dabei so definiert, dass – vereinfacht gesagt – die Zunahme des Rechenaufwands mit der Größe der Aufgabe beim Quantencomputer dramatisch geringer ist als beim klassischen Pendant. Diese Tatsache lässt zunächst keine Aussage darüber zu, welcher Computer für ein konkretes Problem gegebener Größe besser geeignet ist. Letztere Fragestellung ist nämlich unter anderem von der Geschwindigkeit der einzelnen Rechenschritte (Gatteroperationen) und damit der verwendeten Hardware abhängig. Für bestimmte Fragestellungen kann man jedoch pauschal sagen, dass man immer eine Problemgröße angeben kann, ab der ein gegebener Quantencomputer, der prinzipiell in der Lage ist die gestellte Aufgabe zu lösen, besser performt als ein beliebiger gegebener klassischer Computer. Prinzipiell lässt sich jeder Quantencomputer auf einem klassischen Computer simulieren, allerdings stoßen derzeitige klassische Computer und Algorithmen schon bei der Simulation von Quantencomputern mit etwa 50 Quantenbits an ihre Grenzen. Auch gibt es keine Berechnung, die man nicht ebenfalls auf einem klassischen Computer abbilden könnte. Allerdings ist dies für viele Probleme nicht effizient möglich, und damit aus praktischer Sicht in gegebener Zeit unmöglich.

Ein großes derzeit propagiertes Ziel für Quantencomputer der nächsten Generation ist die Erzielung von Ergebnissen, die mit dann existierenden klassischen Supercomputern nicht zu erreichen sind. Eine solche Situation wird mit dem Begriff des Quantenvorteils (*quantum advantage* oder *quantum supremacy*) beschrieben und wäre der erste große praktische Nachweis des Nutzens eines Quantencomputers. Nach Aussage einiger Forscher, unter anderem bei Google, steht die Demonstration eines Quantenvorteils kurz bevor. Hierzu wird aber sicherlich eine sehr spezielle Problemstellung gewählt werden, bezüglich der die intrinsischen Vorteile eines Quantencomputers besonders gut genutzt werden können.

Die vielleicht größte Herausforderung bezüglich eines Quantencomputers liegt in der Skalierung der Hardware. Vereinfacht gesagt nimmt der technologische Aufwand mit der Länge der Berechnung überproportional zu. Auch die Anforderungen an die benötigte Qualität jedes einzelnen Rechenschritts steigt, weil Quantenbits die Fehlertoleranz klassischer Bits fehlt. Es existieren zwar Verfahren zur Quantenfehlerkorrektur, bei der ein logisches Quantenbit in mehreren, typischerweise vielen, physikalischen Quantenbits kodiert wird. Dies ist ein potentieller Ausweg aus der prinzipiellen Fehleranfälligkeit eines Quantencomputers. Es verschärft aber das Skalierungsproblem insofern, als dass die Anzahl der für eine Berechnung benötigten Quantenbits dramatisch ansteigt, was wiederum den technologisch-apparativen Aufwand wachsen lässt. Daher konzentrieren sich die Forschungsanstrengungen derzeit und absehbar für die nächsten Jahre auf Problemstellungen und Algorithmen, die ohne Quantenfehlerkorrektur gelöst werden können.

Die Forschung und Entwicklung von Quantencomputern muss im Kontext der Quantentechnologien gesehen werden. Diesem großen Gebiet der Forschung und Technik werden Technologien zugeordnet, die durch die gezielte Manipulation einzelner Quantensysteme und die Ausnutzung intrinsisch quantenmechanischer Eigenschaften wie Superposition und Verschränkung ausgezeichnet sind. Hierdurch können zum Beispiel eine höhere Empfindlichkeit von Sensoren oder eine größere Präzision von Uhren erzielt werden. Die Quantenkommunikation und -simulation sind weitere Teilgebiete der Quantentechnologien.

2) Welche Position haben im internationalen Vergleich Deutschland und Europa? Wer ist – im nationalen und im internationalen Vergleich – Vorreiter auf dem Gebiet des Quantencomputing, hinsichtlich Grundlagenforschung, anwendungsorientierter Forschung, technischer Entwicklung, sowie der Entwicklung möglicher Geschäftsmodelle? Welche Unternehmen/Akteure sind besonders hervorzuheben?
Welche Position haben China und die USA (Welche Ausprägungen der Technologie sind wo verbreitet?) Sollte die internationale Zusammenarbeit auf diesem Gebiet – z.B. im Bereich der Forschung, der industriellen Anwendung oder der Herstellung von QC – gestärkt werden?

McKinsey hat die Investitionen in nichtgeheime Forschung zu Quantentechnologien für 2015 abgeschätzt[1], und kommt auf ein Gesamtvolumen von 1,5 Mrd. €. Davon sind die fünf Länder mit den größten Investitionen die USA (360 Mio. €), China (220 Mio. €), Deutschland (120 Mio. €), Vereinigtes Königreich (105 Mio. €) und Kanada (100 Mio. €). Auch Australien, die Schweiz und Japan investieren massiv in diesem Bereich. 550 Mio. € entfallen auf die EU inklusive UK. Diese Zahlen lassen natürlich keine direkte Aussage bezüglich des Quantencomputing zu, geben aber eine gute Orientierung. Ein offensichtlicher regionaler Schwerpunkt der Entwicklung und Erforschung von Quantencomputern liegt in den USA, vermutlich sogar überproportional im Vergleich zu den oben genannten Summen für Investitionen in Quantentechnologien allgemein. Aber auch in Europa ist man bezüglich dieses Themas aktiv, und es gibt viele nennenswerte Forschungsgruppen und Akteure. Derzeit treiben Universitäten, US Militär und US Geheimdienste, etablierte, finanzstarke Firmen (unter anderem IBM, Google, Microsoft, Intel) sowie zum Teil gut finanzierte Start-ups (unter anderem D-Wave, Rigetti, IonQ, Alpine Quantum Technologies) das Feld. Es ist anzumerken, dass US-amerikanische Förderprogramme auch Forschung außerhalb der USA, beispielsweise in Delft und Innsbruck, finanzieren. Derzeit wird viel spektakuläre Entwicklung von Firmen getrieben. Die dortigen Abteilungen sind allerdings oft aus universitären Forschungsgruppen heraus entstanden, bauen auf deren Ergebnissen auf und arbeiten zum Teil nach wie vor mit diesen zusammen. In den USA boomen Start-ups im Umfeld des Quantencomputing, insbesondere auch mit Quantentechnologieberatung und Softwareentwicklung für Quantencomputer. Hier wären für Deutschland und Europa mehr Aktivitäten wünschenswert. In einer Studie des BSI[2] aber auch im Internet gibt es zahlreiche Listen von Akteuren in den Bereichen Quantencomputing und Quantentechnologie, die natürlich keinen Anspruch auf Vollständigkeit erheben, aber einen Eindruck vermitteln können[3,4]. China ist besonders stark in der Quantenkommunikation, hat aber meines

[1] siehe z. B. Laser Focus World, Feb. 2018 oder https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own.
[2] *Entwicklungsstand Quantencomputer*, Frank K. Wilhelm et al., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie.pdf?__blob=publicationFile&v=4.
[3] *List of companies involved in quantum computing or communication*, abrufbar unter, https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication.
[4] *Quantum Computing Report*, abrufbar unter https://quantumcomputingreport.com/.

