Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

Jan Dennis Gumz, Simon Sebastian Hunt, Michael Stemmer,
Sebastian Bock, Nikolay Tcholtchev, Denny Mattern,
Adrian Paschke, Marian Margraf

QUANTEN-IKT

Quantencomputing und Quantenkommunikation

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Jan Dennis Gumz, Simon Sebastian Hunt,
Dr. Michael Stemmer,Sebastian Bock,
Dr. Nikolay Tcholtchev, Denny Mattern,
Prof. Dr. Adrian Paschke (Fraunhofer FOKUS)
Prof. Dr. Marian Margraf (Fraunhofer AISEC)

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-948582-12-8

1. Auflage Januar 2022

Bildnachweise:

Seiten	Autoren	Quellen	Bearbeitung
1	insspirito	pixabay.com	geändert am 30.11.2021
10	insspirito	pixabay.com	geändert am 30.11.2021
29	insspirito	pixabay.com	geändert am 30.11.2021
36	insspirito	pixabay.com	geändert am 30.11.2021
40	insspirito	pixabay.com	geändert am 30.11.2021

VORWORT

Quantentechnologie verspricht, Bereiche der Informationsverarbeitung und -übermittlung grundlegend zu verändern. Tatsächlich ist Quanten-IKT bereits heute relevant: Viele der derzeit alltäglich genutzten kryptografischen Verfahren wie z. B. E-Mail-Verschlüsselung und digitale Signaturen sind nur scheinbar sicher, denn Quantencomputer besitzen das Potenzial, diese in sehr kurzer Zeit zu überwinden.

Quanten-IKT, welche Quantencomputing und Quantenkommunikation umfasst, stellt jedoch nicht nur eine Bedrohung dar. Abhörsicherheit könnte durch Quantenkommunikation garantiert sein, ganz unabhängig davon, welche zukünftigen Entwicklungen noch kommen. Quantencomputer sollen zudem Probleme lösen, bei denen klassische Computer scheitern, z. B. die individuelle Gestaltung von Medikamenten für Patient:innen. Außerdem könnten sich Quantencomputer als Treiber für wesentlich leistungsstärkere Künstliche Intelligenz erweisen.

Es ist daher nicht verwunderlich, dass weltweit umfangreiche finanzielle Ressourcen bereitgestellt und Initiativen gegründet werden, um Quantentechnologien voranzutreiben und skalierbare Quantencomputer zu entwickeln. Es hat sich ein regelrechter Quanten-Hype entwickelt.

Allerdings drohen Europa und Deutschland, im Quanten-Rennen den Anschluss an die USA und die VR China zu verlieren. Dabei befindet sich Deutschland mit seiner langen wissenschaftlichen Tradition in der Quantenphysik und einer starken Quantentechnologieforschung eigentlich in keiner schlechten Ausgangsposition. Um jedoch tatsächlich wettbewerbsfähig und souverän bezüglich Quanten-IKT zu sein, muss der Schritt zur Wertschöpfung gelingen.

Dieses White Paper will einen Beitrag dazu leisten, dass dies erfolgreich ist. Es stellt wesentliche Anwendungen der Quanten-IKT vor, bietet einen Überblick über die Quanten-IKT-Landschaft, legt realistische Entwicklungsperspektiven abseits von Hypes dar, benennt die wesentlichen Faktoren und Fallstricke bei der Gestaltung von Quanten-IKT und zeigt Handlungsoptionen auf.

Wir wünschen eine erkenntnisreiche Lektüre!

Ihr Kompetenzzentrum Öffentliche IT

INHALTSVERZEICHNIS

1. THESEN

Quantencomputing ist ein Game Changer.

Es existieren Aufgaben, bei denen klassische Rechner an fundamentale Grenzen stoßen. Dazu gehört etwa die Simulation chemischer Reaktionen, was zum Beispiel für die Entwicklung langlebigerer Batterien relevant ist. Schon bei kleinen Problemgrößen übersteigen die erforderlichen Rechenressourcen die Möglichkeiten klassischer Rechner. Quantenrechner eignen sich dagegen aufgrund ihrer quantenmechanischen Funktionsweise deutlich besser für solche Simulationen. Quantenrechner bieten hier und in Bereichen wie der Optimierung und der Künstlichen Intelligenz (KI) Chancen auf drastische Fortschritte und besitzen daher auch ein hohes Potenzial für eine kommerzielle Wertschöpfung oder für gesamtgesellschaftliche Aufgaben wie den Kampf gegen den Klimawandel.

Klassische IKT wird durch Quantencomputing und Quantenkommunikation ergänzt, nicht ersetzt.

Quanten-IKT ist nicht einfach die Weiterentwicklung klassischer IKT. Es handelt sich um eine Technologie, die sich grundlegend von der klassischen IKT unterscheidet, z. B. bezüglich der Informationseinheiten und der Datenverarbeitung. Quanten-IKT ist in einigen Bereichen deutlich stärker als klassische IKT, z. B. bei der Simulation chemischer Prozesse, in einigen Bereichen aber auch deutlich schwächer, etwa bei der langfristigen Speicherung von großen Datenmengen. Quanten-IKT wird daher neue Möglichkeiten eröffnen, die klassische IKT aber nicht generell ablösen, sondern ergänzen und unter anderem zu hybriden Ansätzen führen. Auf absehbare Zeit werden Quantenrechner nicht zu Heim- oder Bürorechnern werden. Ähnlich wie Supercomputer werden sie als Dienst für Wirtschaft und Wissenschaft zur Verfügung stehen.

Quanten revolutionieren die Verschlüsselung.

Quantencomputer stellen eine Bedrohung für die Datenvertraulichkeit dar: Es existieren Algorithmen für Quantencomputer, die versprechen, etablierte und weit verbreitete kryptografische Verfahren in kurzer Zeit zu überwinden. Hinderungsgrund ist lediglich die Hardware, die noch nicht die erforderliche Leistungsfähigkeit erreicht hat. Als Bereich der Quanten-IKT bietet die Quantenkommunikation hier allerdings auch eine Chance. Beim Informationsaustausch auf Basis von Quantenkommunikation ist es unmöglich, Abhörversuche zu verbergen. Quantenkommunikation bietet daher die Möglichkeit, ein bisher unerreichtes Sicherheitsniveau bei der Übertragung von Daten zu erreichen.

Quanten sind politisch.

Mit ihrem Potenzial für erhebliche, teilweise disruptive Auswirkungen auf breite Bereiche von Wirtschaft, Gesellschaft und Staat weist Quanten-IKT die Kennzeichen einer Schlüsseltechnologie auf. Dies betrifft mit der Fähigkeit, praxistaugliche Quantenrechner zu bauen oder zu betreiben, die digitale Souveränität. Wenn Deutschland und Europa hier stark auf andere Staaten und Wirtschaftsräume angewiesen sind, dann bedeutet dies auch eine starke Abhängigkeit der europäischen Wirtschaft und Forschung, was wiederum generell die Handlungsfähigkeit der Politik einschränken würde. Zudem steht die Kontrolle über die Sicherheit der eigenen Datenübertragungen auf dem Spiel. Die Entwicklung von Quanten-IKT ist also auch für die zukünftigen Handlungsspielräume Deutschlands und Europas relevant.

Quantencomputing ist eine Wette.

Expert:innen gehen davon aus, dass Quantencomputing innerhalb von zehn bis zwanzig Jahren seine Praxistauglichkeit in der Breite erreichen wird. Vorausgesetzt wird dabei ein starkes Wachstum in der Leistungsfähigkeit der Hardware, z. B. gemessen in Anzahl der Qubits eines Quantencomputers. Der Weg dorthin ist jedoch keineswegs gesichert. So ist bislang beispielsweise noch nicht erkennbar, welche der derzeit diskutierten Konstruktionsweisen für Quantencomputer sich letztlich durchsetzen werden. Insgesamt existieren bis zur breiten Praxisreife noch viele unbewältigte Hürden und offene Fragen. Die aktuelle Wette auf Quantencomputing beinhaltet daher zum gegenwärtigen Zeitpunkt zwar erhebliche Chancen, aber auch ein nicht zu verschweigendes Risiko.

Die Karten werden jetzt gemischt.

Während die breite Praxistauglichkeit von Quantencomputing und -kommunikation noch aussteht, hat das Ringen um zukünftige Marktanteile bereits begonnen. Die Wertschöpfung wird bereits vorbereitet und hat vereinzelt bereits begonnen. Derzeit werden gleichzeitig wesentliche Grundlagen erarbeitet, wie etwa durch geeignete Hardware und spezielle Programmier-

sprachen, und Anwendungen vorbereitet, wie etwa durch die Identifikation von Einsatzbereichen und die Entwicklung funktionstüchtiger Algorithmen. Weder einzelne Staaten noch Unternehmen besitzen bislang eine uneinholbare Vormachtstellung.

Quantensprünge sind keine reine Hardwarefrage.

Die Entwicklung und die Praxistauglichkeit von Quanten-IKT sind nicht allein von Fortschritten bei der Hardware abhängig. Auch Software, Standards und Plattformen sind von großer Bedeutung. Beispielsweise mangelt es an Standards zur Bewertung der Leistungsfähigkeit und zur Gewährleistung der Kompatibilität von Quanten-IKT-Lösungen. Um bei der Quanten-IKT den Weg von der Theorie zur Praxis zu gehen, braucht es zudem Spezialist:innen, die sowohl die quantenphysikalischen und mathematischen Grundlagen beherrschen, als auch über Kenntnisse im Bereich der Elektrotechnik und der Informatik verfügen. Da Quanten-IKT eine neue Technologie ist, existieren bisher kaum Ausbildungen, die die erforderlichen Kenntnisse aus den unterschiedlichen Disziplinen bündeln. Die vorhandenen Fachkräfte haben sich die erforderlichen Kenntnisse der ihnen ursprünglich fremden Disziplinen oftmals selbstständig erarbeitet und sind auf dem Arbeitsmarkt entsprechend hart umkämpft. Mit dem Wachstum der Branche wird die Nachfrage nach Spezialist:innen weiter steigen. Auch Entscheider:innen in Wirtschaft und Verwaltung brauchen gewisse Grundkenntnisse, um Bereiche identifizieren zu können, in denen sich durch Quanten-IKT Chancen oder Risiken ergeben, und um frühzeitig geeignete Maßnahmen zu ergreifen.

2. KLASSISCHE IKT UND QUANTEN-IKT

2.1 KLASSISCHE RECHNER UND IHRE GRENZEN

Erfolgsgeschichte und Siegeszug des Computers seit seiner Erfindung in der Mitte des letzten Jahrhunderts sind legendär. Speicher-, Übertragungs- und Rechenkapazität wachsen seit nunmehr etwa achtzig Jahren ungebrochen exponentiell, d. h. sie verdoppeln sich gemäß dem bereits 1965 vorhergesagten »Moore's Law«[1] jeweils innerhalb von ein bis zwei Jahren. Mittlerweile durchdringen und prägen der Computer und die mit ihm verbundene Kommunikationstechnologie nicht nur fast alle Technikbereiche, sondern auch Arbeit und Freizeit von uns allen. Sie sind zum Motor einer digitalen Transformation von Wirtschaft wie Gesellschaft geworden, die vom Umfang her den Vergleich mit der industriellen Revolution nicht zu scheuen braucht.

