Deutscher Bundestag

Ausschuss Digitale Agenda

Ausschussdrucksache
19823)009

Antworten zum Fragenkatalog zur öffentlichen Anhörung „Quantencomputer“ des Ausschusses Digitale Agenda am Mittwoch den 6. Juni 2018

Univ.-Prof. Dr. Frank Wilhelm-Mauch, Fachrichtung Physik, Universität des Saarlandes
fwm@lusi.uni-sb.de

Vorbemerkung

Eine Reihe der hier skizzierten Ausführungen sind sehr viel ausführlicher in einer unter Federführung meiner Arbeitsgruppe entstandenen Studie des Bundesamts für Sicherheit in der Informationstechnik (Titel „Entwicklungsstand Quantencomputer“) behandelt[i]. Auf diese werde ich als „BSI-Studie“ verweisen.

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

Auf der *theoretischen Seite* wurde eine ganze Reihe von Algorithmen für Quantencomputer entwickelt, die gegenüber heutigen Computern (ab jetzt als „klassische Computer“ bezeichnet) eine qualitative Beschleunigung ermöglichen. Dies bedeutet, dass die Rechenzeit bei Vergrößerung der Aufgabe langsamer steigt als bei einem klassischen Computer. Dazu gehören Datenbanksuche, Kryptanalyse (Entschlüsselung von RSA Kryptographie), Modellierung von Materialien und Molekülen sowie Maschinenlernen. Es wurde auch eine ganze Reihe von Algorithmen entwickelt, bei denen eine qualitative Beschleunigung möglich, aber noch nicht mathematisch bewiesen ist. Dazu gehören Optimierung, Analyse von Netzwerken und Lösen von Gleichungssytemen. Genauere Beispiele für Anwendungen erscheinen in den Antworten zu den Fragen 3, 6 und 7.

Auf der *experimentellen Seite* gibt es, ähnlich der Frühzeit des klassischen Computers, eine Reihe von Hardwareplattformen. Im Augenblick sind Quantenprozessoren mit bis zu 20 Quantenbits (Qubits) über die Cloud zugänglich. Deren Eigenschaften sind dadurch gut bekannt. 20 Quantenbits entsprechen 1 Megabyte eines klassischen Computers. Verschiedene Firmen haben bis zu 72 Qubits angekündigt. Dies bedeutet es wurden Bilder von Chips gezeigt, aber es wurden keine Leistungsdaten und Testergebnisse veröffentlicht und es gibt keinen äußeren Zugang. Bei ausreichender Leistungsfähigkeit kann ab ca. 50 Qubits der Quantenvorteil (Quantum supremacy / quantum advantage) erreicht werden, also der Punkt, an dem dieser Quantencomputer nicht mehr durch die größten klassischen Supercomputer simuliert werden kann. Der hier verwendete Begriff der Leistungsfähigkeit bezieht sich vor allen Dingen auf die Fehlerrate der Operationen des Quantencomputers, die die Länge des fehlerfrei abgearbeiteten Algorithmus begrenzt. Eine ausführlichere Würdigung dieses Konzeptes findet sich in der Antwort zu Frage 7.

Damit Algorithmen beliebiger Länge und beliebiger Genauigkeit abgearbeitet werden können, müssen die Qubits aktiv fehlerkorrigiert werden. Dies erfordert ein Vielfaches an physikalischen Qubits für die gleiche Kapazität. Die grundlegende praktische Tragfähigkeit dieses Konzepts wurde experimentell demonstriert, seine vollständige Umsetzung steht aber erst am Anfang.

Eine Sonderrolle nimmt das *adiabatische Quantencomputing* bzw. *Quantenannealing* ein. Dies ist ein alternativer Zugang zur Realisierung eines Quantencomputers, dessen apparative Anforderungen geringer sind als bei konventionellen gatterbasierten Quantencomputern. Die kanadische Firma *d-wave Systems* bietet Maschinen mit 2000 Qubits an. Diese sind für eine kleine Aufgabenklasse geeignet und ihr Beschleunigungspotenzial ist hoch umstritten. Für *kohärente Annealer,* die d-Wave nicht anbietet und deren Entwicklung erst am Anfang steht, werden Beschleunigungen wie bei den vorher beschriebenen konventionellen Quantencomputern erwartet.

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?

Deutschland und Europa leisten entscheidende Beiträge zu den Grundlagen des Quantencomputing. So wurde z.B. die erste Theorie eines supraleitenden Quantencomputers (einer der führenden Plattformen, die u.a. von Google und IBM entwickelt wird, siehe auch Antwort zu Frage 8) am Karlsruher Institut für Technologie entwickelt. Der Übergang von der Grundlagenforschung zur angewandten Forschung, insbesondere dem Bau von Quantencomputern wurde jahrzehntelang in den USA deutlich stärker gefördert als in Europa. Bemerkenswerterweise fördern diese Programme auch in erheblichem Umfang deutsche und europäische Gruppen[ii], was deren internationale Konkurrenzfähigkeit unterstreicht. Dennoch ist die Entwicklung von hardwarebasierten Geschäftsmodellen (Cloud / Quantencomputing als Service) dort mit Abstand am weitesten fortgeschritten.

Eine umfassende Akteursliste findet sich in der BSI-Studie. Die Ausführungen hier können auch durch die Beschreibung von Förderprogrammen in der Antwort zu Frage 11 ergänzt werden. Quantencomputing in der Cloud wird von den US-Unternehmen IBM, Google, Rigetti und IonQ angeboten. Hardware für adiabatisches Quantenannealing wird von der kanadischen Firma d-Wave Systeme angeboten. Intel hat vor kurzem Chips für Quantencomputer vorgestellt, deren Leistungsdaten nicht veröffentlicht sind. Microsoft betreibt mehrere einschlägige Forschungsinstitute. Führende akademische Akteure in den USA sind die Yale University, das California Institute for Technology und das MIT (einschließlich des Lincoln Laboratory) in den USA sowie das Institute for Quantum Computing an der Universität Waterloo in Kanada. Im europäischen Ausland sind QuTech an der TU Delft und Qusoft an der Universität Amsterdam, die ETH Zürich, das Niels-Bohr-Institut in Kopenhagen, CEA in Frankreich an den Standorten Grenoble und Paris, die Chalmers University of Technology in Göteborg, die Oxford University, University of Sussex und die Universität Innsbruck zu nennen. In Deutschland nehmen Gruppen an der Universität Mainz, dem Forschungszentrum Jülich, der RWTH Aachen und der Universität des Saarlandes an großen Programmen teil, darüber hinaus befinden sich führende Arbeitsgruppen in Theorie und Software am Max Planck Institut für Quantenoptik und der FU Berlin.