Wissens bisher noch keine spektakulären Erfolge beim Quantencomputing vermeldet. Vor dem Hintergrund der Stärke bei anderen Quantentechnologien und der großen politischen Begeisterung für dieses Thema ist allergings zu erwarten, dass sich dies ändern wird.

Die internationale Zusammenarbeit, insbesondere im Bereich der Forschung und Technologieentwicklung, sollte unbedingt gestärkt werden. Zur Begründung sei insbesondere auf den momentan noch immensen Forschungsbedarf zu diesem Thema verwiesen. Die Erfolge der Grundlagenforschung – und hier ist das Quantencomputing nach wie vor anzusiedeln – sind zu einem nicht geringen Teil auf internationalen Austausch, Kollaborationen und Offenheit zurückzuführen. Getrieben durch nationale oder regionale Förderprogramme und politische Interessen gibt es einen Trend zu nationalen oder regionalen Alleingängen, die durch die Beteiligung von Firmen mit einer verständlicherweise eingeschränkten Transparenz bezüglich Details Ihrer Ergebnisse noch verstärkt werden. Solange das große Potential und die hiermit verbundenen riesigen Erwartungen an das Quantencomputing auf der einen Seite und der aktuelle Stand der Technik auf der anderen noch so weit auseinanderliegen wie bisher, sind Alleingänge nicht zu empfehlen. Bei der derzeitigen rasanten internationalen Entwicklung des Themas ist nicht zu erwarten, dass geheime Forschung entscheidende Vorteile verschaffen würden. Im Gegenteil würden hiermit Märkte wegfallen und ein internationales Klima der nationalen Alleingänge würde den Fortschritt des Quantencomputers behindern.

3) Welche möglichen gesellschaftlichen Chancen oder gesellschaftlichen Herausforderungen sehen Sie durch Quantencomputing? Welche Auswirkungen können Sie auf unser tägliches Leben haben? Ergeben sich spezielle Herausforderung, sobald diese Computer marktreife und entsprechende Verbreitung erlangen? Welche ökologischen Chancen oder Risiken bieten sich durch den Einsatz von Quantencomputing (z.B. Thema Green IT)?

Für eine belastbare Beantwortung dieser Fragen ist die Forschung zum Thema Quantencomputer noch nicht weit genug vorangeschritten. Insbesondere sind viele der Aufgaben, für die ein Quantencomputer zukünftig eingesetzt werden kann, noch gar nicht abzusehen. Hierzu ist weitere Forschung notwendig, insbesondere theoretische Arbeiten, die zunächst einmal ganz unabhängig von der Hardwareentwicklung zu sehen sind. Denn die Bedeutung eines existierenden Quantencomputers hängt entscheidend von den Algorithmen ab, die effizient auf ihm laufen können. Es gibt sicherlich noch ein großes Potential bisher unentdeckter Anwendungen. Hier kann nur motiviert werden, weitere Forschung auf diesem Gebiet zu unterstützen, um ein besseres Verständnis des Potentials aber auch der durch einen Quantencomputer hervorgerufenen Risiken zu erlangen.

Ökologische Chancen und Risiken existieren sicherlich ganz vordergründig bezüglich des Energiebedarfs zukünftiger Quantencomputer. Effizientere Algorithmen bieten prinzipiell die Chance einer energieeffizienteren Berechnung eines gegebenen Problems, aber neue Möglichkeiten wecken natürlich auch neue Bedürfnisse. Ein derzeit oft zitiertes Beispiel für das enorme Potential von Quantencomputer betrifft die Simulation von Quantensystemen bei chemischen Prozessen. So könnte eine Quantensimulation der Ammoniaksynthese für die Düngemittelproduktion weltweit zu gigantischen Energieeinsparungen führen, wenn mit ihrer Hilfe effizientere Syntheseverfahren entwickelt würden.

Quantencomputer werden klassische Computer nicht ablösen, sondern nur ergänzen. Für die meisten Aufgaben ist ein klassischer Computer algorithmisch ebenso gut geeignet, es gibt seit Jahrzehnten Hardwareentwicklung gemäß dem Mooreschen Gesetz und eine fundamental geringere Störanfälligkeit. Daher wird ein klassischer Computer in den meisten Anwendungsbereichen überlegen bleiben und die Existenz von Quantencomputern in diesen Bereichen keine wichtige Rolle spielen. Dies ist fun-

damental anders für die speziellen Aufgaben, bei denen die konzeptionellen Stärken von Quantencomputer gezielt genutzt werden können. Es werden Rechenzentren für Quantencomputer entstehen, und man wird auf sie wie bei klassischen Supercomputern auch über ein Netzwerk zugreifen. Somit ist eine Nutzung von Quantencomputern prinzipiell von jedem Endgerät mit Netzwerkanbindung aus möglich. Allerdings könnte der Zugang auf nur bestimmte Nutzerkreise oder Nationen beschränkt sein, wenn die Technologie für Quantencomputer nur in den Händen einzelner Firmen oder Nationen existiert. Ein solches Szenario ist unbedingt zu vermeiden, wenn die gesamte Menschheit von dem Potential des Quantencomputing profitieren soll. Hier gibt es Analogien zum Thema des flächendeckenden schnellen Netzzugangs.

4) Sehen Sie zum jetzigen Zeitpunkt regulatorische Anforderungen? Sehen Sie – legislativen und nicht-legislativen – Handlungsbedarf der Politik? Gibt es voraussichtlich einen Handlungsbedarf zum „Thema Dual Use“?

