Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)14

Stellungnahme zum Thema Quantencomputing

für die Anhörung im Ausschuss Digitale Agenda des Deutschen Bundestags am 6.6.2018

Prof. Hendrik Bluhm

RWTH Aachen und Forschungszentrum Jülich

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

Viele Wissenschaftler glauben, dass Quantencomputing ein grundlegend neuartiges Paradigma für die Informationsverarbeitung darstellt, das die Lösbarkeit mancher Rechenprobleme revolutionieren wird. Nach ca. 20 Jahren Grundlagenforschung hat das Feld die Schwelle zur gezielten Technologieentwicklung überschritten.

Theoretische Arbeiten haben zu einer klaren Vorstellung geführt, unter welchen Bedingungen eine praktische Nutzung von Quantencomputing möglich sein sollte. Mehrere Ansätze zur Realisierung von Quantencomputern haben diese Bedingungen auf Ebene einzelner Bauteile experimentell erfüllt oder lassen dies in den nächsten Jahren erwarten. Die große Herausforderung ist nun, Systeme mit letztendlich Millionen oder gar Milliarden von quantenmechanischen Speicherelementen, sogenannten Qubits, zu realisieren. Erste Versuche mit einigen zehn Qubits zeigen, dass es nicht trivial ist, dabei die gewünschten Charakteristiken einzelner Qubits zu erhalten. Dieses Problem ist vermutlich lösbar, braucht aber Zeit.

Das Anwendungspotential der in den nächsten Jahren zu erwartenden, relativ kleinen Systeme ist noch recht wenig erforscht. Erste Ergebnisse deuten darauf hin, dass dafür eine deutlich höhere Genauigkeit als bisher erzielt notwendig ist.

Für die Realisierung von signifikant größeren Systemen gibt es Konzeptüberlegungen, die jedoch noch keinen hohen Reifegrad erreicht haben. Einige Punkte könnten möglicherweise zu fundamentalen Hürden führen, viele Wissenschaftler halten diese Probleme jedoch für überwindbar. Es ist momentan unklar, welcher der führenden Ansätze der geeignetste ist.

Erste Kommerzialisierungsversuche insbesondere in den USA erlangen eine hohe Sichtbarkeit in der Presse und werden von der Wissenschaft aufmerksam verfolgt, zeigen aber noch keinen praktischen Nutzen.

Zusammenfassend verspricht Quantencomputing einen erheblichen gesellschaftlichen und wirtschaftlichen Nutzen, erfordert aber noch einen hohen Entwicklungsaufwand und ist mit beträchtlichen Unabwägbarkeiten behaftet.

Für eine detailliertere Einschätzung sind zwei Parameter besonders wichtig: die Anzahl der in Quantencomputern gekoppelten Qubits und die Genauigkeit ihrer Manipulation, die durch eine Fehlerrate quantifiziert werden kann. Es ist relativ gut verstanden, wie sich mit einer Fehlerrate von etwa 1/1.000 und vielen Millionen von Qubits eine relativ große Klasse von Anwendungen erschließen lässt. Speziellere Anwendungen, die mit etwa 100 bis 1000 Qubits auskommen, werden derzeit intensiv untersucht. Es zeichnet sich ab, dass dabei Fehlerraten im Bereich von maximal 1/10.000 bis 1/1.000.000 toleriert werden können.

Die Manipulation einzelner Qubits hat bei den drei unten näher beschriebenen führenden Ansätzen eine Fehlerrate unter 1/1.000 erreicht. Für Rechenoperationen mit mehreren Qubits wurden Werte unter 1/100 erreicht oder sind absehbar.

Derzeitige Demonstratorsysteme für unumstritten „echte“ Quantencomputer auf Basis supraleitender Qubits weisen bis zu 72 Qubits auf, jedoch hat sich gezeigt, dass die Fehlerrate mit zunehmender Anzahl Qubits deutlich zunimmt und derzeit nicht reproduzierbar unter 1/10 liegt. Dementsprechend müssten sie um mindestens zwei Größenordnungen verbessert werden. Die Expertenmeinungen, wie leicht und in wieweit sich diese Werte mit dem derzeit verfolgten Ansatz verbessern lassen, divergieren.