All dieser Fortschritt beruht bislang weitgehend auf dem klassischen Rechnermodell. Informationen werden digital als Bits und Bytes repräsentiert, gespeichert, übertragen und verarbeitet. Wenn diese Technologie so unvergleichlich erfolgreich ist und sich überdies bis heute exponentiell verbessert, warum lohnt dann dennoch die Beschäftigung mit alternativen Informations- und Kommunikationstechnologien, insbesondere mit Quantencomputing und Quantenkommunikation?

Die Antwort ist schlicht: Das klassische Rechnermodell hat seine Grenzen. Die Informatik beschäftigt sich seit ihrem Beginn in ihren Teildisziplinen u. a. mit Komplexitäts- und Berechenbarkeitstheorien. Während es bei Berechenbarkeit darum geht, ob ein Problem überhaupt prinzipiell lösbar ist – unabhängig vom Rechnermodell und einer konkreten Hard- und Software – strukturiert die Komplexitätstheorie die von Computern prinzipiell lösbaren Probleme in verschiedene sogenannte Komplexitätsklassen. Für einfach- bis mittelkomplexe Probleme ist der klassische Rechner – vereinfacht gesagt – unschlagbar. Die meisten Probleme, die wir heute mit dem Computer lösen, fallen in diese Komplexitätsklassen. Hierzu zählen z. B. Textverarbeitung, Videokonferenzen, Telefonieren und vieles mehr. Es gibt aber eben auch für die Praxis relevante hochkomplexe Probleme, die zwar prinzipiell durch Computer gelöst werden können, für die klassische Computer allerdings an ihre Grenzen stoßen. Hierzu zählen z. B. die Primfaktorzerlegung, die u. a. in der Kryptografie eine zentrale Rolle spielt, sowie aufwendige Simulationen, wie z. B. die Simulation chemischer Reaktionen.

[1] https://de.wikipedia.org/wiki/Mooresches_Gesetz

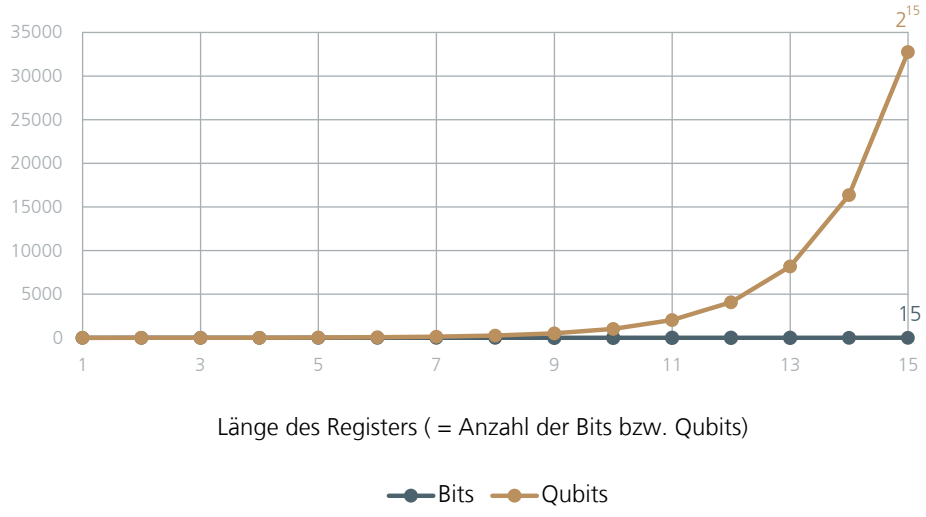


Abbildung 1: Anzahl der gleichzeitig repräsentierten Daten (Binärwerte)

Man versucht in der Regel, die Grenzen dieser Probleme mit besonders leistungsfähiger Hardware – Stichworte: Supercomputer, High-Performance-Computing – zu erweitern. Da diese Probleme jedoch häufig exponentieller Natur sind, lassen sich deren Grenzen auf einem klassischen Rechner selbst mit massiver Leistungserhöhung jeweils nur um eine begrenzte Anzahl an Schritten hinausschieben und daher ab einer gewissen Größe prinzipiell nicht mehr in einer akzeptablen Zeitspanne lösen.

2.2 ÜBERLEGENHEIT DER QUANTEN-IKT

Der Quantencomputer unterscheidet sich vom klassischen Rechner durch ein grundsätzlich anderes Rechenmodell. Statt durch Bits werden Informationen in ihm durch sogenannte Qubits repräsentiert (mehr zu Qubits in Kapitel 4). Während die Größe des Datenraums[2] eines klassischen Rechners mit der Anzahl der Bits linear zunimmt (mit 8 Bits lässt sich beispielsweise ein Zeichen darstellen, mit 16 Bits sind es zwei Zeichen usw.), steigt sie beim Quantencomputer mit der Anzahl der Qubits exponentiell. Berechnungen mit Qubits erfolgen aufgrund der besonderen Eigenschaften der Quantenmechanik zudem nicht wie im klassischen Rechenmodell inhärent sequenziell, sondern inhärent parallel.

Durch diese grundsätzlichen Unterschiede erschließt der Quantencomputer prinzipiell eine höhere Komplexitätsklasse von Problemen einer effizienten Lösung, als dies dem klassischen Rechner möglich ist. Für die Faktorisierung großer Zahlen bedeutet das beispielsweise, dass viele heutige, gegenüber dem klassischen Rechenmodell noch sichere kryptografische Verfahren in Zukunft möglicherweise durch den Einsatz von Quantencomputern geknackt werden können. Hierin steckt insbesondere eine Schwäche klassischer Kommunikationstechnologie, deren Sicherheit an die Limitationen des klassischen Rechnermodells gekoppelt ist. Bei quantenbasierter Kommunikationstechnologie ist dies nicht der Fall (mehr dazu in Kapitel 3.4).

Quanten-IKT beinhaltet zudem Quantenphänomene, bei denen derzeit davon ausgegangen wird, dass sie echt zufällig sind. Deshalb ist Quanten-IKT probabilistisch, während die klassische IKT deterministisch ist. Hieraus ergeben sich überall da mögliche Vorteile für die Quanten-IKT, wo echter Zufall gefragt ist, etwa bei der Generierung von Zufallszahlen für Simulationen.

2.3 ÜBERLEGENHEIT DER KLASSISCHEN IKT

Der theoretischen Überlegenheit des Rechenmodells des Quantencomputers im Vergleich zum klassischen Rechner stehen in der Praxis jedoch eine Reihe von Einschränkungen, Nachteilen und Herausforderungen gegenüber.

So ist zunächst eine Bereitstellung und Auswertung der Daten durch klassische Rechner erforderlich, um Quantenalgorithmen anwenden und ihre Ergebnisse interpretieren zu können. Außerdem eignen sich nur bestimmte, aber nicht alle hochkomplexen Probleme für eine (dann jedoch deutlich) effizientere Lösung auf dem Quantencomputer. Zudem ist es schwierig, ein System aus mehreren Qubits zu erzeugen und hinreichend lange stabil zu halten, um überhaupt relevante Berechnungen durchführen zu können.

Quantentechnologie ist außerdem sensitiver gegenüber Umwelteinflüssen als herkömmliche Technologien. Diese Sensitivität ermöglicht zwar deutliche Fortschritte bei der Präzision von Messtechnik, weshalb hier auch ein großes Forschungsinteresse besteht, für Quanten-IKT ist die Empfindlichkeit aber meist ein Nachteil. Bei der Quantenkommunikation schränkt diese Empfindlichkeit zudem die Wege und Distanzen ein, auf denen Informationen übertragen werden können.

Aufgrund dieser Einschränkungen ist der klassische Rechner dem Quantencomputer zum heutigen Zeitpunkt in der Praxis bis auf erste wenige Beispiele noch durchweg überlegen. Auch wenn es gelingt, in den nächsten Jahren und Jahrzehnten große und stabile Systeme mit mehreren Tausend oder gar Millionen Qubits zu entwickeln, so wird der Quantencomputer den klassischen Rechner nicht verdrängen, sondern für bestimmte (allerdings hoch relevante) Problemklassen ergänzen. So ist der Quantencomputer dem klassischen Rechner zwar wie geschildert z. B. bei der Zerlegung von großen Zahlen in ihre Primfaktoren überlegen, für die Multiplikation von Zahlen gilt jedoch das Umgekehrte – hier ist der klassische Rechner dem Quantencomputer überlegen. Zu weiteren Aufgaben, die klassische IKT gut bewältigen kann und in denen sie der Quanten-IKT überlegen ist, gehören etwa das langfristige Speichern, das Kopieren und die Übertragung von Daten bezüglich Kriterien wie Ge-

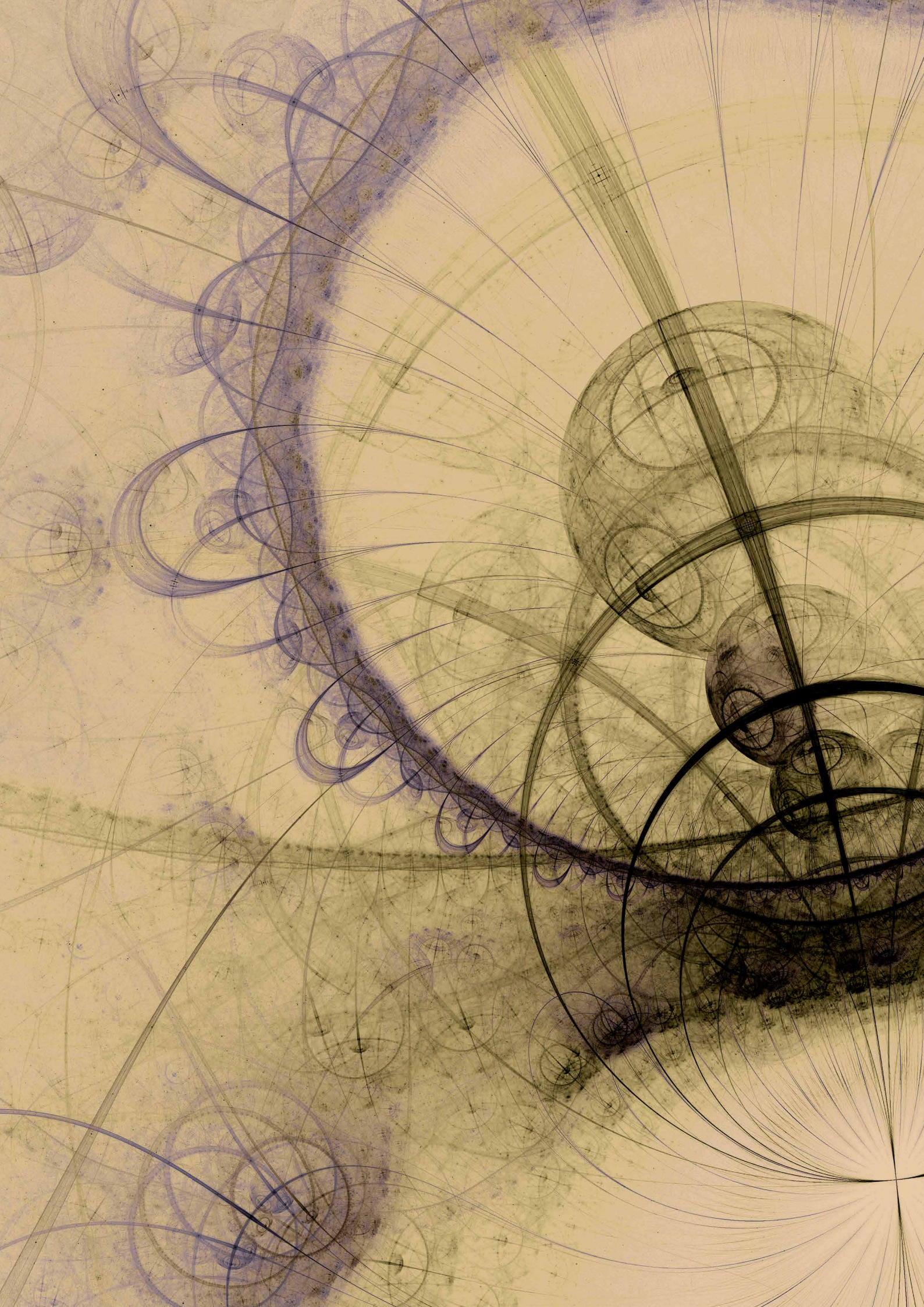
[2] Der Datenraum ist nicht mit dem Zustandsraum zu verwechseln. Die Anzahl der darstellbaren Zustände wächst bereits im klassischen Modell exponentiell mit der Speichergröße, die Anzahl der darstellbaren Daten hingegen nur linear.

schwindigkeit, Zuverlässigkeit, Datenumfang und große Entfernung. Zudem können für die klassische Übertragung im Gegensatz zur Quantenkommunikation auch Wege wie Kupferkabel oder Radiowellen genutzt werden.