Derzeit ist die gesellschaftliche Bedeutung eines Quantencomputers noch nicht vollständig abzusehen. Um so begrüßenswerter ist die Tatsache, dass Fragen zum Handlungsbedarf der Politik zu einem so frühen Zeitpunkt gestellt werden. Es sollte international auf einen möglichst offenen Umgang mit Ergebnissen zu diesem Thema hingewirkt werden. Ich halte den Versuch, sich durch Geheimhaltung einen nationalen Vorteil zu verschaffen, für nicht zielführend. Vor der Größe der Aufgabe und dem Nachdruck, mit dem andere Länder, allen voran die USA, an diesem Thema arbeiten, würde ich die Erfolgsaussichten dafür als eher gering einschätzen. Gleichzeitig gilt es zu verhindern, dass andere durch geheime neue Entwicklungen und Erkenntnisse im Bereich des Quantencomputing sich Vorteile verschaffen, die uns nicht zur Verfügung stehen oder – noch schlimmer – die uns nicht einmal bekannt sind. Daher plädiere ich, zumindest für die nähere Zukunft, für einen möglichst offenen Umgang mit der Forschung zu diesem Thema.

5) Welche Projekte und Erkenntnisse der Technikfolgenabschätzung existieren bereits für den Bereich des Quantencomputing?

Theoretische Arbeiten lassen erwarten, dass zukünftige Quantencomputer die Sicherheit derzeit verwendeter Verfahren für Schlüsselaustausch, asymmetrische Verschlüsselung und Signatur (z. B. RSA) gefährden. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt es daher eine ausführliche Studie zum Entwicklungsstand von kryptographisch relevanten Quantencomputern[2]. In den USA hat das National Institute of Standards and Technology (NIST) einen Wettbewerb zu Post-Quanten-Kryptographie ausgerufen[5]. Kurz gesagt geht es um Verfahren, die auch gegen Angriffe mit einem Quantencomputer sicher sind. Hierbei ist zu bedenken, dass alleine die Möglichkeit, dass es in Zukunft einen leistungsstarken Quantencomputer geben könnte, schon eine Bedrohung darstellt. Derzeit sicher verschlüsselte Nachrichten könnten von Angreifern zwischengespeichert und dann mit zukünftigen Quantencomputern nachträglich entschlüsselt werden. Die Nachricht wäre also nicht dauerhaft geheim. Quantencomputer werden voraussichtlich beschleunigenden Einfluss auf Entwicklungen der künstlichen Intelligenz und des maschinellen Lernens haben. Damit würden dann indirekt die Technikfolgen dieser Bereiche verstärkt. In einer Stellungnahme von Leopoldina, acatech und der Union der

[5] NIST Webseite, abrufbar unter https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
Algorithmenwettbewerb zur Post-Quanten-Kryptographie: Gegen die Apokalypse, Claus Diem, Klaus Schmeh, iX 6/2018, Seite 116 ff.

deutschen Akademien der Wissenschaften „Perspektiven der Quantentechnologien“[6] und einem Positionspapier der Deutschen Industrie zur „Förderung von Quantentechnologien“[7] wird kurz auf Technikfolgenabschätzung und Risiken eingegangen. Eine breite Debatte und Diskussion des Themas unter Experten, aber auch in der Bevölkerung, ist wünschenswert. Hierbei sollten die Chancen und Risiken gleichermaßen benannt und Erkenntnisse, aber auch offenen Fragen kontinuierlich nachverfolgt werden. Diese öffentliche Anhörung des Ausschusses Digitale Agenda ist in dieser Hinsicht sehr zu begrüßen.

6) Welche besonderen Leistungen und Eigenschaften erwarten Sie von Quantencomputern? Welche Aufgaben könnten Quantencomputer erfüllen? Welchen Nutzen können sie generieren? In der Folge: Welche – wissenschaftlichen und ggf. gesellschaftlichen - Herausforderungen und Probleme können mit Quantencomputing gelöst werden?

Die hier gestellten Fragen werden weiter unten gemeinsam mit Frage 7 beantwortet.

7) Welche Anwendungen sind denkbar? Wie belastbar ist die Annahme einer „Quantum Supremacy“ (auch bezogen auf vereinzelte Anwendungsbereiche) im Vergleich zu klassischen (Super-)Computern? Bitte benennen Sie, zur besseren Verständlichkeit, ggf. Beispiele, falls möglich insbesondere in den Bereichen Klima-/Energie-Forschung, Verkehr, Medizin, Industrie 4.0., Verteidigung. Welche Auswirkungen erwarten Sie von Fortschritten auf dem Gebiet des Quantencomputing auf andere Technologiebereiche (Maschinelles Lernen, Künstliche Intelligenz, Blockchain, Supercomputing, Kommunikation, aber auch Autonomes Fahren etc.)?

Die möglichen Anwendungen ergeben sich aus den rechnerischen Problemen, für die effiziente Quantenalgorithmen existieren (siehe hierzu auch die Antwort auf Frage 1). Beispiele sind die Datenbanksuche (Grover-Algorithmus) und die Primfaktorzerlegung (Shor-Algorithmus). Eine große Klasse sind Optimierungsaufgaben. Diese können auch mit einem adiabatischen Quantencomputer effizient bearbeitet werden. So hat etwa Volkswagen mithilfe des D-Wave Quantum-Annealers eine Verkehrsflussoptimierung durchgeführt[8]. Weitere Beispiele sind autonomes Fahren und die Flugroutenoptimierungen, also ganz allgemein Navigation und Logistik, sowie Muster- und Sprachverarbeitung. Bezüglich künstlicher Intelligenz und maschinellen Lernens wird erwartet, dass Quantencomputer eingesetzt werden können, um diese Systeme effizienter zu trainieren. Ein ganz wichtiger Anwendungsbereich ist die Simulation von Quantensystemen. Diese kann nur auf einer Quantenhardware wie einem Quantencomputer effizient erfolgen. Es gibt auch erfolgversprechende Ansätze, dedizierte Quantensimulatoren zu entwickeln, die auf Kosten der Universalität eines Quantencomputers besonders effizient und auch vergleichsweise einfach gezielte Fragestellungen zu quantenphysikalischen Systemen untersuchen. Anwendungsfelder sind in der Physik, der Chemie, der Biologie und Medizin zu finden. Es gibt einige Beispiele mit immenser potentieller Bedeutung für die Menschheit: Medikamentenentwicklung, z. B. über die Simulation von Proteinfaltungen. Entwicklung neuer Materialien, wie Hochtemperatursupraleiter, die Strom verlustfrei über große Distanzen leiten können. Effizientere Syntheseverfahren

[6] Nationale Akademie der Wissenschaften Leopoldina, acatech – Deutsche Akademie der Technikwissenschaften, Union der deutschen Akademien der Wissenschaften (Hrsg) (2015): *Perspektiven der Quantentechnologien*. Halle (Saale), abrufbar unter https://www.leopoldina.org/uploads/tx_leopublication/2015_Quantentechnologien_LF_DE_korr.pdf.