Ich teile den Optimismus vieler Kollegen, dass auch diese Werte in den nächsten Jahren den anwendungsrelevanten Bereich erreichen werden. Dieser Optimismus beruht nicht zuletzt

darauf, dass sich die Kohärenzzeiten (d.h. Lebensdauer der gespeicherten Zustände) und damit die Fehlerraten ähnlich dem bekannten Moorschen Gesetz exponentiell verbessert haben und kein Grund zu der Annahme besteht, dass eine fundamentale Grenze erreicht ist. Jedoch ist noch nicht verlässlich einzuschätzen, welcher Ansatz langfristig am vielversprechendsten ist. Insbesondere der Schritt über ca. 1000 Qubits hinaus wird Lösungen erfordern, die bisher nur ansatzweise untersucht wurden. Dazu gehören z.B. hochintegrierte Kontrollsysteme, die bei den für Festkörperqubits erforderlichen Temperaturen nahe dem absoluten Nullpunkt mit geringster Leistungsaufnahme funktionieren.

Eine Sonderstellung nehmen die bereits kommerziell verfügbaren Systeme von D-Wave ein, die derzeit aus 2000 qubitartigen Bauelementen bestehen, aber architekturbedingt weniger potent sind als echte Quantencomputer. Fehlerraten im obigen Sinne sind hier nicht direkt relevant oder untersucht, man kann zum Zwecke der Einordnung jedoch von Werten um 1/10 ausgehen.

Dem Stand der Hardwareentwicklung ist der Reifegrad der avisierten Anwendungen gegenüberzustellen. Einige mögliche Anwendungen für Quantencomputer sind relativ gut verstanden und die Voraussetzungen dafür recht detailliert analysiert, wenngleich einige vereinfachende Annahmen für tatsächliche Implementierungen noch verfeinert werden müssen. Beispiele dafür sind die für die Kryptologie relevante Primfaktorzerlegung sowie die Simulation mittelgroßer Moleküle. Andere mögliche Anwendungsbereiche, wie z.B. maschinelles Lernen oder Medikamentenentwicklung, sind dagegen weniger konkret ausgearbeitet. Ich gehe davon aus, dass einerseits viele wichtige zukünftige Anwendungsmöglichkeiten noch nicht identifiziert wurden, andererseits nicht alle derzeitig kursierenden Versprechungen realistisch sind.

Für eine weiterführende Diskussion mit konkreten Beispielen sei auf Fragen 6 – 9 verwiesen

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?

Die in Deutschland und Europa vorhandene wissenschaftliche Kompetenz liegt auf international uneingeschränkt konkurrenzfähigem Niveau. Zu den weltweit sichtbarsten Gruppen zählen z.B. die der ETH Zürich, Uni Innsbruck, TU Delft und Chalmers. In Deutschland wurde die Fokussierung auf Quantencomputing bisher durch das Fehlen einschlägiger Förderprogramme beeinträchtigt, jedoch haben gerade jüngere Arbeitsgruppen die notwendige Kompetenz und Einsatzbereitschaft – die eingeladenen Experten sind dafür repräsentativ. Auch die jüngsten Entwicklungen der Förderlandschaft sind mit dem einschlägigen EU Flagship und dem angekündigten Programm der Bundesregierung sehr vielversprechend. Wichtig ist nun eine zielführende Umsetzung.

Im akademischen Bereich sind die verschiedenen Quantencomputing-Technologien auf kontinentaler und nationaler Skala im Allgemeinen etwa gleich stark vertreten. In Deutschland sind Ansätze zur Quantensimulation, d.h. dem Nachbau interessanter Modelle durch gut kontrollierbare physikalische Modelle, sehr gut aufgestellt. Dabei handelt es sich jedoch nicht um Quantencomputing im eigentlichen Sinne, und der absehbare Nutzen ist eher wissenschaftlicher als wirtschaftlicher Natur.