Die Position der USA ist wie schon oben angedeutet dadurch geprägt, dass schon sehr früh die reine Grundlagenforschung ergänzt wurde durch angewandte Forschung, sowohl durch öffentliche als

auch durch privatwirtschaftliche Investitionen. Letztere sind einerseits durch eine große Risikobereitschaft und -befähigung der dortigen Unternehmen und Investoren bedingt – andererseits ist die Beobachtung wichtig, dass auch diese auf den Schultern öffentlicher Forschung stehen: Das Programm von IBM startete 2010 mit der Akquise des ersten Regierungsprojektes und die Expertise des Hardware-Forschungsleiters von Google, John Martinis, entstand ganz entscheidend in seiner Zeit als Professor an der staatlichen University of California Santa Barbara im Rahmen von Regierungsprojekten.

Die Position Chinas ist durch die Heterogenität der Forschungslandschaft und aktuell sehr große Investitionen geprägt, die vor allen Dingen den Schritt von der grundlegenden zur angewandten Forschung beflügeln. Während die Programme in der Quantenkommunikation und -kryptographie (einem Nachbargebiet des Quantencomputing und ein der vier von der EU identifizierten Anwendungssäulen der Quantentechnologien) bereits seit einigen Jahren Weltniveau haben, sind hochkarätige Veröffentlichungen im Bereich Quantencomputing erst in den letzten 12 Monaten aufgetaucht. Diese steile Entwicklung dürfte bald zu einem Aufschließen mit den weltweit besten Aktivitäten führen.

Im Gebiet Quantencomputing, das gerade aus der Grundlagenforschung in die Anwendung hineinwächst, ist internationale Kooperation selbstverständlich. Es ist meines Erachtens wichtig, dies weiter zu betreiben, um weiterhin die besten Köpfe und besten Ideen in Austausch zu halten und der Tendenz von Unternehmen und einigen Regierungsbehörden, Ergebnisse nicht öffentlich zu machen, entgegenzuwirken. Das europäische Flaggschiffprogramm in Quantentechnologien ist hier ein wichtiger Baustein.

Im Bereich von industriellen Anwendungen erleben wir augenblicklich erste Aktivitäten. Insbesondere die amerikanischen Hardwareanbieter versuchen, mit großen deutschen Firmen Partnerschaften abzuschließen um die Anwendungsentwicklung weiter zu bringen – wie auch immer wieder in den Medien berichtet. Dies ist einerseits hochwillkommen, da so die Anwendungsentwicklung von Quantencomputern in der deutschen Industrie ein stark besetztes Thema wird. Andererseits können so frühe Oligopole entstehen sowie ein Spannungsfeld mit der hier weiterhin notwendigen offen zugänglichen Wissenschaft. Ein europäisches Gegengewicht in Form einer offenen Plattform für Quantencomputing ist hier eine geeignete Antwort.

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)?

Als Kontext und zur Begriffsklärung möchte ich vorausschicken: Sowohl die Hardware- als auch die Anwendungsentwicklung im Bereich Quantencomputing zielt im Augenblick in den Bereich Höchstleistungsrechnen und Rechenzentren mit Cloudzugang. Es sind im Augenblick keine Anwendungen bekannt, die persönliches oder mobiles Quantencomputing nahelegen würden. Die Rahmenbedingungen für das Funktionieren von Quantenprozessoren (Kühlung, Vakuum, Laser etc.) sind anspruchsvoll. Dies entspricht der Situation der Frühzeit des klassischen Computings – dort hat es sich bekanntlich grundlegend geändert. Diese Entwicklung kann im Quantencomputing nicht ausgeschlossen werden, ist allerdings nicht seriös absehbar. Anwendungen, Marktreife und Verbreitung beziehen sich also auf diese Höchstleistungsebene. Und die Auswirkung auf unser tägliches Leben ist mittelbar – nicht durch direktes Nutzen von Quantencomputern sondern durch Nutzung von durch Quantenbeschleunigung ermöglichten Anwendungen.