[7] *Förderung von Quantentechnologien*, Positionspapier der Deutschen Industrie, abrufbar unter https://www.photonikforschung.de/media/quantentechnologien/pdf/Quantentechnologie_bf.pdf.

[8] *Verkehrsflussoptimierung mit einem D-Wave Quantum Annealer: Durch Barrieren*, Christian Seidel, Florian Neukart, Gabriele Compostella, iX 2/2018, S. 94 ff.

in der Chemie, zum Beispiel für die energiesparende Synthese von Stickstoffdünger, der für die Ernährung der Weltbevölkerung benötigt wird. Quantentechnologien ermöglichen auch Fortschritte im Bereich der Datensicherheit und Privatsphäre. So gibt es zum Beispiel Protokolle, die eine Quantenberechnung durch eine nicht-vertrauenswürdige Stelle ermöglichen, ohne dass diese Stelle hierdurch Informationen über die Berechnung erlangen könnte (*blind quantum computation*, siehe auch die Antwort auf Frage 15).

Der Nachweis eines Quantenvorteils (*quantum supremacy*) ist immer auch von den klassischen Algorithmen und der klassischen Hardware abhängig, mit denen der Quantencomputer verglichen wird. Insofern ist der Quantenvorteil zwar ein wichtiger, weil sofort einleuchtender Meilenstein der Quantencomputerentwicklung, aber nicht notwendigerweise ein direktes Maß für den möglichen kommerziellen Erfolg von Quantencomputern.

8) Welche (technischen) Herausforderungen bestehen? Welcher Zeitrahmen erscheint realistisch, um diese zu überkommen? Wie können Fehlerrate und Qualität der Qbits verbessert werden? Aktuell werden verschiedene Qbit-Implementierungen erforscht - welche hat, Ihrer Meinung nach, das größte Potenzial?

Aufgrund ihrer im Vergleich zu klassischen Computern geringeren Fehlertoleranz ist die Fehlerkorrektur für Quantencomputer besonders wichtig. Diese beeinflusst zwar den Skalierungsvorteil von Quantencomputern gegenüber klassischen Computern nicht negativ, führt aber trotzdem zu einem großen zusätzlichen Aufwand bezüglich der Anzahl der benötigten Quantenbits und Rechenschritte. So werden beispielsweise viele physikalische Quantenbits benötigt, um ein einzelnes logisches Quantenbit fehlerkorrigiert zu implementieren.

Die Strategien zu Verbesserung von Fehlerrate und Qualität der Quantenbits hängt vom jeweiligen physikalischen System ab. Derzeit am weitesten fortgeschritten ist der Entwicklungsstand bei supraleitenden Systemen auf der Basis von Josephson-Kontakten sowie gefangenen Ionen. Es gibt weitere interessante physikalische Systeme, die als Plattformtechnologie für einen Quantencomputer genutzt werden könnten, darunter Spins in Halbleitern, neutrale Atome, Farbzentren in Diamant und Photonen. Eine besondere Stellung nehmen topologische Quantenbits ein. Sie bieten eine inhärente Fehlertoleranz, sind aber viel schwieriger zu implementieren, weshalb es für ihre Entwicklung noch sehr grundlegender Forschung bedarf. Hier haben die anderen Ansätze einen klaren Entwicklungsvorsprung. Aufgrund der Probleme einer effizienten Fehlerkorrektur könnten sich die derzeit führenden Ansätze jedoch langfristig als schwieriger skalierbar herausstellen.

Jedes System hat seine ganz speziellen Stärken aber eben auch Herausforderungen, die nur über kontinuierliche Forschung weiterentwickelt werden können. Sehr wichtig ist eine fortlaufende Beurteilung der Systeme bezüglich fundamentaler technologischer oder physikalischer Hindernisse, die eine weitere Verbesserung oder Skalierung des Systems verhindern könnten. Exemplarisch seien hierzu die Verluste in optischen Wellenleitern für photonische Systeme genannt. Notwendige Aufgaben für alle Quantenbit-Implementierungen sind die Verlängerung der Kohärenzzeit, die Verbesserung der Qualität (*fidelity*) von Quantenlogikgattern und der Konnektivität. Ganz wichtig sind neue Ansätze für die Skalierbarkeit wie die optische Vernetzung von kleineren Prozessoreinheiten auf Basis von gefangenen Ionen zu einem größeren Quantencomputer. Hierfür ist die Weiterentwicklung von Atom-Photon Schnittstellen essentiell, ein Beispiel für ein nicht inhärent dem Quantencomputing, sondern eher der Quantenkommunikation zugeschriebenes Thema, das trotzdem große Bedeutung für das Quantencomputing bekommen könnte.

Darüber hinaus gibt es viele technologische Herausforderungen, die nicht direkt quantenmechanischer Natur sind. Die Anforderungen an unterstützende Technologie zum Betrieb eines Quantencomputers sind immens und gehen oft über den aktuellen Stand der Technik hinaus. Beispiele sind die Kryostaten für supraleitende Quantenbits, Vakuumtechnologie für gefangene Ionen, Lasersysteme für alle optischen oder optisch kontrollierten Quantenbits sowie allgemein die Kontrollelektronik zum Betrieb eines Quantencomputers. Wenn diese Systeme nicht ebenfalls skaliert werden können, stellt dies ein Hindernis für die Skalierung der zugehörigen Quantentechnologie dar. In jedem Fall wird ein Quantencomputer, der leistungsstark genug ist, um zum Beispiel für Attacken auf kryptographische Verfahren mit typischen Schlüssellängen eingesetzt zu werden, eher einem Großrechenzentrum oder heutigen Supercomputer ähneln als einem Tischgerät oder heutigen Laborgerät. Wenn die zukünftigen Zulieferer nicht bereitstehen oder die notwendige klassische Technik nicht auf die Bedürfnisse der Quantencomputer angepasst werden kann, wird dies die Weiterentwicklung von Quantencomputern verhindern.

9) Welche wirtschaftlichen Chancen können aus Fortschritten im Bereich des Quantencomputing entstehen? In welchen zeitlichen Inkrementen rechnen Sie mit Fortschritten? Wann rechnen Sie mit welchen Formen einer Markteinführung? Welche Entwicklungen veranlassen Sie zu der Annahme, dass Quantencomputer in absehbarer Zeit Marktreife erreichen können oder auch nicht erreichen können?