In der Technologieentwicklung und der Erprobung von Geschäftsmodellen sind derzeit IBM, Google, und Rigetti, ein kalifornisches Startup mit massiver Venture Captial Unterstützung, führend. Intel und Microsoft verfolgen ebenfalls ehrgeizige Programme. Hinzu kommen diverse kleinere Startups, z.B. im Bereich Consulting und Anwendungsentwicklung. In Deutschland wären intensivere Aktivitäten grundsätzlich wünschenswert. Allerdings ist anzumerken, dass Quantencomputing gerade in den USA gehyped wird und die genannten Programme der Großkonzerne mindestens so sehr als Marketingmaßnahme und früher strategischer Einstieg wie als gezielte Produktentwicklung zu betrachten sind.

China hat ehrgeizige Programme angekündigt. Derzeit ist für mich jedoch insgesamt kein technologischer Vorsprung im Bereich Quantencomputing erkennbar. Im Bereich Quantenkommunikation besteht dagegen ein investitionsintensives Demonstrationsprojekt.

Eine internationale Zusammenarbeit ist in zweierlei Hinsicht unerlässlich. Zum einen erfordert ein Kompetenzaufbau in der Entwicklung von Quantensoftware Zugang zu den weltweit am weitesten vorangeschrittenen Demonstratorsystemen, wobei die dafür entstehenden Kosten sorgfältig gegen deren Entwicklungsstand abgewogen werden müssen.

Mit Bezug auf Hardwareentwicklung ist insbesondere eine enge Zusammenarbeit auf europäischer Ebene notwendig, um eine kritische Masse zu bilden und bestehende Kompetenz optimal zu nutzen. So bieten Institutionen wie z.B. IMEC in Leuven weltweit einmalige Möglichkeiten. Das QT Flagship der EU schafft dafür eine solide Grundlage. Durch geschicktes Vorgehen auf nationaler Ebene sehe ich durchaus die Möglichkeit, eine führende Rolle in Europa zu spielen und so längerfristig auch die in Europa vorhandene Expertise für die deutsche Industrie zugänglich zu machen. Dazu gehören z.B.

- Die Unterstützung von Infrastrukturen, welche der gesamten Europäischen Forschung zu Gute kommen und dabei Know-How auf deutschem Boden binden. Eines der beantragten Flaghip-Projekte ist dafür ein gutes Beispiel, weitere könnten folgen.
- Die Ermöglichung von Unteraufträgen an bestimmte andere europäische Forschungseinrichtungen mit Schlüsselfunktionen (wie z.B. IMEC), um deren Kompetenz gezielt einbinden zu können.
- Eine enge Koordination des nationalen Forschungsprogramms mit dem EU Flagship, um Synergien möglichst gut nutzen zu können.

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)?

Eine Herausforderung (aber möglicherweise auch Chance in der Terrorismusabwehr) ist sicher dadurch gegeben, dass derzeit gängige asymmetrische Verschlüsselungsverfahren unsicher werden. Dafür gibt es geeignete technische Lösungen, die jedoch einen höheren Aufwand und Umstellungskosten mit sich bringen. Dem gegenüber steht das Potential, das Quantenkryptographie (wie heute implementiert oder zukünftig in Verbindung mit kleinen Quantencomputern) zu einer höheren Kommunikationssicherheit führt. In der Einschätzung dieses Potentials bestehen noch relativ viele offene Fragen technischer und soziologischer Natur.

Ein universeller Ersatz für derzeitige Rechner ist auf Basis der bekannten Anwendungsbereiche nicht zu erwarten, so dass Quantencomputing nicht als Lösung für den Energieverbrauch der

IT-Technologie zu betrachten ist. Eher könnte Quantencomputing-Forschung durch Spin-offs auch zu energieeffizienteren klassischen Computern führen.