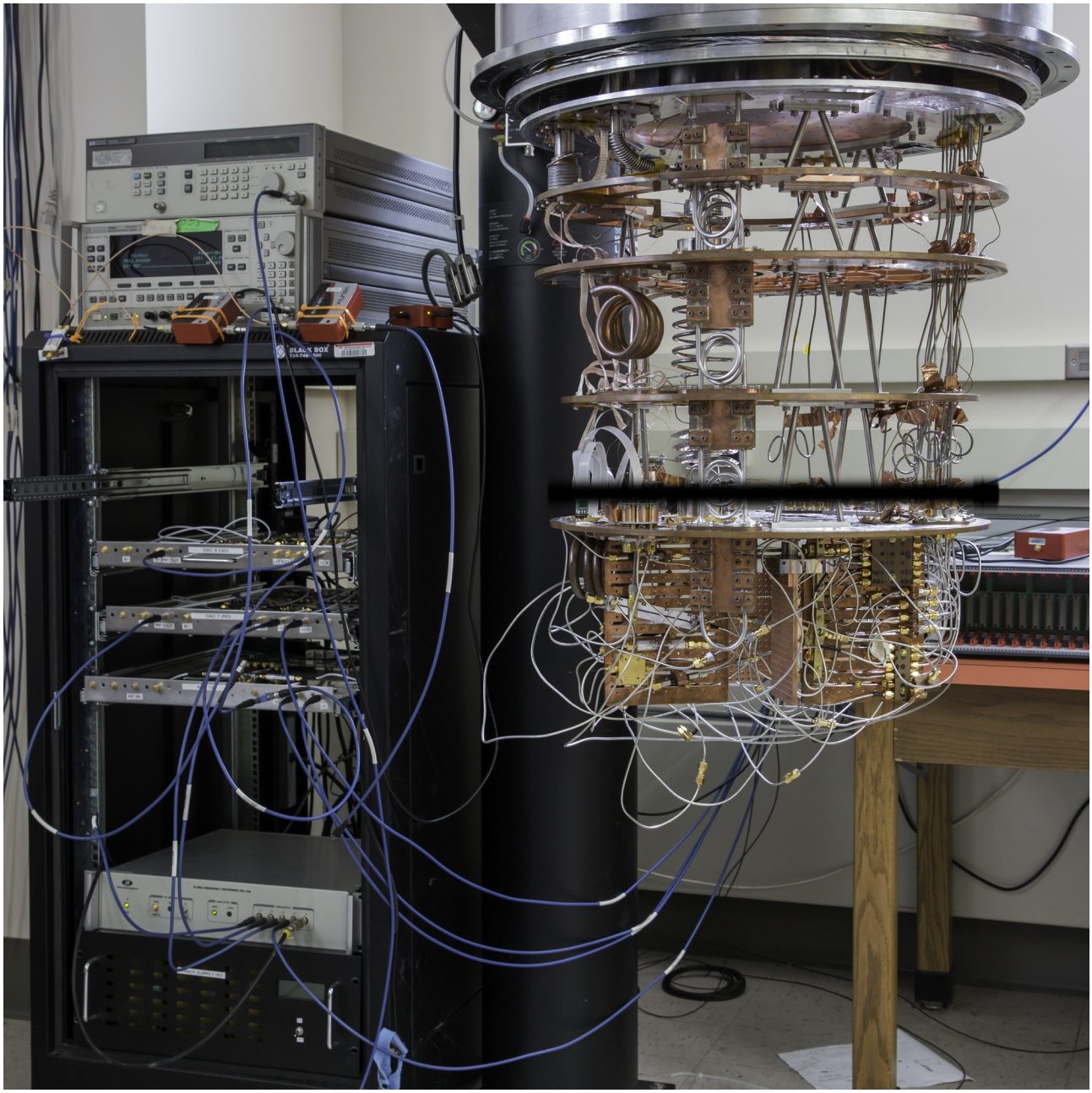

Illustration 1: Beispiel für die Innenansicht eines Quantencomputersystems: Wenige Chips sind am unteren Ende der Kupferstruktur eingebaut. Die Kupferplatten dienen der Wärmeleitung, die darüber erscheinende Hülle ist Teil des Tieftemperatursystems. Foto: Edward Leonard jr., University of Wisconsin, Madison

Gesellschaftliche Chancen und Herausforderungen entstehen aus den Anwendungen. Optimierungsaufgaben in Netzwerken können die Optimierung von Stromflüssen in komplexen Versorgungsnetzen oder das Routing von Individualverkehr sein – hier ist Quantenbeschleunigung möglich. Optimierungsaufgaben entstehen in der künstlichen Intelligenz – diese können bei gleicher Datenmenge potenziell schneller erledigt werden, gesellschaftliche Chancen und Herausforderungen sind im Rahmen der Bewertung künstlicher Intelligenz zu sehen. Die Entwicklung neuer Materialien und Moleküle z.B. in der Katalyse – eine der erwarteten ersten Anwendungen – bietet eine große Chance der Erschließung neuer Prozesse. Ziel dieser Community ist z.B. die Optimierung der Synthese von Stickstoffdünger durch Modellierung von Quantencomputern, die den bisherigen Haber-Bosch-Prozess (ca. 3% des weltweiten CO2-Ausstoßes) durch ein CO2-neutrales Verfahren ersetzen soll. Eine gesellschaftliche

Herausforderung kann durch den Shor-Algorithmus entstehen, mit dem die augenblicklich gängige Verschlüsselung nach dem RSA-Verfahren angreifbar wird, siehe auch Antwort zu Frage 14. Dies ist eine sehr anspruchsvolle Anwendung. Ihr kann aber durch klassische Kryptographieverfahren – der Post-Quanten-Kryptographie – begegnet werden.

Neben dem ökologischen Nutzen der vorher erwähnten Anwendungen kann auch der ökologische Fußabdruck von Quantencomputer-Hardware betrachtet werden. Grundsätzlich ist Quantencomputing reversibel und damit äußerst energiesparend. Praktisch muss jedoch sehr viel Energie aufgewendet werden, um die Rahmenbedingungen für den Quantencomputer zu schaffen – je nach Plattform sind dies tiefe Temperaturen, Ultrahochvakuum etc. Diese Technologie ist im Augenblick nicht energetisch optimiert. Als Anhaltspunkte möchte ich zunächst eine Extrapolation der Universität Sussex nennen, der die Leistungsaufnahme eines großen Quantencomputers abschätzt und zu dem Ergebnis kommt, dass diese zwar hoch ist, aber durchaus kleiner als die von klassischen Supercomputern. Ein weiterer Anhaltspunkt ergibt sich aus Arbeiten des Forschungszentrums Jülich zur Modellierung von Quantencomputing auf klassischen Hochleistungsrechnern – auch deren Energieaufnahme ist deutlich höher als die des simulierten Quantensystems.

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“?

Viele physikalische Hochtechnologien sind dual use (Radar, das Internet mit seinem Vorgänger ARPAnet, Laser, Kernspaltung) und Quantencomputer sind keine Ausnahme. Optimierung und KI haben zivile und militärische Einsatzbereiche, die Kryptanalyse von RSA kann militärisch und geheimdienstlich eingesetzt werden.
Aufgrund der aktuellen und absehbaren Entwicklung würde aber die Entwicklung eines dafür relevanten Quantencomputers ein konzertiertes Programm erfordern mit Akteueren einer Größe, die durch deutsche Regulierung nicht greifbar sein dürften. Insofern sehe ich keinen aktuellen regulatorischen Bedarf. Sehr wohl ist aber zuverlässige Information für die Information wichtig, auch und gerade jetzt in der Zeit hohes Schlagzeilenaufkommens.
Eine verwandte Frage kann aber sein, ob die Nutzung von Quantencomputing nicht unter rein europäischer Legislation möglich sein sollte, was die Entwicklung von offener europäischer Hardware erfordert.

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

Es gibt eine Reihe ökonomischer Analysen, z.B. von Accenture.

Im Sinne der Technikfolgenabschätzung ist mir außer der BSI-Studie nichts weiteres bekannt. Diese evaluiert den Entwicklungsstand von Quantencomputing und entwickelt ein Bewertungssystem. Er soll insbesondere das BSI in die Lage versetzen, die Einführung von Post-Quanten-Kryptographie zu planen.

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?

Ein Teil dieser Frage ist bereits mit den Antworten zu den Fragen 1 und 3 behandelt, insbesondere zu gesellschaftlichen Herausforderungen und Chancen und zur Natur der Quantenbeschleunigung.

Die Grundlage von Quantenbeschleunigung ist der Quantenparallelismus: Wenn auf einem klassischen Computer Daten parallel in mehreren Strängen verarbeitet werden sollen, dann ist pro Strang entsprechende Hardware vorzuhalten. Quantencomputer hingegen können ohne zusätzliche Hardware parallel arbeiten. Insofern sind Aufgaben mit hohem Potenzial für Parallelverarbeitung typisch für Quantenbeschleunigung.
Insbesondere die Anwendungen in Optimierung, Gleichungssystemen, und Netzwerksanalyse sind wichtige Grundlagenalgorithmen mit vielfältigen praktischen Anwendungen. Genaue use-cases für Quantencomputer entstehen aktuell: Durch die angebotene Test-Hardware und die Einbindung von vormals fachfremden Nutzern werden neue Anwendungsfelder dieser Grundalgorithmen erschlossen. Als Beispiel kann ich nennen, dass in meiner Arbeitsgruppe gerade zwei Industriepromotionen bei einem großen deutschen Automobilhersteller zu solchen Use-Cases ausgeschrieben sind und dass eine Promotion mit dem DLR bereits läuft. Ein großer Teil dieser Nutzer sind Technologiescouts forschungsstarker Unternehmen. Diese Entwicklung – die Identifikation von Anwendungen durch früher Generationen von Programmieren – war bei klassischen Computern sehr ähnlich.