Fortschritte im Bereich des Quantencomputing können mittelbar andere Quantentechnologien voranbringen, die voraussichtlich sogar früher Marktreife erreichen werden. Als Beispiele seien Quantenkryptographiesysteme, Quantenzufallszahlengeneratoren und Magnetfeldsensoren genannt. Diese Systeme könnten in den nächsten Jahren in größeren Stückzahlen Eingang in den Markt finden. Des Weiteren gibt es eine Vielzahl von Firmen, welche Teilkomponenten anbieten, wie sie für die Entwicklung und den Betrieb eines Quantencomputers benötigt werden. Computersteuerungen, Vakuumtechnik, Radio- und Mikrowellenfrequenztechnik, Messtechnik, Kryostaten, Laser und andere Komponenten aus dem Bereich Photonik sind nur einige Beispiele. Weitere Schlüsseltechnologien werden im Konzeptpapier der Nationalen Initiative zur Förderung der Quantentechnologie von Grundlagen bis Anwendungen (QUTEGA) genannt[9]. Die Anbieter dieser Schlüsseltechnologien (*quantum-enabling technologies*) müssen zunächst stark investieren, um die Bedürfnisse der Quantencomputerhersteller erfüllen zu können. Weil der gesamte Markt noch eher klein ist, und weil er aufgrund der Vielzahl verschiedener technologischer Ansätze auch noch stark fragmentiert ist, müssen hier finanzielle Anreize etwa durch die Übernahme von Entwicklungskosten geschaffen werden. Langfristig werden die Hersteller dieser Schlüsselkomponenten jedoch mit großer Wahrscheinlichkeit von den für Quantencomputer betriebenen Entwicklungen profitieren, als Zulieferer für Quantencomputerhersteller aber auch in anderen Märkten. Im Bereich der Schlüsseltechnologien sind viele kleine und mittlere Unternehmen aktiv. Sowohl Deutschland als auch Europa als Ganzes sind hier gut aufgestellt. Der Umsatzanteil deutscher Firmen an der globalen Labor-Quantentechnologie wird auf 10% geschätzt[7]. Diese wirtschaftliche Chance sollte nicht ungenutzt bleiben.

Schon jetzt gibt es einen Markt für Quantencomputer, der allerdings noch sehr klein ist. Die Kunden nutzen die Möglichkeit, Programme auf einem Quantencomputer laufen zu lassen, um das Potential

[9] *QUANTENTECHNOLOGIE Grundlagen und Anwendungen*, Konzeptpapier der Nationalen Initiative zur Förderung der Quantentechnologie von Grundlagen bis Anwendungen, abrufbar unter http://www.qutega.de/fileadmin/qutega/Qutega_Grundlagenpapier.pdf.

der neuen Technologie zu erkunden, Erfahrung zu sammeln und daraus neue Impulse für die Entwicklung der entsprechenden Software und bezüglich zukünftiger Anwendungsbereiche zu erhalten. Dieser Markt wird in den nächsten Jahren wachsen, insbesondere wenn wirtschaftliche und politische Kräfte überzeugend vermitteln können, dass die mit der Entwicklung eines Quantencomputers verbundenen Herausforderungen angenommen und diese Entwicklung langfristig unterstützt wird. Es ist selbstverständlich, aber trotzdem erwähnenswert, dass es keine Garantie für den kommerziellen Erfolg des Quantencomputers gibt. Dieser wird jedoch umso wahrscheinlicher, je entschlossener die Entwicklung und die Suche nach neuen Applikationen und Algorithmen vorangetrieben werden.

Die Entwicklung von Quantencomputern hat sich in den letzten Jahren stark beschleunigt. Eine Extrapolation ist sehr schwierig, auch aufgrund der großen Unterschiede zwischen den in Frage kommenden Systemen. Derzeit deutet die Kombination aus einem guten Entwicklungsstand, vielen Akteuren und einer gewissen Ähnlichkeit zu derzeitigen integrierten Schaltkreisen auf supraleitende Systeme als vielversprechendsten Ansatz hin. Konkrete Vorhersagen bezüglich Markteinführungen sind aufgrund des multidimensionalen Parameterraums aus der Anzahl logischer und physikalischer Quantenbits, den Kohärenzzeiten, der Fehlerrate und anderen physikalischen Größen nicht zuverlässig möglich. Außerdem können und werden immer noch neue Anwendungen, Algorithmen und Hardware-Plattformen entstehen, und es besteht eine nicht sehr geringe Wahrscheinlichkeit, dass einige disruptiven Charakter haben werden.

10) Wird sich Deutschland als wesentlicher Hersteller von Quantencomputing-Hardware etablieren können, oder sollte Deutschland eher die Entwicklung von Systemanwendungen oder Software fördern? Sind für die Herstellung von Quantencomputer kritische Ressourcen erforderlich (vgl. z. B. Thema „Seltene Erden"), die deutsche Hersteller im außereuropäischen Ausland beschaffen müssten?

Die Entwicklung von Software und Applikationen für Quantencomputer ist sehr wichtig und sollte auch in Deutschland mit mehr Nachdruck betrieben werden (siehe hierzu auch die Antwort auf Frage 13). Quantensoftware verlangt interdisziplinäre Teams und ein tiefgreifendes Wissen über Quantenphysik und Quanteninformation. Gerade im Bereich der Applikationen liegt ein enormes Marktpotential, das ebenfalls in Deutschland genutzt werden sollte. Die Bedeutung der Hardware für die Softwareentwicklung darf jedoch nicht unterschätzt werden, weshalb der Bereich der Quantencomputerhardware nicht ganz anderen Nationen überlassen werden darf. Die verfügbare Hardware wird immer fehlerbehaftet sein und benötigt an diese Imperfektionen angepasste Software. Auch die unterschiedlichen Ansätze des Quantencomputing (adiabatisch, topologisch, Gattermodell) benötigen angepasste Software. Somit ist eine erfolgreiche Softwareentwicklung ohne tiefes Wissen über die konkrete Hardware sehr schwierig oder sogar unmöglich.