Zu den möglichen Anwendungen von Quantencomputern zählen Optimierungsprobleme und die Simulation von chemischen Verfahren. Beide können zur ressourcenschonenderen Produktion und Logistik beitragen. Nach heutigem Stand der Forschung ist eher zu erwarten, dass der Einfluss auf das tägliche Leben indirekt sein wird, wie eben durch die Verwendung zur Entwicklung neuer Technologien, als das Privatpersonen direkt mit Quantencomputern interagieren.

Insgesamt würde ich die Abwägung zwischen Chancen und Herausforderungen ähnlich wie bei der klassischen Informationsverarbeitung einschätzen, wobei die absehbare Anwendbarkeit von Quantencomputing deutlich weniger universell ist als die derzeitige digitale Revolution.

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“?

Momentan sehe ich keinen akuten regulatorischen Handlungsbedarf, wobei die Fachcommunity vermutlich nicht optimal positioniert ist, um z.B. „Dual Use“ Gefahren einzuschätzen. Eine Beobachtung des Fortschritts durch entsprechende Experten ist sicher sinnvoll. Etablierte Praktiken aus dem klassischen Supercomputing können vermutlich weitgehend übertragen werden.

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

Derartige Projekte sind mir nicht bekannt, wenngleich sich die NSA und ähnliche Organisationen sicher fundierte Gedanken zu bestimmten Anwendungen gemacht haben. Ansonsten kommt dem vielleicht eine Analyse des Marktpotentials von McKinsey (siehe Anhang) am nächsten.

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?

Es ist nicht zu erwarten, dass Quantencomputer einen universellen Ersatz von herkömmlichen Computern darstellen werden. Vielmehr gibt es eine überschaubare Anzahl von derzeit identifizierten Anwendungen, die teilweise jedoch von hoher Bedeutung sind. Dazu zählen insbesondere:

- Die Entschlüsselung von RSA und ähnlichen Verschlüsselungsverfahren.

- Die verbesserte Simulation von Katalysatoren und chemischen Reaktionen, wodurch sich bessere Verfahren für die Chemieindustrie ergeben könnten. Mögliche Anwendungen mit hoher wirtschaftlicher und gesellschaftlicher Relevanz sind z.B. CO_2-Bindung zwecks Reduzierung der Erderwärmung und Stickstoffbindung zur Düngemittelproduktion.

- Simulationen von Materialien wie Hochtemperatursupraleitern, für deren Eigenschaften Quanteneffekte eine große Rolle spielen. Praktischer Nutzen könnte hier z.B. durch

verlustarmen Energietransport über lange Distanzen entstehen, was einen Beitrag zur Energiewende liefern würde. Diese Perspektive ist langfristiger Natur und mit recht hoher Unsicherheit behaftet, da sie nicht nur von der Leistungsfähigkeit von Quantencomputern, sondern auch von den damit ermöglichten Entdeckungen neuer Materialien abhängt.

- Simulation von wissenschaftlich interessanten Quantensystemen, z.B. zur Lösung von Problemen aus der Elementarteilchenphysik.

- Simulationen zur Medikamentenentwicklung.

- Effizientere Lösung von bestimmten Optimierungsproblemen, z.B. für Produktion, Logistik und Verkehr. Hier könnten sich bedeutende, wettbewerbsrelevante Effizienzgewinne für in Deutschland wichtige Industriezweige ergeben, z.B. im Kontext von Industrie 4.0.

- Unter Umständen die effizientere Lösung von linearen Gleichungssystemen und effizienteres Trainieren von neuronalen Netzwerken, jedoch mit offenen Fragen zur Praktikabilität.

Die Nachrichtenentschlüsselung sowie Simulation von Molekülen gehören zu den Anwendungen, deren Anforderungen am besten untersucht sind und damit am konkretesten absehbar sind, wobei bereits hier Probleme recht bescheidener Größe (z.B. Moleküle mit einer Handvoll Atomen) bei Verwendung bekannter Algorithmen atemberaubende Qubitzahlen in der Größenordnung von einer Milliarde erfordern. Die meisten anderen Anwendungen sind mit noch größeren Unsicherheiten behaftet.