Für die meisten Aufgaben, für die heute Computer genutzt werden, wird daher das klassische Rechenmodell das Maß der Dinge bleiben, welches allerdings in der Zukunft möglicherweise für wichtige Spezialaufgaben durch die Fähigkeiten von Quantencomputern ergänzt wird.

	Klassische IKT	Quanten-IKT
Daten/Speicher	Bits	Qubits
System	deterministisch	probabilistisch
Erweiterung des Datenraums durch Vergrößerung des Speichers	linear	exponentiell
Berechnungen	inhärent sequenziell, begrenzte Parallelisierungsmöglichkeiten	inhärent parallel
Geeignete Komplexitätsklassen	einfach bis mittel	hoch bis sehr hoch
Störungsanfälligkeit	gering	hoch
Praxisreife	Bereits seit mehreren Jahrzehnten gegeben	Von Experten in ca. 10 – 20 Jahren in der Breite erwartet, erste kommerzielle Anwendungen bereits verfügbar, z. B. Generierung echter Zufallszahlen, Quanten-Schlüsselaustausch

Tabelle 1: Einige charakteristische Eigenschaften von klassischer IKT und Quanten-IKT im Vergleich



3. ANWENDUNGEN

3.1. SIMULATION

Simulationen bezeichnen (oftmals rechnergestützte) Experimente an einem Modell, also einem vereinfachten Abbild der Realität, mit dem Ziel des Erkenntnisgewinns. Simulationen sind besonders interessant, wenn Experimente in der Realität unmöglich oder zu aufwändig sind.

Oftmals werden Ergebnisse von Simulationen nicht nur in Form von Zahlen ausgegeben, sondern auch grafisch aufbereitet, wodurch sich Erkenntnisse direkt ablesen lassen. So zum Beispiel bei der Simulation von Strömungen an Fahrzeugen oder Tragflächen von Flugzeugen.

Die Durchführung von Simulationen unterliegt verschiedenen Einschränkungen. Die Komplexität oder die Natur eines Prozesses lassen eine 1:1-Simulation aufgrund der gegebenen Rechenkapazitäten häufig nicht zu. Entsprechend muss zwischen Genauigkeit und den für die Simulation erforderlichen Rechenressourcen wie Laufzeit oder Speicherplatz abgewogen werden. Je nach Anwendungsfall kann dies bedeuten, dass bewusst Ungenauigkeiten in Kauf genommen werden, um die Simulation in einer gewissen Zeit ausführen zu können.

Im Bereich der Simulation kommt Quantentechnologien an verschiedenen Stellen eine Bedeutung zu.

3.1.1 Simulation klassischer Systeme durch Quantencomputer

Systeme der klassischen Physik beschreiben z. B. Wärmeleitung oder Strömungen. Diese Systeme sind aus ingenieurwissenschaftlicher Perspektive z. B. für die Produktion hochwertigen Stahls (Wärmeleitung) oder bei der Entwicklung von Fahr- und Flugzeugen (Strömung) relevant. Diese Systeme werden oft in Form von sogenannten partiellen Differenzialgleichungen beschrieben. Diese Gleichungen geben an, wie sich Eigenschaften eines Systems über Zeit und Ort in Abhängigkeit eines Einflussfaktors, etwa einer Wärmequelle, verändern. Partielle Differenzialgleichungen lassen sich meist nicht von Hand, sondern nur per Computer lösen. Die Lösungen zu diesen Gleichungen sind allerdings notorisch schwer zu berechnen, die gewünschte Genauigkeit der Lösung und damit Simulation steht oftmals in Konflikt mit den dafür erforderlichen Rechenressourcen. Entsprechend ist die effiziente Lösung dieser Gleichungen ein Dauerthema der Mathematik. In letzter Zeit werden immer häufiger Quantencomputer und Quantenalgorithmen als Möglichkeit für deutliche Fortschritte in Betracht gezogen. Bekannt ist hier unter anderem[3] z. B. der HHL-Algorithmus. Voraussetzung ist hier die Annährung der partiellen Differentialgleichungen durch ein lineares Gleichungssystem. Dies ist von jeher ein üblicher Schritt bei der computergestützten Lösung von partiellen Differentialgleichungen. Ein lineares Gleichungssystem kann ein Quantencomputer unter Umständen exponentiell schneller lösen als ein klassischer Rechner[4] und verspricht daher einen insgesamt deutlich schnelleren Simulationsvorgang bei typischen Systemen der klassischen Physik. Der hohe Bedarf an Quantenressourcen des HHL-Algorithmus rückt diese Anwendung für die Praxis aber noch in weite Ferne.[5]

3.1.2 Quantensysteme simulieren

Klassische Computer kommen bei der Simulation von Quantensystemen recht schnell an ihre Grenzen. Neben dem allgemeinen probabilistischen Charakter der Quantenphänomene lassen sich insbesondere Vielteilchensysteme oft nur schwer exakt mit klassischen Rechnern nachbilden. Diese Systeme zeichnet aus, dass sie aus vielen einzelnen Quantenobjekten bestehen, die stark miteinander korrelieren und gemeinsam teilweise emergente Verhaltensweisen aufzeigen. Die Rechenressourcen klassischer Rechner reichen meist maximal für die Simulation sehr kleiner Quantensysteme unterhalb der Praxisrelevanz aus. Dies wird sich auf absehbare Zeit auch nicht ändern, das Problem besteht darin, dass klassische Rechner prinzipiell nicht gut darin sind, Quantensysteme nachzubilden und Vorgänge bei diesen zu simulieren.[6]

---

[3] García-Molina, P.; Rodríguez-Mediavilla, J; García-Ripoll, J. J. (2021): »Solving partial differential equations in quantum computers«. https://arxiv.org/abs/2104.02668v2. Zuletzt abgerufen: 18.08.2021.

[4] Harrow, A. W.; Hassidim, A; Lloyd, S. (2009): »Quantum Algorithm for Linear Systems of Equations«. https://arxiv.org/abs/0811.3171v3.
Zuletzt abgerufen: 15.11.2021.

[5] Stollenwerk, T. (2021):»Umfeldstudie Quantencomputing«, S. 25 ff, https://www.dlr.de/content/de/downloads/publikationen/broschueren/2021/umfeldstudie-quantencomputing.pdf?__blob=publicationFile&v=2.
Zuletzt abgerufen: 15.11.2021.

[6] Hintergrund ist, dass die Komplexität von Quanten-Vielteilchensystemen exponentiell mit der Anzahl der Teilchen steigt, die klassischen Ressourcen jedoch nur linear. Vergleiche auch Abbildung 1 in Kapitel 2.

Daher entstand die Idee, für zu simulierende Quantensysteme ein gut kontrollierbares quantenphysikalisches Referenzsystem zu nutzen. Solche Referenzsysteme können als spezialisierte Maschine gebaut werden, also als Quantensimulator. Allerdings kann auch ein weniger spezialisierter Quantencomputer aufgrund seiner quantenphysikalischen Natur zur Simulation genutzt werden. Tatsächlich mündete die Idee eines Quantensimulators schließlich in der Überlegung, Allzweckquantencomputer zu entwickeln, also Quantenrechenmaschinen, die vielseitiger programmierbar sind und neben der Simulation auch für andere Aufgaben genutzt werden können. Der Übergang zwischen Quantensimulatoren und Quantencomputern ist aufgrund des Entwicklungsstandes noch fließend.

Die grundlegende Anwendbarkeit von Quantensimulatoren für bestimmte Probleme ist neben der Theorie auch praktisch belegt[7], die gegenwärtige Herausforderung liegt vielfach bei der Wirtschaftlichkeit, Universalität und einer praxisrelevanten Skalierbarkeit der unterschiedlichen Ansätze.

3.1.3 Populäre Anwendungsgebiete

Derzeit finden Quantensimulatoren hauptsächlich Anwendung im Bereich der Grundlagenforschung. Die Technologie ist jedoch aufgrund ihres Potenzials für ein besseres Verständnis vieler gesellschaftlich relevanter Prozesse von Bedeutung. Chemie, Materialentwicklung und die Pharmaindustrie sind einige Bereiche, die von besseren Simulationen profitieren können. Insbesondere zwei Prozesse werden regelmäßig erwähnt, wenn es um Quantensimulatoren geht: Simulation von Molekülinteraktionen für die Medikamentenentwicklung und eine effizientere Gestaltung der Produktion von Ammoniak.

Bei der Entwicklung von Medikamenten ist es oft entscheidend, die Interaktionen von körpereigenen Molekülen, bspw. Eiweißen, und medizinischen Wirkstoffen zu verstehen. Diese Interaktionen sind hochgradig von Quanteneffekten abhängig und lassen sich nur schwer klassisch simulieren. In der Praxis muss entsprechend mit einem breiteren Portfolio an möglichen Wirkstoffen in den klinischen Teil der Medikamentenentwicklung gegangen werden, da sich der Kreis vielversprechender Kandidaten nicht ausreichend eingrenzen lässt. Dies kostet Zeit und Geld.

Im Bereich der Chemie und insbesondere der Düngemittelsynthese spielt Ammoniak eine herausragende Rolle. Den Kern der industriellen Ammoniaksynthese bildet das Anfang des 20. Jahrhunderts entwickelte Haber-Bosch-Verfahren. Hierbei wird unter hohen Temperaturen und hohem Druck Wasser und atmosphärischer Stickstoff in Ammoniak umgewandelt, was als einzelner Prozessschritt allein 1 – 2 Prozent des Weltenergieverbrauchs beansprucht[8]. Deshalb ist auch vor dem Hintergrund des Klimawandels ein besseres Verfahren interessant. Die Natur schafft die Synthese in bestimmten Mikroorganismen über Stickstoff-Fixierung mittels des Enzyms Nitrogenase deutlich energieeffizienter. Das notwendige Verständnis, um dieses komplexe Eiweißmolekül bzw. den enthaltenen chemischen Prozess biotechnisch nutzbar zu machen, konnte bisher durch kein klassisches Verfahren gewonnen werden. Hier wird Hoffnung in Erkenntnisse aus Quantensimulationen gesetzt.