Ein weiterer Grund, weshalb Deutschland bezüglich der Entwicklung von Quantencomputing-Hardware aktiv bleiben sollte, ist die enge Verknüpfung mit anderen Quantentechnologien. So werden schon heute Konzepte aus dem Quantencomputing, konkret Quantenlogikgatter, für die Verbesserung hochpräziser optischer Ionen-Uhren eingesetzt. Diese Synergien können nicht genutzt werden, wenn Deutschland sich ausschließlich auf Quantentechnologien fokussiert, bezüglich der man im internationalen Vergleich besonderes stark ist, z. B. die Bereiche Quantensensorik und -metrologie oder Quantenkommunikation. Außerdem ist die Entwicklung von Quantencomputern in Deutschland nicht so weit zurück, dass man das Feld zwingend anderen Nationen überlassen müsste. Insbesondere im Verbund mit unseren europäischen Partnern sind wir in einer ausgezeichneten Position.

11) Welche Art der (öffentlichen) Förderung und welche weiteren Rahmenbedingungen sind aus Ihrer Sicht erforderlich, um diese Technologie voranzubringen? Wie viele Mittel fließen weltweit in die Forschung und Entwicklung von Quantencomputing, welche Länder und welche Firmen investieren am meisten?

Wie schon in der Antwort auf Frage 2 erwähnt, hat McKinsey die Investitionen in nichtgeheime Forschung zu Quantentechnologien für 2015 abgeschätzt[1]. Ein großer Teil des Gesamtvolumens von 1,5 Mrd. € entfällt auf die USA (360 Mio. €), China (220 Mio. €), Deutschland (120 Mio. €), Vereinigtes Königreich (105 Mio. €) und Kanada (100 Mio. €). Auch Australien, die Schweiz und Japan investieren massiv in diesem Bereich. Mit 550 Mio. € werden in der EU inklusive UK mehr als ein Drittel der weltweiten Investitionen in diesem Bereich getätigt. Im Vereinigten Königreich wird schon seit einigen Jahren von staatlicher Seite im Rahmen des *UK national quantum technologies programme* in Quantentechnologien investiert, insgesamt in diesem Programm 270 Mio. £, unter anderem in den mit Quantencomputing befassten Quantum Technology Hub NQIT (Networked Quantum Information Technologies). Auch Singapur und die Niederlande haben früh die Bedeutung der Quantentechnologien erkannt und mit einer staatlichen Förderung begonnen.

Die Europäische Kommission hat mit dem Quantentechnologie-Flaggschiff-Programm eine Förderung über 10 Jahre mit einem Gesamtvolumen von 1 Mrd. € angekündigt und den Vergabeprozess begonnen[10]. Dies ist sowohl bezüglich der Fördersumme als auch aufgrund der Signalwirkung ein ganz wichtiger Beitrag zur Stärkung der Quantentechnologien in Europa. In Deutschland wird diese Forschungsförderung von der nationalen Initiative „Quantentechnologie – Grundlagen und Anwendungen (QUTEGA)“ flankiert[9]. Ziel ist es, den Transfer von Forschungsergebnissen in die Industrie zu fördern. In den USA wurde eine Nationale Quanteninitiative mit 10 Jahren Laufzeit und einem staatlichen Budget von 500 Mio. US$ für die ersten 5 Jahre vorgeschlagen, quasi als Reaktion auf Initiativen wie das europäische Quantentechnologie-Flaggschiff. Es gibt Berichte, China wolle 10 Mrd. US$ investieren und in Hefei werde das weltweit größten Forschungszentrum für Quantentechnologien gebaut[11,12]. Das politische Interesse und die finanzielle Unterstützung der Quantentechnologien in China sind enorm. Seine Stärke im Bereich der Quantenkommunikation hat China mit einem Quantenkryptographie-Netzwerk zwischen Peking und Shanghai und dem Satelliten *Micius*, mit dem schon spektakuläre Experimente zur Quantenkommunikation und Quantenkryptographie durchgeführt wurden, eindrucksvoll unter Beweis gestellt. Dies zeigt die Bedeutung von Quantentechnologien im All. Auch in Europa ist man in diesem Bereich aktiv[13].

---

[10] *https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship.*
Quantum Technologies Flagship Final Report, High-Level Steering Committee, abrufbar unter http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46979.
The European quantum technologies flagship programme, M. Riedel et al., Quantum Sci. Technol. 2, 030501 (2017).
The European Quantum Technologies Roadmap, A. Acin et al., arXiv:1712.03773v2, abrufbar unter https://arxiv.org/ftp/arxiv/papers/1712/1712.03773.pdf.

[11] https://www.lightourfuture.org/getattachment/Home/About-NPI/Resources/NPI-Recommendations-to-HSC-for-National-Quantum-Initiative-062217.pdf,
https://www.lightourfuture.org/getattachment/85484dca-465a-46f4-8c8c-090aeb845d09/FINAL-Action-Plan-for-a-NQI-Apr-3-2018.pdf,
https://www.aip.org/fyi/2018/science-committee-seeks-launch-national-quantum-initiative.

[12] http://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility.

[13] siehe z. B. http://www.qtspace.eu oder *Satellite-Based QKD*, I. Khan et al., Optics & Photonics News 29, 26-33 (2018).

Nicht vergessen werden darf die ganz wichtige Grundförderung der Universitäten sowie der Max-Planck-Institute, die einen wichtigen Teil der Forschung bezüglich Quantencomputern leisten. Insbesondere wird an Universitäten und staatlichen Forschungsinstituten die gesamte wissenschaftliche Breite der Quantentechnologien inklusive ganz wichtiger exotische Ideen und Ansätze verfolgen. Es sollte darauf hingewirkt werden, dass die Forschung international offen bleibt und nicht im Geheimen passiert. Unterbundener wissenschaftlicher Austausch würde zum einen großes Misstrauen ob der Fähigkeiten anderer Länder und einen damit verbundenen Druck bezüglich sicherheitsrelevanter Themen erzeugen, aber auch den weltweiten Fortschritt bei diesem Thema behindern. Nicht zuletzt müssen die Rahmenbedingungen für die Anbieter von Schlüsseltechnologien so gestaltet werden (siehe auch die Antwort auf Frage 9), dass sie mit ihren Produkten die Hersteller der Quantencomputer optimal unterstützen.

12) Welche Forschungsstrategie sollte Deutschland bzw. Europa entwickeln, um international anschlussfähig zu bleiben?

Europa und insbesondere Deutschland sind sehr stark in der Grundlagenforschung. Dies ist eine gute Ausgangsposition für Aufgaben wie die Entwicklung eines Quantencomputers. Es muss wieder eine solide Grundfinanzierung, die übermäßige administrative Belastungen der Forscher vermeidet, sichergestellt werden, wenn Fortschritte mit höchstem Tempo erzielt werden sollen. Eine gute Ausbildung ist essentiell, insbesondere vor dem Hintergrund der Vielzahl an notwendigen Qualifikationen. Es müssen Informatiker und Ingenieure in Themen der Quanteninformationsverarbeitung geschult werden, damit sie das in ihrer Profession vorhandene Wissen auf die Entwicklung und Programmierung von Quantencomputer übertragen und anwenden können. In Deutschland werden im internationalen Vergleich, gemessen an der Höhe der Investitionen und der Anzahl der Publikationen zu wenige Patentanträge im Bereich der Quantentechnologien gestellt[14].