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.)?

Für Anwendungsbeispiele siehe auch Antwort auf Frage 6.

Das Konzept einer Quantum-Supremacy oder auch eines Quanten-Vorteils ist gemäß unserem derzeitigen theoretischen Verständnis grundsätzlich korrekt, kommt aber nur für bestimmte Probleme zum Tragen. Die heute absehbare Nutzung von Quantencomputern wird eher der von Supercomputern als von PCs ähneln.

Auswirkungen auf maschinelles Lernen, künstliche Intelligenz und autonomes Fahren sind noch schwer abzuschätzen. Es gibt konkrete Ideen, wie Quantencomputer das Trainieren bestimmter Arten von neuronalen Netzen, einem in den genannten Bereichen weit verbreiteter Ansatz, effizienter machen könnten. Jedoch bestehen noch offene Fragen bezüglich deren Praktikabilität.

Zusammenfassend ist eine Reihe von Anwendungen mit hoher wirtschaftlicher und gesellschaftlicher Relevanz konkret vorstellbar. Für viele besteht jedoch noch eine beträchtliche Unsicherheit bezüglich Umsetzbarkeit und Anforderungen an die entsprechende Hardware, so dass sich manche dieser Anwendungen als nicht machbar erweisen könnten oder erst in mehreren Jahrzehnten realisierbar sind. Andererseits sind deutliche Erleichterungen durch Optimierung der Algorithmen und neue Ideen zu erhoffen.

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?

Die verschiedenen Ansätze stehen zum Teil unterschiedlichen Schwierigkeiten und offenen Fragen gegenüber. Die wichtigsten sind:

Halbleiterqubits:

- Demonstration von Operationen mit mehreren Qubits mit hoher Genauigkeit. Dies ist in den nächsten 1-2 Jahren zu erwarten.

- Lösung zur Kopplung von Qubits über hinreichend große Distanzen, um komplexe Schaltkreise realisieren zu können – Erkenntnisse in ca. 3 Jahren zu erwarten.

- Automatisierung der Kalibration – im Vergleich zu anderen Ansätzen ist diese relativ schwierig und erfordert derzeit menschliche Intervention. Dies ist vermutlich kein grundlegendes Problem, einzelne Lösungen existieren bereits.

Supraleitende Qubits:

- Präzise Kontrolle von Schaltkreisen mit vielen Qubits. Unerwünschte Kopplungen und Übersprechen sind derzeit ein Problem, dessen Bedeutung schwer einzuschätzen ist. Schlimmstenfalls müssten andere Qubitvarianten verwendet werden, was den derzeitigen Vorsprung zu Nichte machen könnte.

Ionenfallen:

- Die laserbasierte Kontrolle und Auslese bringt eine sehr hohe Systemkomplexität und schlechte Integrierbarkeit mit sich. Skalierungskonzepte erscheinen sehr aufwändig, da viel Hardware involviert.

Alle Qubitarten:

- Kontrolle von Systemen mit mehr als 100 - 1000 Qubits, da externe Kontrollsysteme wie bisher verwendet aufgrund der hohen Verdrahtungsdichte dann an ihre Grenzen stoßen. Deren Realisierbarkeit, Kosten oder Eigenschaften können auch die Wahl des Qubitsystems beeinflussen. Erste Demonstratoren sind in den nächsten fünf Jahren denkbar, das volle Potential wird sich jedoch erst deutlich später ausschöpfen lassen.

- Verbesserung der Material- und Herstellungsqualität zwecks Reduzierung der Fehlerrate und Verbesserung der Reproduzierbarkeit.

Supraleitende Qubits und Ionenfallen sind derzeit etwa gleich weit entwickelt. Halbleiterqubits liegen größtenteils historisch bedingt ca. 5 Jahre zurück, haben aber möglicherweise entscheidende Vorteile bei der Hochskalierung zu sehr großen Qubitzahlen. Sie sind am direktesten kompatibel mit Halbleitertechnologie, insgesamt robuster gegenüber Störeinflüssen als supraleitende Qubits, und können diverse Schwierigkeiten bei der Realisierung hochintegrierter Kontrollysteme vermeiden.