3.2. OPTIMIERUNG

Optimierung ist allgegenwärtig und tief verwurzelt in Wirtschaft, öffentlicher Verwaltung und Zivilgesellschaft. Zum Beispiel kann es darum gehen, qualitativ hochwertigere Produkte als die Wettbewerber anzubieten, die Kosten der Leistungserbringung der öffentlichen Verwaltung zu senken oder den eigenen Tagesablauf so zu organisieren, dass maximal viel Zeit für Hobbys, Freunde und Familie bleibt. Als Fachgebiet der Mathematik bietet die Optimierung die Möglichkeit, eine Aufgabe als mathematisches Problem zu modellieren und mittels bewährter Verfahren das Optimum zu ermitteln. Immer leistungsstärkere Computer und verbesserte Algorithmen haben dafür gesorgt, dass immer umfangreichere und komplexere Aufgaben in akzeptabler Zeit gelöst werden können.

3.2.1 Probleme und Lösungsmöglichkeiten

Mathematische Optimierungsprobleme lassen sich in verschiedene Typen mit unterschiedlichen Lösungsverfahren einteilen. Während klassische Computer bei einigen dieser Typen sehr leistungsfähig sind, existieren auch Problemtypen, mit denen

[7] Hempel, C. et al. (2018): »Quantum Chemistry Calculations on a Trapped-Ion Quantum Simulator«. https://doi.org/10.1103/PhysRevX.8.031022. Zuletzt abgerufen: 19.08.2021.

[8] Höhere Schätzung bspw. bei Fernandez, A. F.; Hatzell, M. C. (2020): »Economic Considerations for Low-Temperature Electrochemical Ammonia Production: Achieving Haber-Bosch Parity«. https://doi.org/10.1149/1945-7111/abc35b. Zuletzt abgerufen: 19.08.2021; Niedrige Schätzung zitiert vom Wissenschaftlichen Dienst des Bundestages (2018): »Energieverbrauch bei der Produktion von mineralischem Stickstoffdünger«, AZ WD 8 – 3000 – 088/18.; Nennung des Bereichs bei Kyriakou, V. et.al. (2019): »An Electrochemical Haber-Bosch Process«. https://doi.org/10.1016/j.joule.2019.10.006. Zuletzt abgerufen: 19.08.2021.

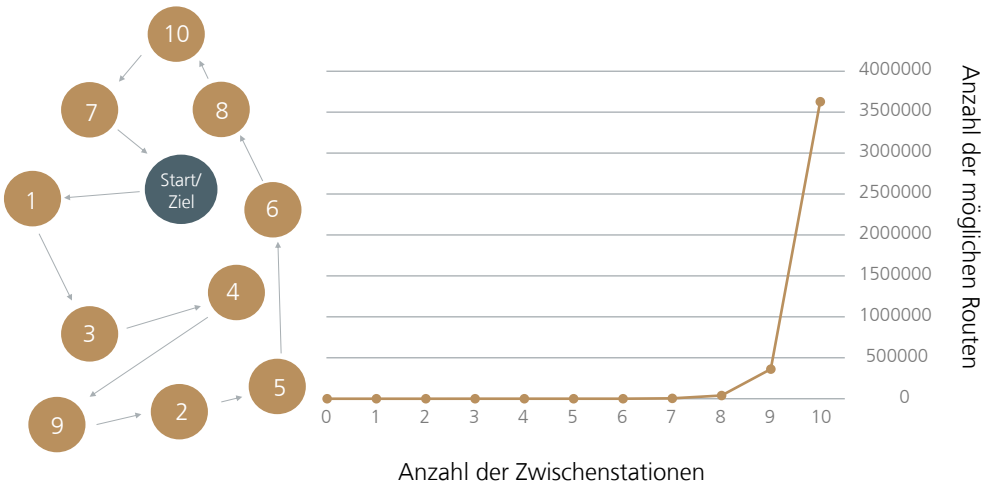


Abbildung 2: Bei 10 Zwischenstationen ist das Problem der optimalen Rundreise (mitsamt einer Lösungsmöglichkeit) noch gut darstellbar (links), allerdings existieren bereits mehr als 3,5 Millionen Lösungsmöglichkeiten (rechts).

sich klassische Rechner außerordentlich schwertun. Als Beispiel sei das Rundreiseproblem (englisch: Travelling Salesman Problem) genannt: Ausgehend von einem festgelegten Startpunkt soll durch eine festgelegte Menge von Zwischenstationen gereist werden. Jede der Zwischenstationen soll dabei einmal besucht und am Ende der Startpunkt wieder erreicht werden. Die Reihenfolge, in der die Zwischenstationen besucht werden, ist frei wählbar und kann optimiert werden, z. B. bei Lieferprozessen hinsichtlich der Dauer oder der Treibstoffkosten. Während die Problemformulierung einfach ist, erweist sich die Lösung mit zunehmender Anzahl an Zwischenstationen als extrem schwierig. Verantwortlich hierfür ist die sogenannte kombinatorische Explosion. Beim Problem der Rundreise wächst die Anzahl der möglichen Reihenfolgen von Stationen, sprich der Lösungsmöglichkeiten, sogar stärker als exponentiell, nämlich entsprechend der Fakultätsfunktion mit der Anzahl der Stationen. Um die optimale Lösung zu finden, müssen mitunter alle Lösungsmöglichkeiten überprüft werden. Aus diesem Grund ist der Ressourcenaufwand klassischer Algorithmen enorm, teilweise auch so groß, dass das Optimum nicht in akzeptabler Laufzeit ermittelt werden kann. Daher sind bei schweren Optimierungsproblemen auch sogenannte Approximationsalgorithmen populär. Solche Algorithmen ermitteln Näherungslösungen, d. h. gute, wenn auch suboptimale Lösungen, dies allerdings in weniger Laufzeit als echte Optimierungsverfahren.

3.2.2 Optimierung mit Quantencomputern

Es besteht eine große Nachfrage nach Algorithmen, die hinsichtlich der Ressourceneffizienz und Optimalität besser als herkömmliche Algorithmen sind, um so umfangreichere Probleme zu lösen und dies am besten auch schneller. Dies ist z. B. relevant für Echtzeitanwendungen. Bei schweren Problemen wie etwa dem Rundreiseproblem stoßen klassische Rechner jedoch an Grenzen, sie können schlichtweg nicht mit dem Wachstum der Ressourcenanforderungen mithalten. Und genau das könnte bei Quantenrechnern anders sein. Die Anzahl der gleichzeitig überprüfbaren Lösungsmöglichkeiten wächst deutlich stärker mit der Anzahl von Qubits eines Quantenrechners als mit der Anzahl von Bits eines klassischen Rechners. Dies öffnet die Tür zur schnelleren Lösung umfangreicherer Probleme.

3.2.3 Perspektive und Anwendungen

Für die Lösung von Optimierungsproblemen kommen verschiedene Typen von Quantencomputern infrage (mehr zu diesen Typen in Kapitel 4). Es werden verschiedene Algorithmen entwickelt und erprobt, bisher wurde die Performanz klassischer Rechner allerdings nicht eindeutig übertroffen. Das Vertrauen, dass Quantencomputer die Leistungsfähigkeit klassischer Rechner bei der Verarbeitung einiger Optimierungsproblemtypen zukünftig deutlich übertreffen werden, ist groß und äußert sich z. B. in der Gründung von spezialisierten Start-ups und oder dem Engagement großer Unternehmen, die z. B. versuchen, Anwendungsmöglichkeiten zu identifizieren und teilweise auch schon die Wertschöpfung vorbereiten. Airbus möchte über die optimierte Auslastung und das optimierte Design von Flugzeugen die Treibstoffeffizienz erhöhen.[9] Angesichts der niedrigen Gewinnmargen in der Luftfahrtindustrie können schon kleine Vorteile große Auswirkungen auf diesen Wirtschaftszweig

[9] https://www.airbus.com/innovation/industry-4-0/quantum-technologies/airbus-quantum-computing-challenge.html. Zuletzt abgerufen am 14.12.2020.

haben. VW beschäftigt sich im Rahmen eines Projekts mit der Optimierung des Verkehrsflusses – für jeden Bus einer ganzen Flotte soll z. B. bei Staus die individuell optimale Route nahezu in Echtzeit ermittelt werden.[10] Ein weiterer Anwendungsfall ist die Optimierung von Portfolios. Tatsächlich könnte die Anwendung von Quantencomputern in der Finanzindustrie früher als in anderen Bereichen wie Medizin oder Flugzeugdesign zur Wertschöpfung beitragen, da vor dem Praxiseinsatz von Finanzlösungen weniger ausgiebige Tests akzeptabel sind.

3.3. KÜNSTLICHE INTELLIGENZ

In den vergangenen zehn Jahren haben Verfahren der Künstlichen Intelligenz Einzug gehalten in die verschiedensten Bereiche des menschlichen Lebens. Dabei geht es gegenwärtig hauptsächlich um Methoden aus dem Bereich des Maschinellen Lernens. So untersuchen Bilderkennungsalgorithmen medizinische Aufnahmen und dank Sprachassistenten gleicht die Bedienung technischer Geräte einer Alltagsszene aus einem Science-Fiction-Film. Um diese Funktionalitäten zu entwickeln, müssen die KI-Algorithmen zunächst mit vielen Daten trainiert werden. Ein solcher Trainingsprozess ist ein Optimierungsproblem, bei dem die optimale Lösung allerdings schrittweise approximiert wird. Das macht das Training von KI-Algorithmen mit großen Datenmengen zeitaufwändig und sehr ressourcenintensiv.

In der Forschung arbeitet man daran, das Potenzial von Quantencomputern für das Maschinelle Lernen nutzbar zu machen. Beispielsweise basiert ein wesentlicher Teil der Algorithmen, die im Maschinellen Lernen Anwendung finden, auf mathematischen Objekten und Operationen aus dem Gebiet der Linearen Algebra, wie etwa Matrizen. Es wurden bereits Quantenalgorithmen vorgeschlagen, die einen bedeutenden Geschwindigkeitsvorteil etwa bei der Matrixinversion auf Quantencomputern erreichen können.

Gleichwohl haben heutige Quantencomputer noch mit vielen technischen und physikalischen Hürden zu kämpfen, wodurch die Berechnungsergebnisse oftmals verrauscht und fehlerbehaftet sind. Man spricht daher von Noisy Intermediate-Scale Quantum Computing (NISQ). Da aber Algorithmen des Maschinellen Lernens vergleichsweise tolerant gegenüber verrauschten Daten sind, erscheinen die Verfahren des Maschinellen Lernens als eine vielversprechende Möglichkeit mit Quantencomputern relevante Problemstellungen auch außerhalb des akademischen Bereichs zu bearbeiten.

Ein Schwerpunkt der Forschung liegt derzeit bei der Entwicklung sogenannter hybrider quantenklassischer Algorithmen. Diese Algorithmen zerlegen ein Problem in einzelne Teilprobleme und nutzen sowohl die klassischen Computer mit ihren Prozessoren und Grafikkarten als auch Quantenhardware – je nachdem, welches Gerät am besten für ein Teilproblem geeignet ist. Zum Schluss werden die Ergebnisse der einzelnen Teilberechnungen in eine Gesamtlösung überführt. Einige der gängigen Softwaretools für Maschinelles Lernen unterstützen bereits die Anbindung von Quantenhardware.[11]

[10] https://www.volkswagen-newsroom.com/de/pressemitteilungen/volkswagen-optimiert-verkehrsfluss-mit-quantencomputern-5507.
Abgerufen am 14.12.2020.

[11] Z. B. PennyLane vom kanadischen Unternehmen Xanadu (https://pennylane.ai/) und Tensorflow Quantum von Google (https://www.tensorflow.org/quantum).