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 Aktuelle Diskussion zur „Quantum supremacy“ bezieht sich zunächst auf die ersten Anwendungen, in denen ein Quantencomputer einen klassischen Supercomputer übertrifft. Dies werden voraussichtlich sehr akademische Anwendungen sein (Quantenchaos, Bosonensampling).

Zu Anwendungen verweise ich im Grundsatz auf Fragen 1,3 und 6. Zu den konkret genannten Anwendungsgebieten führe ich Beispiele an einschließlich dem Wissensstand über die Anwendungen:

- Energieforschung: Quantencomputerassistierte Entwicklung von energiereduzierten Prozessen. Quantenvorteil mathematisch bewiesen
- Verkehr: Planung von Verkehrsfluss. Quantenvorteil nicht quantifiziert
- Verkehr: Schaltungsfehlersuche in Luft- und Raumfahrtsystemen
- Medizin/Pharmazie: Quantencomputerassistierte Entwicklung von Wirkstoffen. Quantenvorteil mathematisch bewiesen
- Industrie 4.0: Schnelles Lösen von Gleichungssystemen im Hintergrund. Quantenvorteil nicht quantifiziert
- Industrie 4.0: Sichere Kommunikation von Sensordaten durch Quantenkommunikation mit kleinen Quantenprozessoren als Quantenrepeater. Quantenvorteil mathematisch bewiesen
- Verteidigung: Kryptanalyse wenn die zu entschlüsselnde Nachricht auf RSA basiert, Quantenvorteil mathematisch bewiesen
- Maschinenlernen: Schnelles Trainieren; Quantenvorteil bewiesen aber extreme Hardwareanforderungen
- Kommunikation: Siehe Industrie 4.0
- Blockchain: Prinzipielle Angreifbarkeit von komplexitätsbasierter Verschlüsselung

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 BSI-Studie nimmt hier eine sehr ausführliche Gliederung und Einordnung vor. Im Augenblick sind zwei Qubit-Implementierungen führend: Einmal in Vakuumapparaturen gefangene Ionen – eine mit Atomuhren verwandte Technologie – und zum anderen Mikroprozessoren aus supraleitenden Materialien – meistens stark gekühltes Aluminium oder Niob. Es ist aber durchaus noch Bewegung in dem Gebiet. Insbesondere Fortschritte im Bereich von Nanostrukturen aus Silizium und Fehlstellen in künstlichen Diamanten sind vielversprechend, jedoch sind hier zum Aufschließen auf die Erstgenannten noch Verbesserungen notwendig.

Die technologischen Herausforderungen sind im Detail plattformabhängig. Grundsätzlich muss aber die Fehlerrate zuverlässig und in allen Fällen gesenkt werden und bei dieser niedrigen Fehlerrate müssen Prozessoren größer werden. Diese beiden Eigenschaften können in bestimmten Grenzen gegeneinander aufgerechnet werden: Die Technik der Quantenfehlerkorrektur erlaubt es, Komponenten mit Fehlerraten von 1:1000 oder geringer (Fehlerkorrekturschwelle) zu benutzen und mit Overhead in der Qubitzahl dennoch Algorithmen zuverlässig durchzuführen.

In den führenden Implementierungen sind diese Fehlerschwellen nahezu erreicht bzw. in Einzelfällen erreicht. Die nötige Zuverlässigkeit erfordert eine Reihe von inkrementellen technologischen Fortschritten. Strukturell besteht die Herausforderung, dass diese Art der spezialisierten Technologieentwicklung schwer an Universitäten zu leisten ist, was der Industrie aber auch der nichtuniversitären Großforschung eine Schlüsselrolle zuweist.

Prognosen sind schwierig, jedoch gehe ich davon aus, dass die Fehlerkorrekturschwelle in supraleitenden Schaltkreisen in wenigen Jahren konsistent überwunden werden wird, dass also auch die schlechtesten Qubits eines großen Prozessors gut genug sind. Die Frage, ob Ionenfallen bei Skalierung auf große Prozessoren genau so fehlerarm arbeiten können wie die augenblicklichen Systeme, ist schwerer einzuschätzen.

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?

Firmen, die Quantencomputer als Werkzeuge für Forschung und Entwicklung oder als Teil ihrer IT-Infrastruktur einsetzen, können dadurch einen qualitativen Entwicklungsvorsprung erreichen, insbesondere in entwicklungsintensiven Bereichen.

Am Beispiel der chemischen Industrie und der Materialentwicklung kann man verdeutlichen, dass Quantencomputer die Zahl der modellierbaren Materialien sprunghaft vergrößert und neue Materialklassen der Modellierung zugänglich macht, was einen entscheidenden Entwicklungsvorsprung bedeuten kann. Angesichts der gut bekannten Algorithmen, den bereits vorhandenen Modellierungsaktivitäten in einschlägigen Unternehmen, und der Bedeutung eines solchen Entwicklungsvorsprungs der bereits heute hohe Entwicklungskosten nach sich zieht kann diese Industrie ein Pionier in der Quantencomputeranwendung sein.

Analoges wird für andere Branchen erwartet, insbesondere auch Logistik und Produktionsoptimierung.

Die Markteinführung von Quantencomputern geschieht in Phasen, bezogen auf den Charakter als HPC-Technologie (siehe auch Frage 3):