Aus wissenschaftlicher Sicht halte ich es für empfehlenswert, zunächst alle drei Ansätze weiterzuverfolgen, und ggf. später Prioritäten zu setzen. Dabei kann auch die Plausibilität eines Technologietransfers, der nennenswert zu wirtschaftlichen Aktivitäten in Deutschland beitragen kann, als Kriterium herangezogen werden. Sollte eine Prioritätensetzung notwendig oder

gewünscht sein, halte ich Ionenfallen aufgrund der angesprochenen Skalierungsproblematik am ehesten für verzichtbar.

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?

Die wirtschaftlichen Chancen ergeben sich direkt aus den möglichen Anwendungen. Erste spezielle Anwendungen sind in den nächsten fünf Jahren durch Nutzung relativ kleiner Systeme (bis zu etwa 1000 Qubits) denkbar. Die wichtigste Voraussetzung dafür ist die Reduzierung der Fehlerrate, welche sich historisch rasant entwickelt hat. Für die meisten und mächtigsten Anwendungen sind jedoch voraussichtlich deutlich größere Systeme notwendig, für die ein Entwicklungshorizont von zehn Jahren optimistisch erscheint. Unabhängig davon, wann erste Anwendungen möglich sind, erwarte ich eine Weiterentwicklung über mehrere Jahrzehnte.

Grundsätzlich werden erste Schritte zur Markteinführung bereits gemacht, insbesondere von D-Wave und durch Cloud-Zugang zu den Demonstratorsystemen von IBM. Diese lassen jedoch noch keinen praktischen Nutzen über die Erforschung ihrer Fähigkeiten hinaus erkennen.

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?

Dies hängt stark davon ab, inwieweit deutsche Firmen einschlägige Aktivitäten entwickeln. Infineon und Global Foundries haben z.B. für Halbleiterqubits hochrelevante Kompetenz, verfolgen derzeit jedoch primär eine eher kurzfristige, auf Massenmärkte ausgerichtete Strategie. Grundsätzliches Interesse und Dialogbereitschaft sind jedoch vorhanden. Ähnlich verhält es sich mit anderen europäischen Firmen. Weiterhin wird eine Rolle spielen, welche Qubit-Technologie am erfolgreichsten sein wird. Halbleiterqubits sind wohl am stärksten von bestehender Großindustrie abhängig.

Selbst ohne eine komplette Chipproduktion in Deutschland könnte ich mir gut vorstellen, dass z.B. mit Design und Systementwicklung ein nennenswerter Anteil der Wertschätzungskette in Deutschland angesiedelt werden könnte. Ähnliche Geschäftsmodelle funktionieren auch in der Halbleiterindustrie.

Softwareforschung und die Entwicklung von Anwendungskompetenz für Quantencomputer sollte auf jeden Fall gefördert werden. In der deutschen Industrie besteht starkes Interesse an Anwendungsmöglichkeiten (z.B. Verfahrenstechnik, Pharmazeutik, Optimierung von Produktion und Logistik). Zukünftige Quantencomputer gar nicht nutzen zu können, wäre viel fataler, als sie aus anderen Ländern erwerben zu müssen.

Meiner Meinung nach sollte auch die Hardwareentwicklung aus strategischen Gründen unabhängig davon im europäischen Verbund vorangetrieben werden. Airbus ist ein erfolgreiches Beispiel dafür. Im Bereich Hochleistungsrechnen entwickelt sich gerade im Rahmen des „EuroHPC Joint Undertaking“ eine europäische Antwort auf die Dominanz amerikanischer Firmen. Es erscheint sinnvoller, von vorne herein am Ball zu bleibe, statt später nachzubessern.