Eine ausschließliche Fokussierung auf das Thema Quantencomputer zu Lasten anderer Quantentechnologien sollte unterbleiben. Erstens, weil Quantencomputer andere Quantentechnologien unterstützend benötigen, beispielsweise Quantennetzwerke für die Vernetzung von Quantencomputern. Zweitens können technologische Entwicklungen und Forschungsergebnisse oft für mehrere Quantentechnologien genutzt werden. Diese Synergien sollte man unbedingt nutzen. Und drittens ist ein kommerzieller Erfolg bei vielen anderen Quantentechnologien deutlich früher zu erwarten als beim Quantencomputer. Über diese wirtschaftlichen Erfolge kann auch eine weitere Entwicklung des Quantencomputers zumindest teilweise refinanziert werden.

Parallel zu einer breiten Grundlagenforschung müssen einzelne Leuchtturmprojekte gefördert werden, wodurch die Bündelung von Ressourcen auf ein wichtiges Zwischenergebnis möglich wird. Diese Leuchtturmprojekte sollten den Übergang der jeweiligen Quantentechnologie von akademischen Gruppen in die Industrie fördern. Neben einer erfolgreichen Kollaboration und einem Transfer von Wissen und Personal muss das Marktpotential der jeweiligen Technologie besonders berücksichtig werden. Idealerweise finden diese Leuchtturmprojekte unter Führung eines oder mehrerer der beteiligten Industriepartner statt, weil dort typischerweise eine viel größere Kompetenz in der Abwicklung größerer Projekte und bezüglich einer marktreifen Entwicklung besteht. Diesen Leuchtturmprojekten sollte eine breitangelegte, mit Fördergeldern finanzierte Marktforschung vorangehen, welche die Be-

[14] *The quantum age: technological opportunities*, Government Office for Science, UK, abrufbar unter https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf.

reiche und Projekte mit dem größten Potential ermittelt. Nicht vergessen werden darf dabei, dass wissenschaftlicher Fortschritt oft ein Ergebnis technologischer Neuerungen ist. Beispielsweise werden Simulationen komplexer Systeme mit leistungsstärkeren Computern besser oder überhaupt erst möglich. So verhält es sich auch bei den Quantentechnologien und speziell beim Quantencomputer. Daher sollte jedes Forschungsprojekt von einem Technologieentwicklungsprojekt begleitet werden, in dessen Rahmen die Zulieferer für einen Quantencomputer oder eine andere Quantentechnologie dabei unterstützt werden, die notwendigen Entwicklungen durchzuführen. Diese Unterstützung kann in Form von Fördergeldern, aber auch über die Schaffung von Märkten, z. B. die Garantie von Abnahmemengen, erfolgen.

Eine nationale und auch internationale Abstimmung der Förderung entlang einer klaren Roadmap ist wichtig, um den Erfolg zu maximieren und Planungssicherheit bei allen Akteuren zu garantieren. Die Entstehung von Ausgründungen und Start-ups ist zu unterstützen, weil dort am ehesten die notwendige Expertise vorhanden ist. Ebenso sind Maßnahmen wünschenswert, die in Deutschland ein größeres Interesse von Venture Capital Firmen am Quantencomputing generieren.

13) Ist die Nutzung der QC-Hardware abhängig von einer neuen Art Software? Falls ja, ist die Forschung und Weiterbildung daran in Deutschland auf internationalem Niveau oder wie müsste nachgebessert werden?

Die Entwicklung von Software für Quantencomputer ist ein wichtiges Thema. Die hierfür notwendigen Konzepte werden im Informatikstudium so noch nicht gelehrt. Wie in der Frage zurecht vermutet wird, ist eine neue Art Software notwendig. Vor allem Start-ups in den USA bieten Beratungstätigkeit in diesem Bereich an und entwickeln Softwarepakete wie Compiler und höhere Programmiersprachen. Zur Ausbildung, für die Forschung und für die Entwicklung neuer Algorithmen sind Quantencomputersimulationen, die auf klassischen Computern laufen, sehr wichtig. IBM, Microsoft, Rigetti, Intel und das französische Unternehmen Atos haben hier schon Systeme entwickelt, welche die Simulation von universellen Quantencomputern mit bis zu etwa 50 Quantenbits ermöglichen. Derartige Systeme sollten auch in Deutschland entwickelt und eingesetzt werden.

In einem Positionspapier der Deutschen Industrie wird darauf hingewiesen, dass „das Hauptaugenmerk der akademischen Community in Europa auf der Hardware-Entwicklung zu liegen [scheint]“[7]. Dort wird zurecht die Entwicklung eines leistungsfähigen Softwarestacks parallel zur Hardware und eine Stärkung der Anwendungsseite gefordert. Hier ist ein großes Profitpotential zu erwarten. Neugründungen wie Rigetti Computing tragen der großen Bedeutung von sowohl Hard- als auch Software Rechnung, indem sie trotz des insbesondere für ein Start-up immensen Aufwands in beiden Bereichen aktiv sind. Viele andere neue Firmen, vor allem in den USA, sind auf die Softwareentwicklung für Quantencomputer spezialisiert[15]. Solche Neugründungen sind auch für Deutschland wünschenswert und sollten dementsprechend unterstützt werden.

14) Ab wann werden heute angewendete Verschlüsselungsalgorithmen und Instrumente aus dem Bereich der IT-Sicherheit (z.B. Verschlüsselungstechnologien, Blockchain-Technologien) voraussichtlich unsicher? Bitte schlüsseln Sie die angenommenen zeitlichen Horizonte für möglichst viele Verschlüsselungsalgorithmen und Instrumente einzeln auf. Warum werden die benannten Verschlüsselungsalgorithmen und Instrumente unsicher? Wie kann sichergestellt werden, dass wir rechtzeitig darauf vorbereitet sind

[15] siehe z. B. die Liste unter https://quantumcomputingreport.com/players/privatestartup/.