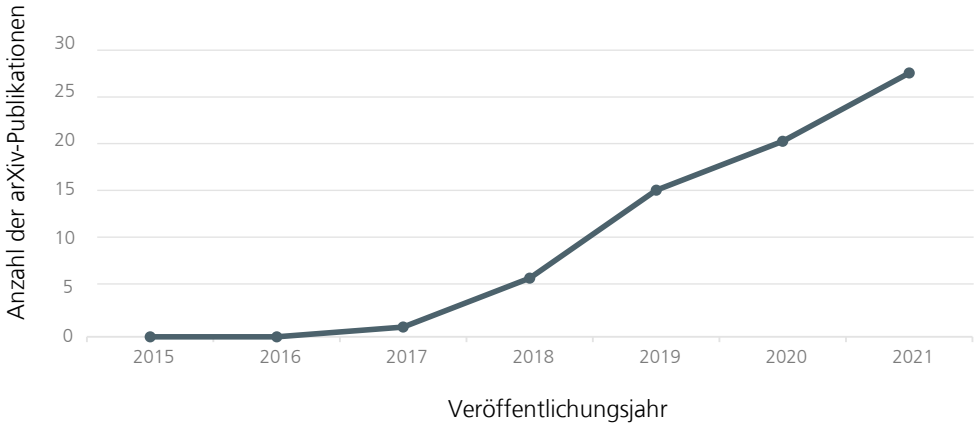


Abbildung 3: Wissenschaftliche Publikationen zu Variational Quantum Circuits

Ein weiterer wichtiger Forschungsgegenstand im Zusammenspiel von Maschinellem Lernen und Quantencomputern ist die Frage nach guten Architekturen von trainierbaren Quantenschaltungen (sogenannte variational quantum circuits), um diese etwa in Klassifikationsalgorithmen einzusetzen. Darüber hinaus wird intensiv an Verfahren für die effiziente Ein- und Ausgabe von Daten bei Quantencomputern geforscht.

3.4. ABHÖRSICHERE KOMMUNIKATION

Die klassische Kommunikationstechnologie[12] hat neue Möglichkeiten zur Übertragung von Information geschaffen, die sich stetig weiterentwickeln. Je nach Einsatzzweck muss eine technische Lösung verschiedene Anforderungen erfüllen, z. B. dass Daten störungsfrei, schnell, energieeffizient, über große Distanzen und in großen Mengen übertragen werden. Information ist oftmals schützenswert, d. h. bei der Übermittlung zwischen zwei oder mehr befugten Kommunikationspartnern sollte sie sich nicht durch Dritte abhören lassen. Dies betrifft zum Beispiel Bankgeschäfte, Patientendaten, Geschäftsgeheimnisse, Informationen zu kritischen Infrastrukturen und Kommunikation von Politiker:innen oder beim Militär.

Die klassische Kommunikationstechnologie bietet verschiedene Verfahren, um Schlüssel zu generieren und Information mit relativ geringem Aufwand zu verschlüsseln. Die erforderlichen Rechenressourcen, um eine Verschlüsselung in praktikabler Zeit zu überwinden, d. h. verschlüsselte Information zu entschlüsseln, ohne im Besitz des Schlüssels zu sein, übersteigen die aktuellen und absehbaren technischen Möglichkeiten klassischer IKT. Die Abhörsicherheit ist also nicht absolut, sondern an den Stand der Technik gebunden. Die technischen Möglichkeiten von Quantencomputern stellen die Sicherheit heutzutage weit verbreiteter klassischer Verschlüsselungsverfahren jedoch infrage (Mehr dazu auch in Kapitel 6.4).

Quanten-IKT bietet die Chance, Kommunikationstechnik auf ein bisher unerreichtes Sicherheitslevel zu heben. Ein wesentlicher Bestandteil verschlüsselter Kommunikation ist die Erzeugung einer Zeichenfolge, die als geheimer Schlüssel für die befugten Kommunikationspartner dient. Diese Zeichenfolge muss zufällig erzeugt werden, da andernfalls unbefugte Dritte den Schlüssel einfach erraten können. Weil klassische IKT deterministisch ist, werden externe Vorgänge, etwa Mausbewegungen, für die Erzeugung von zufälligen Zeichenfolgen genutzt. Für Quanten-IKT gilt dies nicht. Die derzeitigen Erkenntnisse aus der Quantenphysik gehen davon aus, dass die messbaren Phänomene von Quantenobjekten echten Zufall abbilden. Dies ermöglicht die Konstruktion von Quanten-Zufallsgeneratoren. Solche Generatoren lassen sich nicht nur für die Erzeugung geheimer Schlüssel, sondern auch für Simulationen (siehe Kapitel 3.1) nutzen, bei denen eher echter Zufall statt Reproduzierbarkeit gefragt ist.

Tatsächlich gehen die Möglichkeiten der Quanten-IKT bezüglich sicherer Kommunikation noch wesentlich über die Schlüsselerzeugung hinaus: Quantenkommunikationstechnologie ermöglicht die inhärent abhörsichere Übertragung von Information. Das Sicherheitslevel beruht hierbei auf quantenphysikalischen Gesetzmäßigkeiten und ist damit unabhängig von Rechenressourcen, die Dritten zu Verfügung stehen. Zum Beispiel ist es anders als bei einem (klassischen) Bit nicht möglich, den Zustand eines Qubits zu messen, ohne dessen Zustand zu verändern. Dadurch können Kommunikationspartner jeden Abhörversuch bemerken und entsprechend reagieren.

Im Bereich der Quantenkommunikationstechnologie ist der Quanten-Schlüssel-Austausch (englisch Quantum Key Distribution, kurz QKD) besonders weit fortgeschritten. Hierbei wird Quantenkommunikation für die Verteilung eines Schlüssels an die Kommunikationspartner genutzt. Gab es dabei einen Abhörversuch, so wird der Schlüssel verworfen und ein neuer Schlüssel wird erzeugt und verteilt. Gab es keinen Abhörversuch, so ist der Schlüssel tatsächlich nur den befugten Kommunikationspartnern bekannt. Der geheime Schlüssel kann dann zur Absicherung von Informationsübertragung, die auf klassische Weise erfolgt, genutzt werden.

Mittels Quantenkommunikationstechnologie können zudem Datenbankabfragen oder Anweisungen an einen Quantencomputer geschützt werden. Bei Quantencomputern könnte dies zum Beispiel bedeuten, dass Eingabe-Information so an einen Quantencomputer übertragen wird, dass zwar damit gerechnet werden kann, diese Information aber nicht für Außenstehende einsehbar ist.[13]

[12] Kommunikation erfolgte zunächst vor allem analog und seit etwa 30 Jahren dann immer häufiger digital.

[13] Dieser Ansatz wird auch als Blind Quantum Computation bezeichnet.

3.5. VERTEILTES QUANTEN-COMPUTING

Praxisrelevante Probleme lassen sich erst ab einer gewissen Anzahl qualitativ hochwertiger Qubits schneller auf Quantencomputern als auf klassischen Computern lösen. Sehr vereinfacht gesagt: Je mehr Qubits ein Quantencomputer hat, desto besser. Die Konstruktion, die Produktion und der Betrieb von Quantenprozessoren sind jedoch große Herausforderungen, die sich mit steigender Anzahl von Qubits immer schwieriger gestalten. Quantenkommunikationstechnologie bietet eine Möglichkeit, diesem Skalierungsproblem bei der Entwicklung leistungsfähiger Quantencomputer zu begegnen.

Quantenteleportation ist ein Teilbereich der Quantenkommunikation, der dazu geeignet ist, räumlich voneinander getrennte Qubits aneinander zu koppeln. Dies bedeutet, dass die Zustände dieser Qubits quasi unzertrennlich voneinander sind, obwohl sie sich auf verschiedenen Quantenprozessoren befinden. Dies kann zum Beispiel durch Photonensignale an mittels Glasfaserkabel verbundene Prozessoren realisiert werden. Ultimativ bedeutet dies, dass die Ressourcen einzelner Quantenprozessoren gebündelt werden, d. h. Qubits, die sich auf unterschiedlichen Prozessoren befinden, verhalten sich, als ob sie sich auf dem gleichen Prozessor befänden. So sind Problemgrößen lösbar, für die die Qubitanzahlen der einzelnen Prozessoren nicht ausreichend sind. Verschiedene Entwickler von Quantencomputern verfolgen daher diesen Ansatz, um mittels eines verteilten Quantencomputing-Systems hohe Qubitanzahlen zu erreichen.[14]

Quantenkommunikation könnte also bei den in den Unterkapiteln 3.1, 3.2 und 3.3 beschriebenen Anwendungen den Schritt zur Praxisreife schneller oder gar überhaupt erst ermöglichen und ist daher auch ein Treiber der Entwicklung von Quantencomputing.

[14] Z. B. IBM (https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/, abgerufen am 18.08.2021) und QuTech (https://www.qutube.nl/quantum-algorithms/distributed-quantum-computing, abgerufen am 18.08.2021)

4. ENTWICKLUNG UND STATUS QUO DER QUANTEN-IKT

Anfang des 20. Jahrhunderts kam es zu einer Revolution in der Physik. Bis dato bestehende Theorien waren nicht vereinbar mit neuen Erkenntnissen zu sehr kleinen physikalischen Objekten, wie beispielsweise Molekülen, Elektronen, Atomen und Photonen. Die Eigenschaften von und die Wechselwirkungen zwischen diesen sogenannten Quantenobjekten erforderten grundsätzlich neue Modelle. Mit der Quantenphysik entstand ein neues Teilgebiet der Physik. Quantenobjekte und -phänomene sind zwar stets präsent, allerdings einzeln viel zu klein, als dass Menschen sie im Alltag wahrnehmen könnten.

Erkenntnisse aus der Quantenphysik mündeten in bahnbrechenden Erfindungen wie etwa der Magnetresonanztomografie, dem Laser und dem Transistor. Bauteile, die auf quantenphysikalischen Prinzipien beruhen, sind wesentliche Bestandteile herkömmlicher Informations- und Kommunikationstechnik, z. B. in Form von Transistoren bei Computerchips. Die Funktionsweise klassischer IKT lässt sich im Allgemeinen allerdings auch ohne quantenphysikalische Kenntnisse nachvollziehen.

Während klassische IKT sehr mächtig ist, existieren auch Probleme, für deren Lösung sie schlichtweg ungeeignet ist, zum Beispiel die Simulation quantenphysikalischer Effekte bei chemischen Prozessen (siehe z. B. Kapitel 2 und 3.1). In den 1980er Jahren entstand daher die Idee, eine Rechenmaschine zu entwickeln, die Quanteneffekte bereits beinhaltet, anstatt sie erst simulieren zu müssen. Daraus entwickelten sich über die Zeit verschiedene Software- und Hardwareansätze, um quantenphysikalische Prinzipien gezielt für die Informationsverarbeitung und -übermittlung zu nutzen: Es entstand die Quanteninformations- und Quantenkommunikationstechnologie, welche als wesentliche Teilgebiete Quantencomputing und Quantenkommunikation umfasst.

4.1 DAS QUBIT – HERZSTÜCK DER QUANTEN-IKT

Die kleinste Informationseinheit bei der Quanten-IKT ist das Quantenbit, kurz Qubit. Bei einer Messung eines Qubits können zwei verschiedene Werte festgestellt werden, die dann 0 bzw. 1 repräsentieren. Vor einer Messung können sich 0 und 1 aber auch überlagern, was bei Bits, der kleinsten Informationseinheit der klassischen IKT, nicht möglich ist, da diese immer eindeutig 0 oder 1 sind. D. h. Qubits können sich vor der Messung gleichzeitig in einem Zustand befinden, in dem sie sowohl 0 als auch 1 repräsentieren.