1. Die Markteinführung von Quantencomputern als Versuchsplattform in der Cloud – Quantencomputer von interessanter Größe die aber noch nicht leistungsfähiger sind als klassische Computer – ist bereits im Gange. Diese Quantencomputer werden i.A. beim Hersteller gehostet.
2. Die Markteinführung von Quantencomputer als Hardware für Rechenzentren auf dem Niveau einer Versuchsplattform startet augenblicklich. Die umstrittene d-Wave Quantenannealing-Plattform (siehe Frage 1) wurde einige Male verkauft. Das US-Energieministerium hat augenblicklich ein Programm aufgelegt, in dem „Quantum testbeds“ in verschiedenen Forschungseinrichtungen installiert werden sollen. Der Schritt von 1 nach 2 erfordert vor allen Dingen mehr Stabilität der verwendeten Anlagen und benutzerfreundlichere Infrastruktur, so dass der Computer nicht mehr von Fachwissenschaftlern betrieben werden muss, sondern von einschlägig weitergebildeten Ingenieuren und Technikern. In den folgenden Schritten ist auch von diesem Wechsel von Cloudzugang beim Hersteller hin zur Installation in Rechenzentren auszugehen.
3. Der Schritt zur Quantenüberlegenheit (siehe Frage 7) in den ersten Anwendungen wurde von verschiedenen Anbietern angekündigt. Ich gehe davon aus, dass wir in 2019 erste Demonstrationen sehen. Die Zutaten dazu wurden gezeigt, das Skalieren in eine größere Maschine erscheint eine lösbare Herausforderung.
4. Das Erreichen von Quantenüberlegenheit in interessanten Anwendungen, aber mit nur rudimentärer Fehlerkorrektur, ist eine logische Fortsetzung des vorherigen Schrittes und erfordert weiteres Skalieren. Eine Analyse der Ergebnisse von Schritt 3 hat Einfluss auf eine Einschätzung von dessen Machbarkeit, aber es ist davon auszugehen, dass dies in 3-5 Jahren erreichbar ist.
5. Der vollständige, universelle, fehlertolerante Quantencomputer ist ein Langzeitziel. Es wurden erste, beeindruckende Demonstrationen von Fehlerkorrektur gezeigt. In der BSI-Studie ist ausgeführt, dass z.B. ein kryptanalytisch relevanter, fehlerkorrigierter Quantencomputer mit einer Million Qubits die konzertierte Forschungsanstrengung einer Industrienation (vergleichbar etwa dem Apollo-Programm) benötigen würde, und dann einige Jahre benötigen würde. Das Ergebnis wäre ein wissenschaftliches Großgerät. Diese Studie geht davon aus, dass die Schritte für Niveau 4 erreicht werden und dann hochskaliert. Die Forschungsagenda des EU-Quantentechnologie-Flaggschiffs setzt 50 fehlerkorrigierte Qubits (bestehend aus etwa 50000 physikalischen Qubits) als Ziel in 10 Jahren – dies wird von der Community als sehr ambitioniert angesehen.

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 erfolgreichste Softwareentwicklung für Quantencomputer findet augenblicklich nah an der Hardware statt. So können Einschränkungen der Hardware und Software optimal aufeinander abgestimmt werden. Dieses Prinzip des „Ko-Design“ von Hard- und Software spielt für Quantencomputer eine größere Rolle als im klassischen Supercomputing. Insofern sind diese Gebiete meiner Ansicht nach nicht trennbar – erfolgreiche Softwareentwicklung benötigt mindestens einen offenen Zugriff auf Hardware und detaillierte Kenntnis ihrer Eigenschaften sowie regen Austausch zwischen beiden Ebenen. Schutzinteressen von großen Konzernen außerhalb der EU beginnen diesen zu erschweren.

Deutschland hat das wissenschaftliche Know-How zur Entwicklung von Hardware, was z.B. die Einbindung deutscher Wissenschaftlerinnen und Wissenschaftler in entsprechende globale Programme (siehe Frage 2) belegt. Im Augenblick fehlt in Deutschland auf diesem Gebiet ein konzertierter Impuls zur tatsächlichen integrierten Systementwicklung. Auf diesem Gebiet haben andere Länder eine Vorsprung, der aber aufgrund des frühen Stadiums der Entwicklung aufholbar ist. Neben den US-Programmen ist zu erwähnen, dass große öffentliche Investitionen in dieses Gebiet u.a. in Australien, Schweden, den Niederlanden und Österreich getätigt werden und dass strategische Partnerschaften in diesen Ländern aber auch in Frankreich geplant sind – eine solche Entwicklung fehlt in Deutschland. Auf geeignete Förderinstrumente wird bei Frage 11 noch eingegangen.

Da Quantenphysik die Physik des Mikroskopischen ist, ist der Materialeinsatz im Kern eines Quantencomputers im Allgemeinen gering. Die Peripherie des Quantencomputers kann allerdings sehr umfänglich sein, siehe Abbildung. In verschiedenen Plattformen sind Materialien im Einsatz, die schwierig herzustellen sind, deren Ausgangsmaterialien allerdings leicht zu erhalten sind. Dazu gehören

- bei Tieftemperatur-Quantencomputern einschließlich supraleitenden und halbleitenden Schaltkreisen: Das Isotop Helium-3. Dieses wird i.A. als Nebenprodukt von Nukleartechnologie gewonnen oder gezielt aus ausgebrütetem Tritium hergestellt. Da es nur noch einen Reaktor gibt, der dies tut (in den USA) gibt es eine globale He-3 Krise mit hohen Preisen.
- Bei siliziumbasierten Quantencomputern (siehe Frage 8) ist es von großem Vorteil, mit isotopenreinem Silizium zu arbeiten, das aus dem natürlichen Silizium aufwändig hergestellt werden muss
- Quantencomputing mit Fehlstellen (siehe Frage 8) erfordert die Herstellung gezielt verunreinigter künstlicher Diamanten

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?

Die Grundlagenforschung in Quantencomputing in Deutschland ist exzellent und breit aufgestellt. Nur weniger Arbeitsgruppen spezialisieren sich allerdings auf den Übergang zur Angewandten Forschung. Eine Ursache davon liegt in der Struktur wissenschaftlicher Karrieren – solange nicht längerfristige Anstellungsmöglichkeiten gezielt für Quantencomputing entstehen neigen Wissenschaftler(innen) zur thematischen Diversifizierung. Dies gilt umso mehr, als dass beim Skalieren jenseits von wenigen Qubits die Aufgaben oftmals sehr spezialisiert technologisch sind – zu technologisch für eine Karriere in der Physik, zu spezialisiert für eine Karriere in den Ingenieurwissenschaften.

Folgende kurzfristige Maßnahmen erscheinen sinnvoll:

- *Bekenntnis zu Quantencomputing als angewandtes Forschungsgebiet und Etablierung von Programmen in diesem Bereich*: Eine Schlüsselrolle können dabei die nichtuniversitären Forschungseinrichtungen haben (Helmholtz, Fraunhofer, Leibniz), die in ähnlichen Situationen demonstriert haben, dass sie gerade diese spezialisierten Technologieaufgaben überzeugend und mit der nötigen Ausdauer lösen können. Ein erstes Ziel wäre darum die Schaffung einer Technologiestruktur für Quantencomputing die mehreren Hardwareplattformen zugute kommt – Software, Steuerelektronik, zuverlässige

Probenherstellung, Laser etc. Ein ähnliches Programm wurde vom BMBF bereits aufgelegt, dieses ist allerdings anbietergetreieben, während ein neues Programm für Quantencomputing nutzergetrieben sein sollte. Eine solche Strategie ist auch Förderung für die in dem Bereich bereits tätigen Unternehmen, die hier eingebunden werden können und für die z.B. die Kundenbasis für maßgeschneiderte Hilfstechnologien für Quantencomputer verlässlicher wird.