Rohstoffengpässe sind nicht absehbar. Allenfalls könnte man an isotopenreines Silizium denken, das für hochperformante siliziumbasierte Halbleiterqubits benötigt wird. Die dazu notwendige Technik ist ähnlich der zur Anreicherung von Uran, jedoch tritt keine Radioaktivität auf. Es zeichnet sich hier eine europäische Versorgungskette über Urenco und Air Liquide ab, die allerdings maßgeblich von Intel initiiert wurde.

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?

Für am wichtigsten halte ich ein gezieltes Förderprogramm, das insbesondere für den Übergang von der Grundlagenforschung zur Technologieentwicklung und Transfer an die Industrie eine langfristige Perspektive und kritische Masse schafft. Bislang fehlte ein solches, jedoch ist das EU QT Flagship ein gutes Beispiel und die Signale von BMBF und Projektträgern deuten darauf hin, dass Deutschland auf dem richtigen Weg ist, wenn auch nicht gerade eine Vorreiterrolle einnimmt. In der Umsetzung ist auf die richtige Balance zwischen strategischer Fokussierung und Offenheit für neue Ideen zur Lösung spezifischer Herausforderungen zu achten. Beides ist langfristig wichtig und kann dazu beitragen, die Community zusammenzuführen. Weiterhin halte ich es für zielführend, bei der Projektgestaltung und im strategischem Projektmanagement nicht nur auf Selbstorganisation der Fachcommunity zu setzen, sondern ausgewiesene, möglichst unabhängige Experten (z.B. emeritierte Wissenschaftler und Industrievertreter) kontinuierlich und intensiv in die Koordination einzubinden. Auch diese Gedanken decken sich mit Verlautbarungen des BMBF.

Um dem Nachwuchs klare Perspektiven zu bieten und den Kompetenzaufbau zu fördern, liegt eine Weiterführung des Quantum Futur Programms nahe, wobei neben der wissenschaftlichen Exzellenz ggf. auch strategische Aspekte stärker berücksichtigt werden könnten.

Darüber hinaus ist es wünschenswert, zusätzliche Anreize für industrielle Forschung und Entwicklung zu setzen. Ein auf europäischer Ebene verankertes legislatorisches Hindernis ist dabei, dass Industriebeiträge zu Forschungsprojekten grundsätzlich einen Eigenanteil von 25 % - 50 % liefern müssen. Dies ist nicht zuträglich, Firmen zu einem frühzeitigen Engagement in risikoreichen Technologien wie Quantencomputing zu bewegen. In den USA dagegen ist es nicht ungewöhnlich, dass Forschungsprojekte von Firmen mit Vollkosten gefördert werden. Die Aktivitäten von IBM sind zum Beispiel direkt aus einer solchen Förderung entstanden.

Zu guter Letzt möchte ich noch die Förderung von Hochrisiko-Startups empfehlen. Zwar gibt es gute Förderprogramme für Existenzgründer, diese erfordern meines Wissens jedoch konkrete und kurzfristig umsetzbare Geschäftsmodelle. Natürlich spielt auch die Verfügbarkeit von privatem Risikokapital eine Rolle. Vielleicht besteht auch Spielraum für steuerliche Anreize.

Als Anhaltspunkt für den Umfang der Forschungsförderung in anderen Ländern kann die im Anhang umrissene Studie von McKinsey herangezogen werden. Dabei sollte jedoch beachtet werden, dass diese sich auf alle Quantentechnologien bezieht, was vermutlich zu einer gewissen Verzerrung führt.

Die prominentesten Beispiele für staatliche Forschungsprogramme und Investitionen aus der Wirtschaft sind:

Dedizierte Forschungsprogramme

- Schweden: 100 M€ durch Wallenberg Stiftung

- UK: 330 M€ über fünf Jahre für alle Quantentechnologien
- EU Flagship: 1 Milliarde € über zehn Jahre für alle Quantentechnologien (EU und Nationale Beiträge). Eine Aufstockung in ähnlicher Größenordnung zur Schaffung von Infrastruktur wird wohlwollend diskutiert.
- China: 10 Milliarden USD für ein Nationales Zentrum für Quanteninformationswissenschaft (laut South China Morning Post, http://www.scmp.com/news/china/economy/article/2140860/china-winning-race-us-develop-quantum-computers)