In der Quanten-IKT wird versucht, sich diese Überlagerungsmöglichkeit zunutze zu machen. Durch Überlagerungen kann ein Register von Qubits zum Beispiel wesentlich mehr Information repräsentieren als ein Bitregister vergleichbarer Größe (ersichtlich z. B. anhand Abbildung 1 in Kapitel 2). Ob nun mit Qubits gerechnet wird oder diese zum Zweck der Informationsübermittlung versendet werden: Den Abschluss eines solchen Vorgangs in der Quanten-IKT stellt die Messung von Qubits dar. Dabei kollabieren die Überlagerungszustände von Qubits und es ergibt sich eine gewöhnliche Folge aus Nullen und Einsen.

Es gibt verschiedene Möglichkeiten, Qubits zu konstruieren. Zum Beispiel können Photonen, Ionen oder supraleitende Schaltkreise als physikalische Grundlage solcher Konstruktionen dienen. Die Möglichkeiten unterscheiden sich zum Beispiel bezüglich der Anfälligkeit gegenüber Störungen, der Skalierbarkeit von wenigen auf viele Qubits und darin, ob und wie Qubitzustände fehlerfrei und schnell geändert werden können. Je nachdem, ob die Qubits zur Kommunikation oder als Grundlage einer Rechenmaschine, sprich eines Quantencomputers, eingesetzt werden sollen, ergeben sich dabei mitunter unterschiedliche Anforderungen bezüglich dieser Eigenschaften. Festhalten lässt sich, dass einige Konstruktionsweisen zwar weiter fortgeschritten und populärer sind als andere, aber sie derzeit allesamt unterschiedliche Vorteile und Nachteile haben.

4.2 MIT QUBITS KOMMUNIZIEREN

Es existieren zwei Möglichkeiten zur Quantenkommunikation. Zum einen das Versenden von Qubits als Informationsträger zwischen Kommunikationspartnern. Aufgrund quantenphysikalischer Prinzipien kann der Zustand des Qubits auf dem Weg vom Sender zum Empfänger nicht von Dritten abgehört werden, ohne dass das Qubit selber verändert wird. Wenn nun eine Folge von Qubits versendet wird, können die Kommunikationspartner einen Abhörversuch durch statistische Berechnungen nachweisen. Diese Tatsache wird zum Beispiel bei sogenannten Prepare-and-Measure-Protokollen genutzt.

Die andere Möglichkeit ist die sogenannte Quantenteleportation. Dabei verfügen die Kommunikationspartner über jeweils ein Teil eines verschränkten[15] Paars von Qubits. Weil Änderungen am Zustand eines Qubits auch über große Distanzen mit sofortiger Wirkung Änderungen am anderen Qubit nach sich ziehen, können Kommunikationspartner so abhörsicher Information austauschen.[16] Der Zustand des übertragenen Qubits bleibt dabei für alle außer dem Empfänger prinzipiell unbekannt, wodurch Information sicher übertragen werden kann.

Der bei der Quantenkommunikation vorwiegend eingesetzte Qubittyp sind Photonen. Diese eignen sich insbesondere deshalb, weil sie sich mit der maximal möglichen Geschwindigkeit, also der Lichtgeschwindigkeit, bewegen. Aus technischer Sicht existieren zwei wesentliche Übertragungswege für Photonen-Qubits: Zum einen sind das herkömmliche Glasfaserkabel und zum anderen können Photonen auf direktem Wege durch den Raum übertragen werden, also etwa von einem Satelliten zu einer Empfängerstation auf der Erdoberfläche. Eine solche Verbindung dient dann als sogenannter Quantenkanal.

4.3 MIT QUBITS RECHNEN

Bei Quantencomputern werden mehrere Qubits zu einem sogenannten Qubitregister zusammengefasst. Um ein Problem zu lösen, wird dieses Register in einen Startzustand versetzt, der so verändert wird, dass der Endzustand mit hoher Wahrscheinlichkeit die korrekte Lösung für das Problem darstellt. Eine Garantie, innerhalb eines Durchlaufs das korrekte Ergebnis zu erhalten, existiert für viele Algorithmen nicht. Dies ist darin begründet, dass Quanten-IKT und damit ein Quantencomputer probabilistisch und nicht deterministisch funktioniert. Allerdings kann z. B. durch mehrere Durchläufe eines Algorithmus die Wahrscheinlichkeit für die korrekte Lösung gesteigert werden.

Vorteilhaft für die Leistungsfähigkeit von Quantenrechnern ist eine hohe Anzahl von Qubits, da sie die Lösung größerer, komplexerer Probleme ermöglicht.

Es gibt zwei verbreitete Typen von Quantenrechnern. Ein Typ ist der sogenannte Quanten-Annealer. Dabei werden die Qubits in einen bekannten Startzustand versetzt, wobei sie unter Einfluss eines externen Magnetfelds stehen. Ein solches Magnetfeld kann so gestaltet werden, dass es den Parametern eines gegebenen Problems entspricht. Ein natürlicher, quantenphysikalischer Optimierungsprozess[17] sorgt dafür, dass die Qubits nach einer gewissen Zeit einen Zustand einnehmen, der bei einer

[15] Verschränkung ist ein quantenphysikalisches Phänomen. Bits können im Gegensatz zu Qubits nicht verschränkt werden. D. h. dieser Effekt ist eine Besonderheit der Quanten-IKT gegenüber der klassischen IKT. Eine Erklärung des Phänomens findet sich z. B. in Frank Wilczek, wired.com (2016): » Your Simple (Yes, Simple) Guide to Quantum Entanglement«. https://www.wired.com/2016/05/simple-yes-simple-guide-quantum-entanglement/.
Zuletzt abgerufen am 13.10.2021.

[16] Während bei der Quantenteleportation Änderungen am anderen Qubit instantan erfolgen, handelt es sich trotzdem nicht um überlichtschnelle Informationsübertragung, da zur Informationsübertragung zusätzlich ein klassischer Kanal erforderlich ist.

[17] Hier bestehen durchaus Ähnlichkeiten zu Analogrechnern, die größtenteils durch Digitalrechner abgelöst wurden. Weitere Informationen z. B. in Wolfgang Stieler, heise.de (2018): »Zurück in die Zukunft«. https://www.heise.de/hintergrund/Zurueck-in-die-Zukunft-4232274.html. Zuletzt abgerufen am 13.10.2021.

Exkurs: Hardware

Zur Hardware von Quanten-IKT gehören neben den Qubits, die die Informationsspeicher darstellen, auch Elemente zur Steuerung und Messung. Messgeräte ermöglichen es überhaupt erst, ein Ergebnis festzustellen. Steuerungstechnik wird dazu genutzt, Qubits in einen bekannten Startzustand zu versetzen und die Quantengatter zu realisieren, die eine gezielte Veränderung der Zustände ermöglichen. Wesentliche Anforderungen an die Steuerungs- und Messtechnik sind, dass sie schnell, aber auch fehlerfrei operieren. Welche Technik dabei überhaupt zum Einsatz kommen kann, hängt auch immer von der Konstruktionsweise der Qubits ab. Zudem sind Bauteile von Bedeutung, die Quanten-IKT gegen unerwünschte Umwelteinflüsse isolieren. Sie sind kein direkter Teil der Funktionsweise von Quanten-IKT, sind aber erforderlich, um die Fehlerrate zu reduzieren. Insgesamt sind der Bau und der Betrieb von Quanten-IKT extrem kompliziert, aufwändig und fehleranfällig. Daher wird Quanten-IKT auch auf absehbare Zeit kein Bestandteil der Heim- und Bürotechnik werden.

Messung mit überdurchschnittlich hoher Wahrscheinlichkeit der Lösung des Problems entspricht. Für diesen Typ existieren mittlerweile Rechner mit einigen tausend Qubits.

Der andere Typ ist der gatterbasierte Quantenrechner. Auch hier werden die Qubits in einen bekannten Startzustand versetzt. Die Veränderung der Zustände wird hier aber keinem natürlichen Prozess überlassen. Der Prozess ähnelt eher dem Prozess beim klassischen Rechner. Beim klassischen Rechner werden Gatter (kleine logische Operationen) auf Bitregister in einer durch einen Algorithmus festgelegten Reihenfolge angewendet. Anstelle von Gattern, Bits und Algorithmen sind es beim Quantenrechner nun aber die sogenannten Quantengatter, Qubits und Quantenalgorithmen. Quantenalgorithmen unterscheiden sich grundlegend von klassischen Algorithmen, weil sie zur quantenphysikalischen Natur der Rechner passen müssen und die Vorteile der Quantenphänomene nutzen sollten. Die Qubitanzahl ist bei gatterbasierten Quantenrechnern noch deutlich niedriger als bei den Quanten-Annealern, allerdings sind sie aufgrund des algorithmischen Ablaufs programmierbarer und dadurch vielseitiger einsetzbar.

4.4 HYBRIDE SYSTEME & QUANTUM-INSPIRED COMPUTING

Quanten-IKT und klassische IKT stehen nicht zwangsläufig in Konkurrenz. Es existieren sowohl Aufgaben, für deren Bearbeitung eher Quanten-IKT geeignet ist, als auch Aufgaben, für die eher klassische IKT infrage kommt. Dementsprechend wird z. B. auch an hybriden Systemen gearbeitet, die Teilaufgaben einer Gesamtaufgabe an den jeweils geeigneten Rechnertyp verteilen. Zudem bereichert Quanten-IKT die klassische IKT auch auf andere Weise: Durch die Entwicklung von Quanten-IKT entstehen auch neue Denkweisen, aus denen durch Quantenphänomene inspirierte klassische Bauteile und Algorithmen resultieren (Stichwort Quantum-Inspired Computing).