- *Ausbau von akademischen Programmen mit Dauerperspektive*: Es soll möglich sein, dass sich insbesondere vielversprechende Nachwuchswissenschaftler(innen) beim Durchstarten in ihrer Karriere auf Quantencomputing konzentrieren können. Ein Ziel einer solchen Initative, z.B. durch ein nachhaltiges Programm des BMBF sollte sein, dass deutsche Arbeitsgruppen in europäischen Verbünden zentrale und strategische Rollen spielen können (und nicht hinter Schweden, Österreich, und der Schweiz zurückstehen).

- *Konsolidierte Forschungsstrategie für Quantencomputing basierend auf den vorherigen Schritten, entsprechende Investition:* Eine solche Strategie kann eine Priorisierung vornehmen, wie man sich konkret engagieren möchte (Priorisierung einer oder weniger Hardwareplattformen, Priorisierung von Rechenmodellen, Priorisierung zwischen full stack Entwicklung oder Konzentration auf bestimmte Ebenen). Ergebnis einer solchen Strategie kann eine Forschungseinrichtung oder einem Großverbund im Bereich Quantencomputing sein. Dieser Schritt wurde z.B. in Schweden von der Wallenberg-Stiftung gerade durchgeführt – das dortige Programm fördert supraleitende Quantencomputer über 10 Jahre mit 1 Mrd. SEK (100 Mio Euro). Diese nationale Quantencomputingstrategie kann aufgrund der Marktreife früher Quantencomputer bereits potenzielle Nutzer mit einbeziehen. Das Programm QUTEGA des BMBF, das Quatententechnologien in größerer Breite fördert, konzentriert sich im Augenblick auf andere Quantentechnologien, die kleinteiliger betrieben werden können.

Zur Entwicklung des nötigen interdisziplinären Ökosystems ist auch eine Reform der Ausbildung in Quantenphysik notwendig, insbesondere die Ausbildung für Nicht-Fachphysiker so wie Ingenieurinnen/Ingenieure, Informatiker(innen), und Lehrer(Innen). Ein solches Programm wird auf EU-Ebene diskutiert[iii] . Die Reform dieser Nebenfachausbildung erfordert zusätzliche Anstrengungen, die mit der aktuell schrumpfenden Grundfinanzierung von Universitäten nicht ohne weiteres geleistet werden kann.

Eine klare, belastbare Übersicht über die Investitionen in Quantentechnologien kann nicht gegeben werden, da sowohl privatwirtschaftliche Investionen als auch die Investitionen der US-Regierungsprogramme nicht offengelegt werden. Schätzungen belaufen sich auf $200 Mio pro Jahr.

Stattdessen können einige Eckinvestitionen benannt werden

1. Das europäische Flaggschiff-Programm für Quantentechnologien hat ein Volumen von 1 Mrd. Euro für 10 Jahre. Eine Erhöhung auf 2 Mrd wird im Augenblick diskutiert. Hier ist Quantencomputing eine von vier Anwendungssäulen. Die Ergebnisse der ersten Antragsrunde werden unmittelbar erwartet.
2. Die Regierung Kanadas hat allein in das Institute for Quantum Computing an der University of Waterloo bisher mindestens $C 100 Mio investiert und legt darüber hinaus landesweite Programme in beachtlicher Größe auf.
3. Die Investition der Wallenberg-Stiftung in eine Aktivität an einer einzigen Universität beträgt 100 Mio Euro über 10 Jahre

4. Die Regierung Australiens fördert die Entwicklung von Quantencomputern seit über 20 Jahren in einer Reihe von Programmen. Letztes Jahr allein wurden Investionen von $AU 40 Mio angekündigt.
5. In China wurde eine Investition von $10 Mrd angekündigt. Die Aufteilung der Mittel zwischen Quantenkommunikation und Quantencomputing ist mir nicht bekannt.

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

Auf europäischer Ebene wurde im Zuge der Vorbereitung des Flaggschiffes eine Forschungsagenda entwickelt, deren Ansichten ich weitestgehend teile, und die in verschiedenen Detailtiefen dargestellt ist [iv].

Eckpunkte dieser Strategie sind:

- sie ist nach Anwendungen gegliedert (Computing, Simulation, Kommunikation, Sensorik), nicht nach Plattformen
- sie bleibt kompetitiv – EU-Mittel werden in eng gestaffelten Runden augeschrieben, das Flaggschiffprogramm hat kein Kernkonsortium
- sie wird durch eine regelmäßig fortgeschriebene Forschungsagenda getrieben, die unter Einbeziehung sowohl von akademischen und industriellen Wissenschaftler(inne)n als auch von Vertreter(inne)n der Anwenderindustrie weiterentwickelt wird

Dem hinzuzufügen ist die Notwendigkeit von Infrastruktur für die begleitenden Technologien, siehe Antwort zu Frage 11, auch auf europäischer Ebene.

Für ein deutsches Programm verweise ich auf die Antwort zu Frage 10.

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?

Sowohl die von Quantencomputern unterstützten Operationen als auch die präzisen Methoden zur Nutzung der Quantenbeschleunigung sind von der Programmierung klassischer Computer deutlich verschieden. Über die letzten Jahre sind Programmierumgebungen und -sprachen für Quantencomputer entwickelt worden und beginnen sich zu konsolidieren. Erste Erfahrungswerte z.B. mit den Programmierwerkzeugen für die Cloudplattformen von Rigetti und IBM gewonnen hat sind durchaus vielversprechend, was das Erlernen durch vorher nicht quantenaffine Informatiker(innen) angeht.

An einigen Orten existieren interdisziplinäre Kurse und Programme zwischen Informatik und Physik, in denen diese Ausbildung entwickelt wird, z.B. in Delft, Waterloo (Kanada) und Grenoble. An deutschen Hochschulen ist mir nichts derartiges bekannt. Ein guter Ansatzpunkt wäre die Einrichtung von Vertiefungsrichtungen, Wahlpflichtbereichen oder evtl. spezialisierten Studiengängen im Masterbereich. Als Vorbereitung würde zunächst die Entwicklung von interdisziplinären Curricula wie in der Antwort zu Frage 11 beschrieben.