Privatwirtschaftliche Investitionen

- Rigetti: 70 M USD Venture Capital
- Intel: 50 M USD über zehn Jahre an TU Delft, zzgl. eigenes Personal (schätzungsweise 10-20 Personen)
- Google: Hardware-Team schätzungsweise 30-50 Wissenschaftler, entspricht 10-20 M USD pro Jahr.
- IBM: Etwas größeres Team als Google

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

Neben den genannten strukturellen Aspekten empfehle ich inhaltlich eine Fokussierung auf Technologie- und Demonstratorentwicklung für Ionenfallen, supraleitende und Halbleiterqubits. Weiterhin sollten Möglichkeiten bestehen, für die avisierten Systeme besonders wichtige grundlegende Forschungsprojekte zu priorisieren. Insbesondere in den nächsten Jahren muss auch der Mut bestehen, Gruppen mit relevanter Kompetenz, aber ohne einschlägige Vorarbeiten einzubeziehen, z.B. aus den Ingenieurwissenschaften. Die Prioritätensetzung (wie auch Umsetzung) sollte einer regelmäßigen Evaluation mit langfristiger Perspektive unterworfen werden. Selbst wenn z.B. in zehn Jahren kommerzielle Systeme verfügbar sein sollten wird es voraussichtlich weiterhin ein umfangreiches Weiterentwicklungspotential geben, das nur mit entsprechender Forschung ausgeschöpft werden kann. Einerseits ist denkbar, dass manche Systeme sich als nicht konkurrenzfähig erweisen, andererseits könnten sich neuartige, noch wenig etablierte Ansätze (wie z.B. Majorana-Qubits) als performanter erweisen. Für die reine Grundlagenforschung bestehen meiner Meinung nach bewährte Instrumente, die fortgeführt werden sollten.

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 Übertragung herkömmlicher Programme auf Quantencomputer ist unmöglich oder zumindest sinnlos. Es müssen nicht nur neue Software, Programmiersprachen und Programmierwerkzeuge entwickelt werden, sondern auch neue Algorithmen, die ein grundlegendes Umdenken erfordern.

Aus meiner experimentellen Sicht ist die Forschung in diesem Bereich in Deutschland nicht von hoher Sichtbarkeit, wobei anzumerken ist, dass anwendungsorientierte Studien von relativ

wenigen Gruppen dominiert sind. Eine Ansiedlung neuer Professuren wäre wünschenswert, müsste vermutlich jedoch stark incentiviert 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

Im Detail möchte ich hier auf die Kompetenz anderer, dem Thema näherstehenden Experten verweisen. Ich gehe davon aus, dass bis dahin mindestens zehn Jahre vergehen werden, möglicherweise deutlich länger. Jedoch können auch Durchbrüche, die zu einer rascheren Entwicklung führen, nicht ausgeschlossen werden. Auch der schwer vorherzusagende Umfang von Förderung und Industrieinvestition spielt eine Rolle.

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?

Auch hier sind andere Experten versierter als ich. Die staatliche oder staatlich geförderte Beschaffung von Quantenkryptographiesystemen würde dem Feld vermutlich Vorschub leisten. Jedoch ist mir nicht klar, in wieweit derzeitige Kryptographiesysteme einen nennenswerten Vorteil bieten. Deren tatsächliche Sicherheit im Feld ist noch unzureichend untersucht, und sie stellen nur eine Teillösung dar. Eine weitere Beforschung und Systemkompetenzentwicklung ist sinnvoll, der praktische Nutzen von groß angelegten Implementierungsprojekten mit bereits demonstrierten Ansätzen sollte meines Erachtens jedoch nicht überbewertet werden.

Anhang

Präsentation von Marc de Jong, McKinsey im Rahmen der Quantum Europe Konferenz in 2016 in Amsterdam, verfügbar unter http://j.mp/qe2016-presentation.