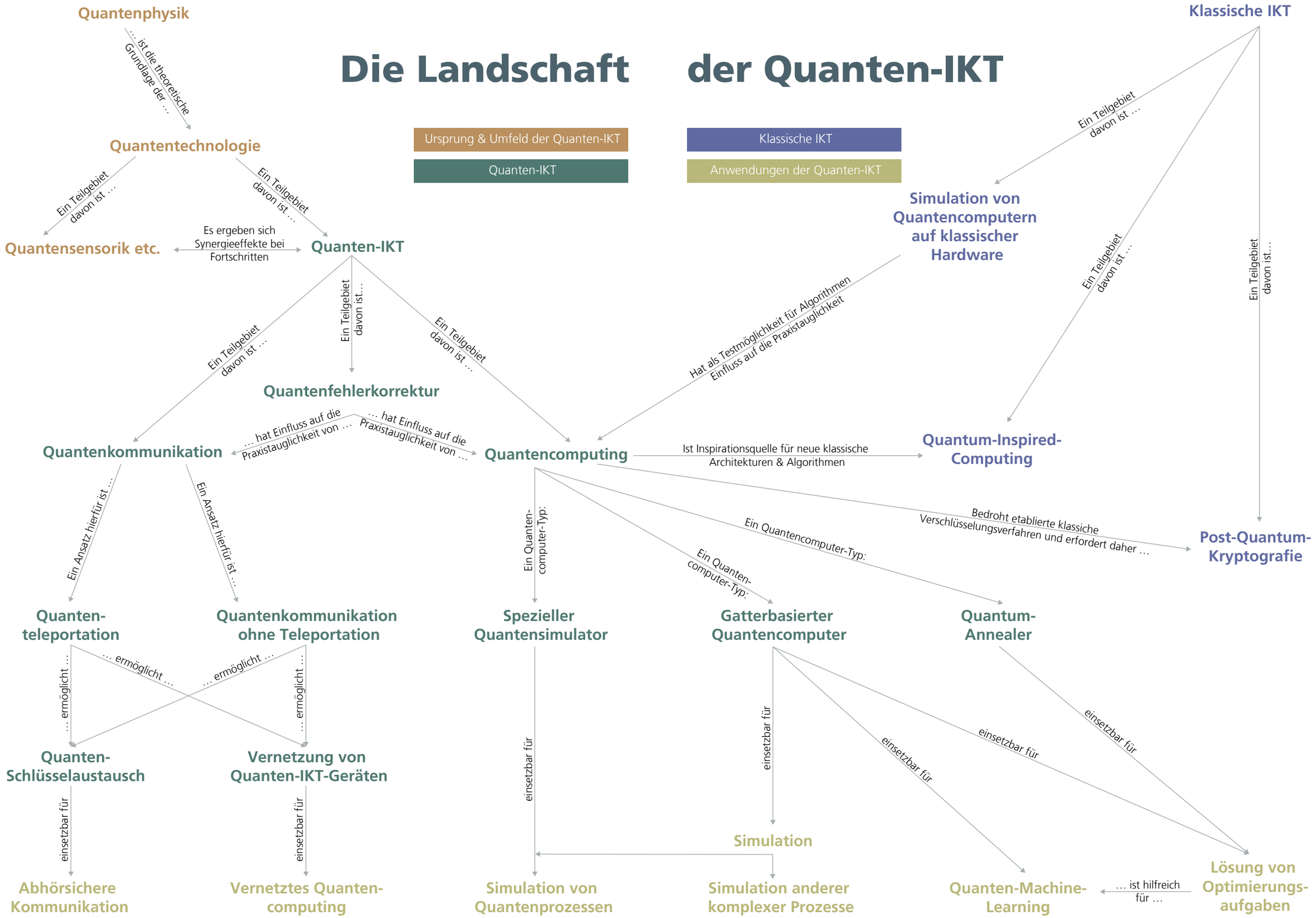
Die Landschaft der Quanten-IKT

Ursprung & Umfeld der Quanten-IKT

Quanten-IKT

Klassische IKT

Anwendungen der Quanten-IKT



5. WETTBEWERB, AKTEURE & INITIATIVEN

Wie in Kapitel 4 aufgezeigt wurde, besteht die Quanten-IKT aus mehreren Teilbereichen und es existieren verschiedene technische Ansätze, etwa bei der Konstruktionsweise von Qubits oder der Quantenkommunikation. Verschiedene Akteure treiben unterschiedliche Ansätze voran, in der Hoffnung, schneller als die Konkurrenz die Praxisreife zu erreichen und sich so Marktanteile zu sichern. Als Einzelkämpfer werden es europäische Staaten und Unternehmen allerdings schwer haben, sich durchzusetzen.

5.1. WETTBEWERBSSITUATION

Weltweit investieren Forschungseinrichtungen, spezialisierte Start-ups und etablierte Unternehmen in Quanten-IKT. Um einen Überblick der internationalen Konkurrenzsituation mit besonderem Augenmerk auf Deutschland und Europa zu ermöglichen, wurde ein datenbasierter Ansatz gewählt.

5.1.1 Grundlagenforschung

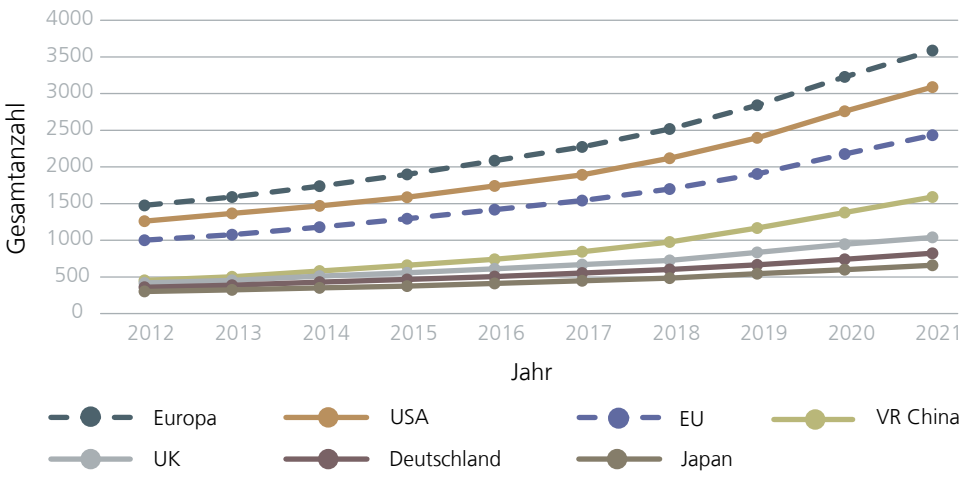
Quanten-IKT ist in der Grundlagenforschung ein Dauerthema. Werden die Forschungsergebnisse dabei an der Anzahl der in Fachzeitschriften veröffentlichten Artikel gemessen, so sind die USA und die VR China hier die mit Abstand führenden Nationen. Dabei sind die USA führend bei Artikeln zu Quantencomputing, Quantenalgorithmen und Quantenfehlerkorrektur und die VR China bei Quantenkommunikation und speziell z. B. bei Quantennetzwerken[18]. Aus dem asiatischen Raum sind in der Verfolgergruppe zudem Südkorea und noch stärker Japan präsent. Deutschland kann sich mit allen Nationen außer den USA und der VR China messen, in einigen Bereichen, wie etwa bei Qubitkonstruktionsweisen, die auf Stickstoff-Fehlstellen in Diamanten oder auf Photonen basieren, befindet sich Deutschland auch gegenüber den USA und der VR China in einer starken Position. Generell sind die europäischen Nationen bezüglich der Publikationszahlen in der Grundlagenforschung erst gemeinsam konkurrenzfähig, hierzu tragen unter anderem Spanien, Frankreich, Italien und Österreich bei. Deutschland ist dabei knapp nach dem Vereinigten Königreich der zweitstärkste europäische Staat. Das Vereinigte Königreich ist allerdings vor Kurzem aus der EU ausgetreten ist, was die zukünftige Zusammenarbeit erschweren könnte.

5.1.2 Wertschöpfungsmöglichkeiten

Im Bereich der Wertschöpfung ist im letzten Jahrzehnt und insbesondere den letzten fünf Jahren ein starker Anstieg der Aktivitäten zu beobachten. Hier ist das Rennen um zukünftige Marktanteile bereits in vollem Gange, wobei sich in einigen Bereichen Vorentscheidungen anbahnen, während andere Bereiche noch sehr offen sind.

[18] Hierbei handelt es sich um miteinander verbundene Quantenkanäle und -prozessoren, die ein Netzwerk bilden.

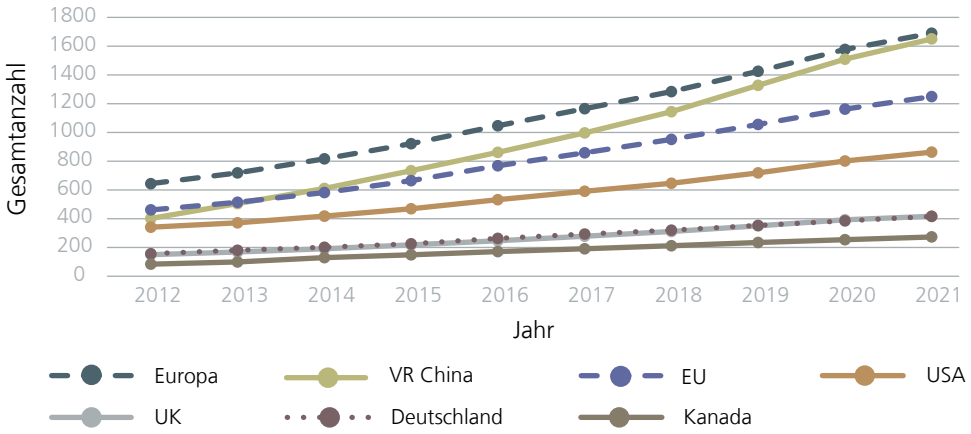
Abbildung 4: Wissenschaftliche Artikel zu Quantencomputing



Entwicklung der Anzahl von wissenschaftlichen Artikeln über die Zeit. Berechnung anhand von Web-of-Science-Daten. Die Artikel wurden anhand der Adressen der Autor:innen Regionen zugeordnet. Stand: 18.10.2021.

Abbildung 5: Wissenschaftliche Artikel zu Quantenkommunikation

Entwicklung der Anzahl von wissenschaftlichen Artikeln über die Zeit. Berechnung anhand von Web-of-Science-Daten. Die Artikel wurden anhand der Adressen der Autor:innen Regionen zugeordnet. Stand: 18.10.2021.



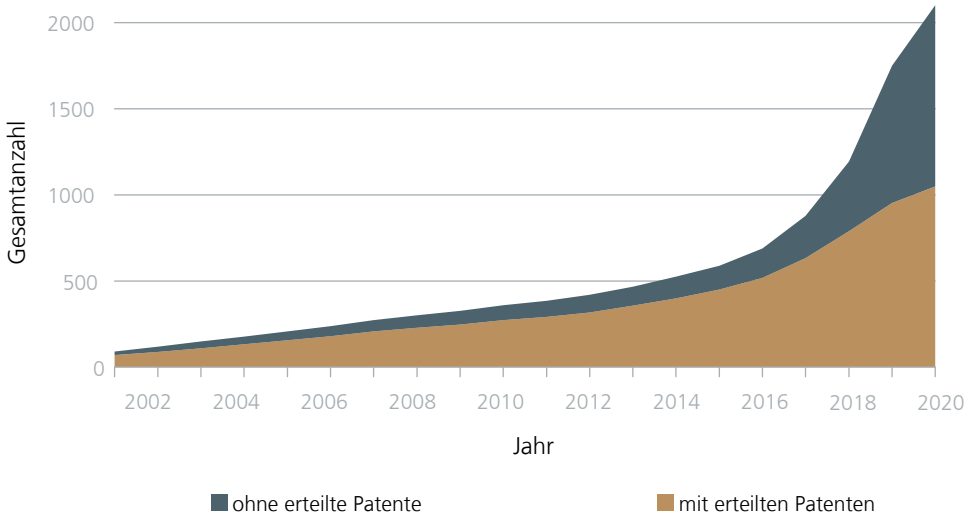


Abbildung 6: Patentfamilien zu Quantencomputing.

Entwicklung der Anzahl der Patentfamilien. Die Patentfamilien wurden anhand der Prioritätsdaten den Jahren zugeordnet. Die Berechnung erfolgte auf Basis von PatBase-Daten. Stand: 17.11.2021.