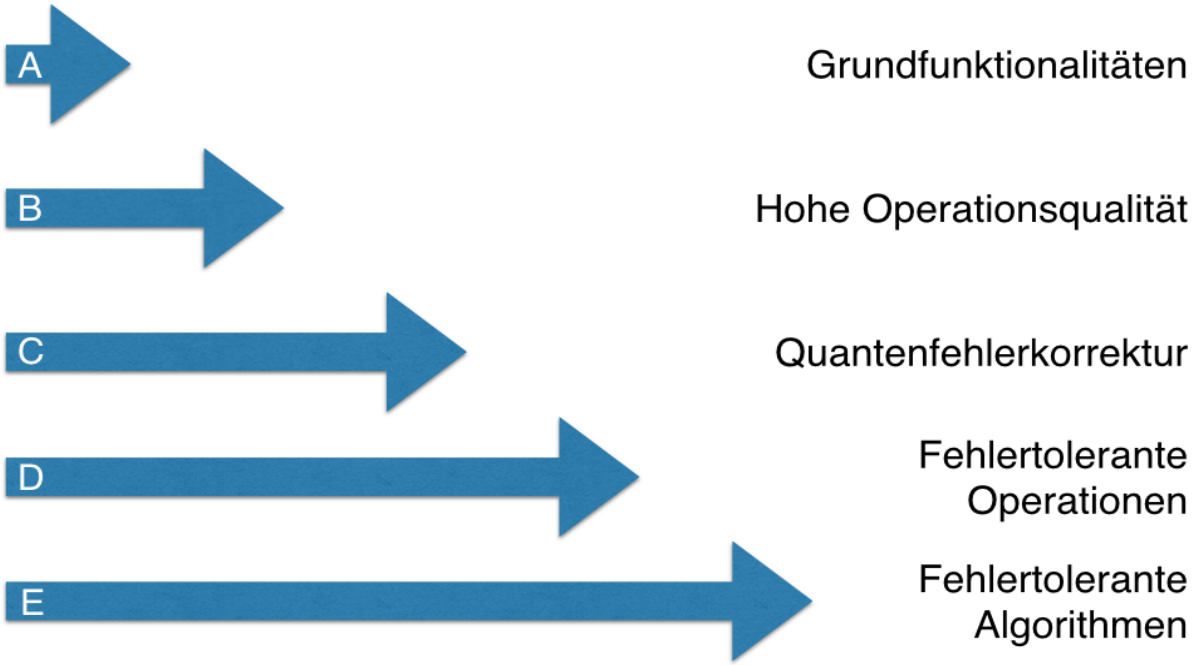

Illustration 2: Schichtenmodell zur Entwicklung eines Quantencomputers

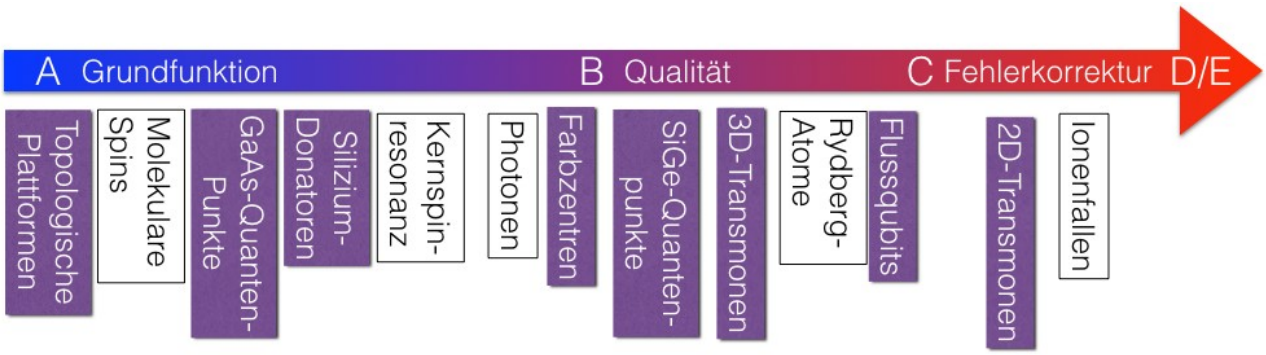

Illustration 3: Einordnung verschiedener Plattformen in das Schichtenmodell

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

Dies ist Gegenstand der BSI-Studie. Dort sind die wichtigsten Schlussfolgerungen:

- Kryptanalyse ist eine anspruchsvolle Aufgabe, die auf jeden Fall einen fehlerkorrigierten Quantencomputer erfordert (Punkt 5 der Antwort zu Frage 9). Leistungsanalyse und Platz/Zeit-Kompromisse werden durch die Fehlerkorrektur dominiert
- Es wurde ein 5-Schichten Modell der Bewertung von Quantencomputern entwickelt, an dessen Ende ein solcher fehlertoleranter Quantencomputer steht. Die erfolgreichsten Plattformen sind Augenblicklich in der dritten Schicht. Aufstieg zwischen den Schichten ist ein großer Forschungserfolg und dementsprechend zeitlich schwer einzuschätzen.
- Für Kryptanalyse haben wir die Annahme zugrunde gelegt, dass die augenblicklichen mittelfristigen Ziele z.B. im Bereich der Fehlerraten erreicht werden können
- Entschlüsseln von 2048 Bit RSA in 100 Tagen erfordert dann einen fehlertoleranten Quantencomputer mit etwa einer Million physikalischen Qubits. Ausgehend vom aktuellen 72-Qubit Meilenstein erfordert dies eine Forschungsanstrengung vergleichbar dem Apollo-Programm, erscheint aber erreichbar.
- Entschlüsseln 2048 Bit RSA ein einem Tag erfordert eine Milliarde Qubits. Hier können Kapazitätsprobleme entstehen z.B. bei der notwendigen Kühltechnologie und dies geht deutlich über die vorherige Herausforderung heraus
- Aufgrund der Effizienz von Quantencomputern ist, wenn dieses erreicht ist, eine Schlüsselvergrößerung kein nachhaltiger Schutz mehr
- Unten der gleichen Annahmen sind Kryptographieverfahren auf der Basis diskreter Logarithmen auf elliptischen Kurven bis 512 Bit in der gleichen Zeit angreifbar