Aktuell verwendete Verschlüsselungsalgorithmen basieren darauf, dass es ein für klassische Computer „schweres" Problem ist, sie zu brechen. Ein Beispiel ist die bei der RSA-Methode verwendete Primfaktorenzerlegung oder die Berechnung diskreter Logarithmen. „Schwer" bedeutet in diesem Kontext, dass die Rechenzeit exponentiell mit der Schlüssellänge zunimmt. Ein Quantenalgorithmus kann eine solche Aufgabe „leicht" lösen, d.h. der Aufwand nimmt mit der Schlüssellänge nicht mehr exponentiell zu. Wie schon in der Antwort auf Frage 5 erwähnt, ist allein die Möglichkeit eines leistungsstarken Quantencomputers eine Bedrohung für das dauerhafte Bewahren aktueller Geheimnisse. Derzeit sicher verschlüsselte Nachrichten könnten von Angreifern zwischengespeichert und dann mit zukünftigen Quantencomputern nachträglich entschlüsselt werden. Solange keine Gewissheit über den zum Teil geheimen Forschungsstand anderer Länder existiert, muss der schlimmste Fall angenommen werden, nämlich dass ein solcher Quantencomputer schon existiert, auch wenn dies auf Basis des derzeitigen Stands der frei zugänglichen Forschung sehr unwahrscheinlich erscheint.

Einen möglichen Ausweg bietet neben den Ansätzen der Post-Quanten-Kryptographie interessanterweise die Quantenkryptographie. Sie nutzt dieselben physikalischen Phänomene wie Superposition und Verschränkung, die auch einem Quantencomputer zugrunde liegen, ermöglicht jedoch unter anderem den absolut abhörsicheren Schlüsselaustausch. Diese Technologie muss unbedingt gefördert und weiterentwickelt werden, um weite Verbreitung zu finden. Weitere Aspekte werden in der Antwort auf die nachfolgende Frage 15 diskutiert.

Die Autoren einer Studie[2] im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) haben berechnet, wie viele Elementarschritte und Quantenbits in Abhängigkeit von der Fehlerrate und der Schlüssellänge für einen Angriff auf derzeit genutzte Kryptographieverfahren benötigt werden. „Wenn … Forschungsanstrengungen auf dieses Ziel konzentrieren würde[n], ähnlich den Manhattan- und Apollo-Projekten des 20. Jahrhunderts, so erscheint ein Quantencomputer mit wenigen Millionen physikalischer Qubits, der zumindest in 100 Tagen 2048-Bit RSA brechen kann, erreichbar, wenn auch die physikalische Fehlerrate angemessen sinkt…"[16].

15) Was wird für die Weiterentwicklung von Quantenkryptografie benötigt? Wie können alle notwendigen Fachgebiete in der Wissenschaft bei der Weiterentwicklung von Quantenkryptografie eingebunden werden? Wie können die Entwicklungen der Quantenkryptografie breit zugänglich gemacht werden in Industrie, Ausbildung und für die End User? Wie kann Quantentechnologie auch kleinen Start-ups oder Einzelpersonen zugänglich gemacht werden, um Anwendungen zu entwickeln? Gibt es mögliche Implikationen für den Datenschutz, wenn Quantenkryptografie weit verbreitet ist?

Die Quantenkryptographie erlaubt den sicheren Schlüsselaustausch. Sie löst nicht das Problem der Authentifizierung, ist sonst aber gegen beliebig mächtige Angreifer sicher. Sie beruht auf der Gültigkeit der Gesetze der Quantenmechanik. Konkrete Implementierungen können attackiert werden, indem Schwachstellen der verwendeten Komponenten (z. B. von Photodetektoren) ausgenutzt werden. Dieses potentielle Problem löst das Verfahren des geräteunabhängigen Quantenschlüsselaustauschs (*device-independent QKD*). Gegen ein Unterbinden der Kommunikation durch einen Angreifer ist natürlich auch die Quantenkryptographie nicht gefeit.

Für Distanzen von deutlich mehr als 100 km sind bisherige Quantenkryptographiesysteme aufgrund der Absorption in Glasfasern nicht geeignet; es kommt irgendwann schlicht nichts mehr am anderen

[16] *Studie Entwicklungsstand Quantencomputer (Zusammenfassung in deutscher Sprache)*, Frank K. Wilhelm et al., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Zusammenfassung.pdf?__blob=publicationFile&v=4.

Ende an. Der Einsatz von optischen Verstärkern wie in herkömmlichen Fasernetzwerken ist nicht möglich, weil Quanteninformation prinzipiell nicht kopiert werden kann, ohne sie dabei zu verändern. Daher ist der Einsatz sogenannter Quantenrepeater notwendig. In Deutschland forscht ein breit aufgestelltes Konsortium von Wissenschaftlern zu diesem Thema und wird seit mittlerweile 7 Jahren vom BMBF gefördert. Noch ist kein Quantenrepeater experimentell demonstriert worden, aber es gibt große Fortschritte. Für Erfolge auf diesem Gebiet werden insbesondere bessere Quantenspeicher benötigt. Quantennetzwerke sind bei weitem nicht auf die Quantenkryptographie als einzige Anwendung beschränkt. So gibt es zum Beispiel Protokolle, die es ermöglichen, eine Quantenberechnung an eine nichtvertrauenswürdige Stelle zu vergeben, ohne dass diese dadurch Informationen über die Berechnung erlangen könnte (*blind quantum computation*). Solche Anwendungen, die sich an Schnittstellen unterschiedlicher Quantentechnologien ergeben, sollten genutzt und weiter erforscht werden.

Quantenkryptographie schützt nur die Kommunikation derjenigen, denen sie zur Verfügung steht. Als Konsequenz dieser zunächst trivialen Aussage müssen Rahmenbedingungen geschaffen werden, so dass diese Technologie allen Bürgern und Unternehmen zur Verfügung steht. Insbesondere in Bezug auf die Quantenkryptographie hat der Staat die große Chance, durch den Kauf oder die Beauftragung von Quantenkryptographiesystemen seinen Institutionen und Bürgern Dienste anzubieten, die einen fundamental sicheren Austausch sensibler Informationen ermöglichen. Er würde damit ein Zeichen für die Bedeutung des Datenschutzes setzen und somit möglicherweise einem fehlenden Bewusstsein in der Industrie entgegentreten. Hier kann der Staat eine Vorreiterrolle einnehmen. Gleichzeitig würde durch eine frühe staatliche Nachfrage nach Quantenkryptographiesystemen ein Markt geschaffen, der die Weiterentwicklung dieser Technologien fördert, Kosten senkt und damit auf längere Sicht die Verfügbarkeit dieser Technologie auch für Start-ups und Einzelpersonen ermöglicht.