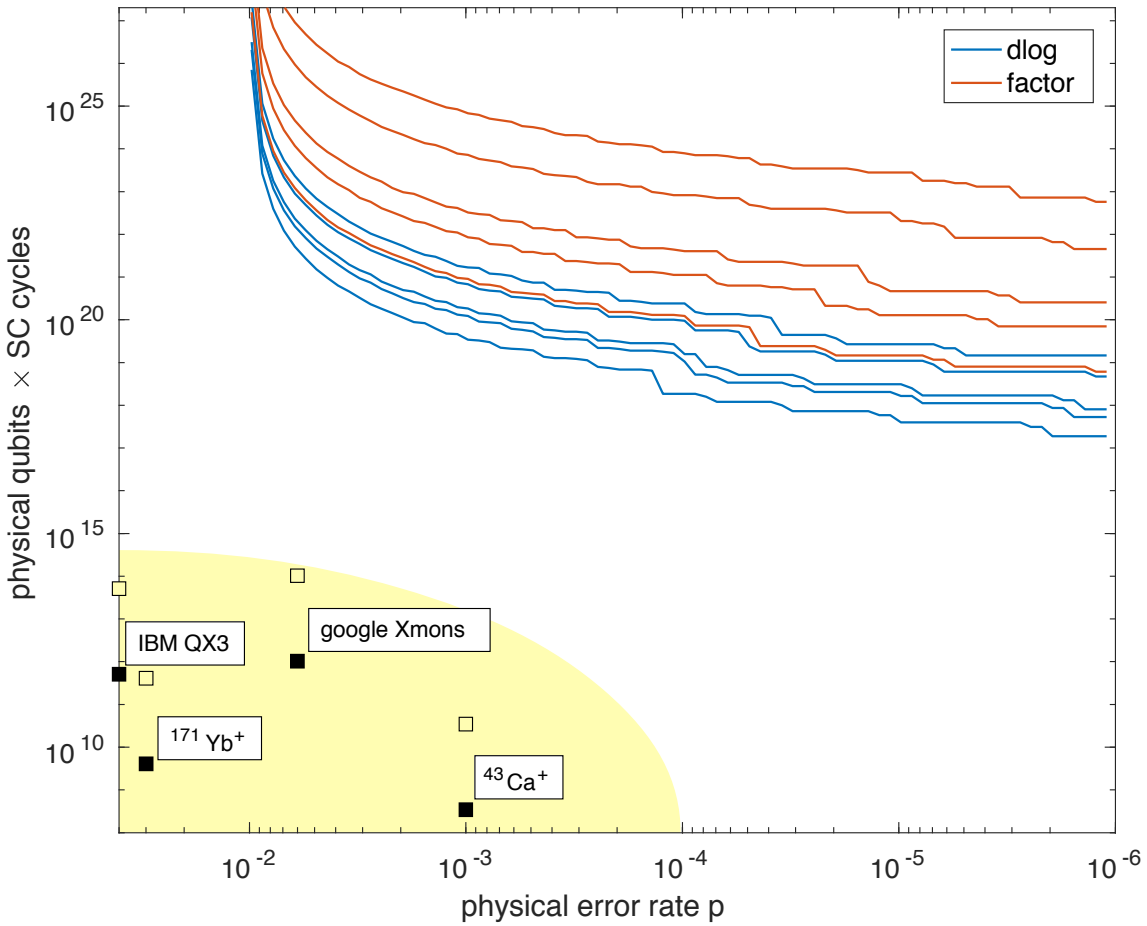

Illustration 4: Standortbestimmung: Wechselspiel von Fehlerrate und Zahl der Qubits für algorithmische Anwendungen. Gelber Bereich: Stand der Forschung anhand einzelner Experimente bei Laufzeit von einem Tag (gefüllt) oder 100 Tagen (offen); Linien: Anforderungen von diskreten Logarithmus zur Enschlüsselung elliptischer Kurven für 160,224,256,384 und 512 Bit bzw. Faktorisierung zur Entschlüsselung von RSA mit 1024, 2048, 3072, 7680 und 15360 bit.

Das BSI (Referat KT13) beobachtet dieses Thema und hat die zitierte Studie bereits frühzeitig (Jahreswechsel 2016/17) in Auftrag gegeben[v]. Grundlagenbeschlüsse zur Implementierung von Post-Quanten-Kryptographie sind bereits gefallen, z.B. auf er Ebene des europäischen Instituts für Telekommunikationsnormen (ETSI) und der Internet Engineering Task Force (IETF). Hier wäre es wichtig, dass Deutschland eine stärkere Rolle spielt und sich klar positioniert. Verschiedene Firmen (u.a. Infinieon und T-Systems) sind ebenfalls im Bereich Post-Quanten-Kryptographie aktiv. Für eine klarere Rolle Deutschlands sowohl bei der Festlegung dieser Standards als auch bei der proaktiven Umsetzung durch die deutsche Industrie wäre es wichtig, diese Aktivität im BSI deutlich zu intensivieren.

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?

Quantenkryptographie ist eine wichtige Quantentechnologie und ein direkter Nachbar des Quantencomputing. Ich gehe davon aus, dass andere Expert(inn)en hier detaillierter antworten können.

Quantenkryptographie kann durch Quantencomputer nicht überwunden werden. Grundfunktionalitäten der Quantenkryptographie wurden alle gezeigt – sie ist deutlich weiter fortgeschritten als Quantencomputing. Die Sicherheit von Quantenkryptographie beruht darauf, dass Angriffe immer detektiert werden können, bevor Daten ausgetauscht werden können – ein anderes Paradigma als RSA, dessen Sicherheit auf der Komplexität von mathematischen Aufgaben beruht. Damit kann Datenübertragung nachhaltig geschützt werden: Während man bei RSA z.B. die verschlüsselten Daten zunächst abspeichern kann und dann lange auf Fortschritte in der Computertechnologie zur Enschlüsselung warten kann ist dies bei Quantenkryptographie nicht der Fall.

Hier sind Feldversuche und der Aufbau von geeigneter Infrastruktur geeignete nächste Schritte für staatliches Handeln. Dies kann ein Programm zur satellitengestützen Quantenkryptographie sein, ein weiterer Ausbau des BMBF-Programms zum Quantenrepeater oder eine Version des Intercity-Backbones für Quantenkryptographie wie er einerseits auf europäischer Ebene diskutiert wird, andererseits auch im Westen der Niederlande vorangetrieben wird würden auch Startups und letztlich Bürger(inne)n den Weg in die Quantenkryptographie ebnen.

Nachdenklich stimmt, dass das Quantenkryptographie-Startup ID Quantique aus der Schweiz von SK Telecom aus Südkorea gekauft wurde.

i Siehe https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html
ii https://www.iarpa.gov/index.php/research-programs/logiq
iii „Supporting quantum technologies beyond H2020“, https://qt.eu/app/uploads/2018/05/Supporting-QT-beyond-H2020_v1.1.pdf
iv Siehe vorherige Endnote; außerdem http://qurope.eu/manifesto ; https://arxiv.org/abs/1712.03773; https://ec.europa.eu/digital-single-market/en/news/quantum-flagship-high-level-expert-group-publishes-final-report;
v Publikationen des BSI u.a. https://www.bsi.bund.de/DE/Publikationen/BSI-Magazin/BSI-Magazin_node.html, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html, https://www.bsi.bund.de/SharedDocs/Termine/DE/2017/15DeutscherITSicherheitskongress.html