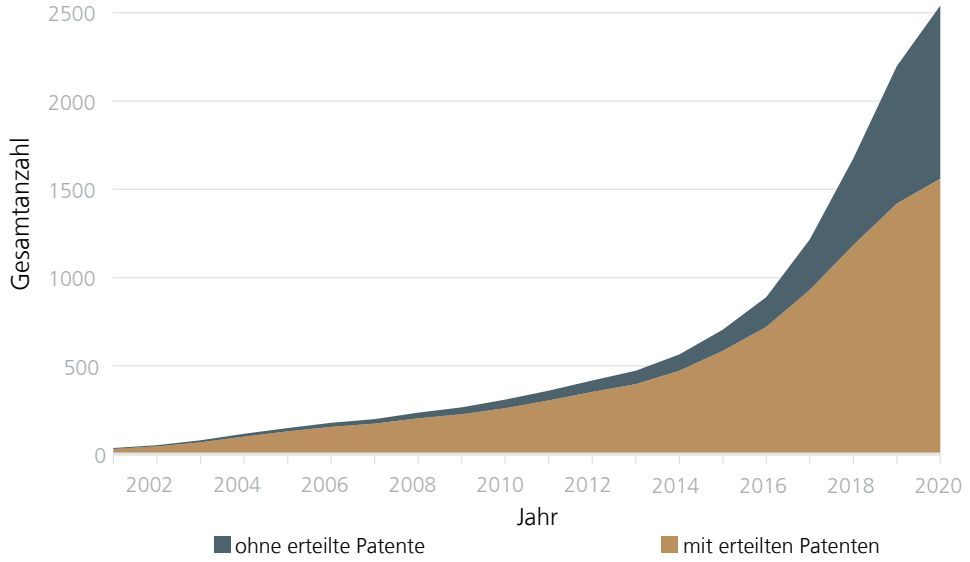


Abbildung 7: Patentfamilien zu Quantenkommunikation

Entwicklung der Anzahl der Patentfamilien. Die Patentfamilien wurden anhand der Prioritätsdaten den Jahren zugeordnet. Die Berechnung erfolgte auf Basis von PatBase-Daten. Stand: 17.11.2021.

Werden Patentfamilien als Indikator gewählt[19], ist ein starker Anstieg der Gesamtanzahl in den letzten Jahren beobachtbar (siehe Abb. 6 und 7). Im Bereich Quantencomputing sind dabei nordamerikanische und insbesondere US-amerikanische Unternehmen tendenziell führend (siehe Abb. 8). Schwergewichte der IKT-Branche wie etwa IBM, Google und Microsoft haben sich hier bereits viele Patente gesichert und gehören auch bezüglich der Leistungsstärke existierender Quantenrechner zu den führenden Organisationen. Unter den Top-Patentanmeldern befinden sich im Weiteren auch einige Unternehmen aus der VR China sowie Japan.

Im Bereich der Quantenkommunikation sind nordamerikanische Unternehmen weniger stark vertreten, hier dominieren Organisationen aus der VR China und Japan (siehe Abb. 9). Im Vergleich zu den Patenten im Bereich Quantencomputing handelt es sich im Bereich der Quantenkommunikation bei den Anmeldern häufiger um Universitäten und staatliche Einrichtungen statt um private Unternehmen. Im Bereich der Quantenfehlerkorrektur sind Organisationen aus den USA, der VR China und Japan unter den aktivsten Patentanmeldern.

5.1.3 Start-ups

Während große Organisationen wie staatliche Institute, große IKT-Unternehmen und Mischkonzerne in der Wertschöpfung stark präsent sind, bietet Quanten-IKT auch Chancen für auf dieses Feld spezialisierte Start-ups. Seit 2010 sind viele solche Unternehmen entstanden, die sich viele Patente sichern konnten und Teil wirtschaftlich vielversprechender Kooperationen sind. Dies sind zumeist Start-ups aus den USA und der VR China wie etwa Rigetti (Gründung 2013, Hauptsitz USA) und Origin Quantum Computing Technology (Gründung 2017, Hauptsitz VR China).

5.1.4 Deutschland und Europa im internationalen Vergleich

Im Bereich der Wertschöpfung haben Deutschland und Europa bereits Rückstand zu den führenden Nationen. Wird die Anzahl der Patentfamilien als Indiz für besonders hohe Wertschöpfungsmöglichkeiten betrachtet, fällt auf, dass Organisationen aus Deutschland und Europa im weltweiten Vergleich Rückstand haben. Tatsächlich werden leistungsstarke Quantencomputer derzeit zumeist außerhalb Europas entwickelt.[20] Die Anzahl der wissenschaftlichen Fachartikel zu Quanten-IKT zeigt, dass die Grundlagenforschung in Europa durchaus mithalten kann. Dies ist ein Anzeichen dafür, dass in Deutschland und Europa ein Problem besteht, die Stärke der Grundlagenforschung in Wertschöpfungsmöglichkeiten zu übersetzen. Doch selbst wenn diese Übersetzung von Grundlagenforschung in Wertschöpfung besser klappen würde, zeigt die Publikationsanzahl von wissenschaftlichen Artikeln doch auf, dass die europäischen Nationen nur gemeinsam wirtschaftlich konkurrenzfähig gegenüber den USA und der VR China sein können.

5.1.5 Chancen

Quanten-IKT besteht aus vielen einzelnen Bereichen, davon sind einige weiter fortgeschritten als andere. Wenn Deutschland und Europa in diesen Bereichen nicht bereits vergleichsweise weit auf dem Weg zur Wertschöpfung sind, dürfte es hier entsprechend schwieriger als in anderen Bereichen sein, konkurrenzfähig zu werden. Andere Bereiche befinden sich hingegen erst am Anfang, d. h. hier existieren bisher kaum Vorsprünge und dementsprechend Markteintrittsbarrieren.

Ein Beispiel für einen unterschiedlich besetzten Teilbereich der Quanten-IKT ist die Konstruktionsweise von Qubits. Für Qubits auf Basis supraleitender Schaltkreise existieren bereits z. B. viele Patentfamilien, wobei sich außereuropäische Unternehmen hier bereits in gute Positionen gebracht haben (siehe Abb. 10).

Andere Konstruktionsweisen sind weniger reif. Bei der als »topologische Qubits« bekannten Konstruktionsweise ist allerdings schon ein klarer Vorsprung von Microsoft zu erkennen, das stark auf diese Konstruktionsweise setzt. Für Qubits, die auf Stickstoff-Fehlstellen in Gittern basieren, existieren bisher kaum Patente (siehe Abb. 12). Diese Konstruktionsweise ist aus europäischer Perspektive auch deshalb interessant, weil gerade Deutschland hier vergleichsweise stark in der Grundlagenforschung ist (siehe Abb. 11). Trotzdem wäre es ein Fehler, die europäischen Bemühungen nur auf eine Konstruktionsweise zu beschränken, da noch nicht geklärt ist, welche Konstruktionsweise das größte Potenzial mitbringt. Hier bietet es sich an, mehrgleisig zu fahren.

[19] Patente sind eine, aber natürlich nicht die alleinige Grundlage der Wertschöpfung. Die Anzahl und die Verteilung der Patentfamilien sind daher Indizien für Wertschöpfung, zeichnen alleine aber kein vollständiges Bild. Die hier beschriebenen Erkenntnisse ergeben sich nicht alleine aus der Auswertung von Patentdaten, sondern auch aus Fachkonferenzen und -diskussionen. Bei Patentdaten ist zudem stets zu beachten, dass die Erteilung von Patenten mehrere Jahre in Anspruch nehmen kann, weshalb die Zahlen für Patentfamilien mit erteilten Patenten ab dem Prioritätsjahr 2016 weniger verlässlich sind als für den Zeitraum davor.

[20] Eine Auflistung findet sich z. B. hier: https://en.wikipedia.org/wiki/List_of_quantum_processors. Zuletzt abgerufen am 17.11.2021.

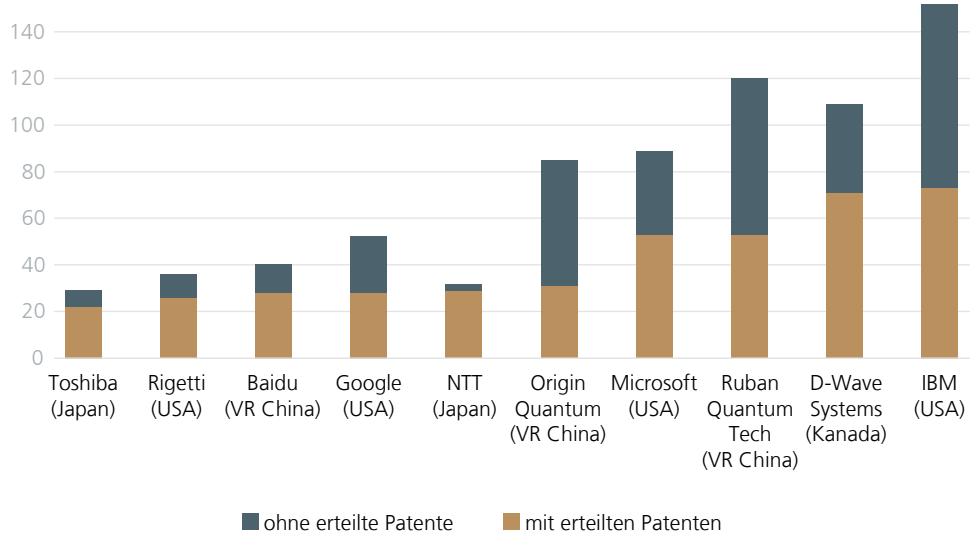


Abbildung 8: Patentfamilien zu Quantencomputing

Inhaber von Patentfamilien mit Prioritätsjahr von 2001 bis 2020, sortiert nach Familien, für die mindestens ein Patent erteilt wurde. Die Berechnung erfolgte auf Basis von PatBase-Daten. Stand: 17.11.2021.

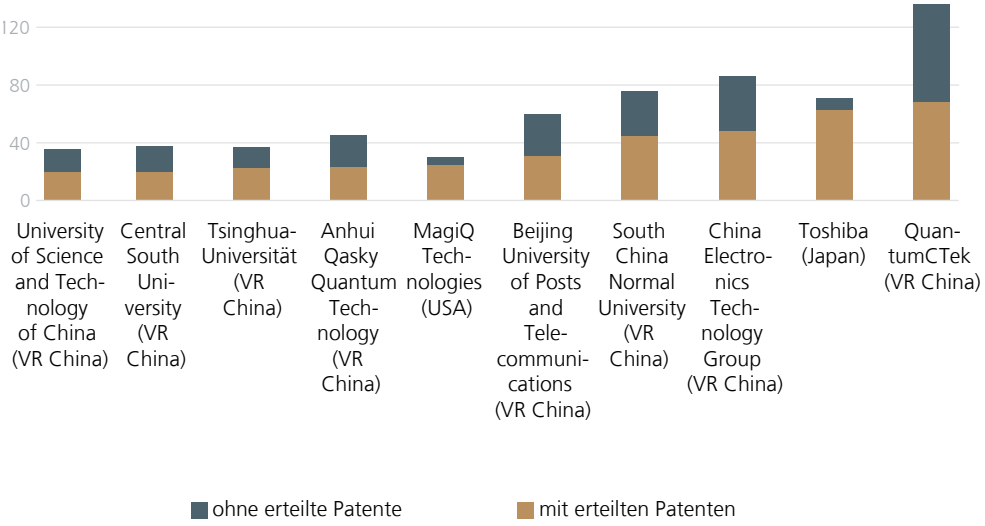


Abbildung 9: Patentfamilien zu Quantenkommunikation

Inhaber von Patentfamilien mit Prioritätsjahr von 2001 bis 2020, sortiert nach Familien, für die mindestens ein Patent erteilt wurde. Die Berechnung erfolgte auf Basis von PatBase-Daten. Stand: 17.11.2021.

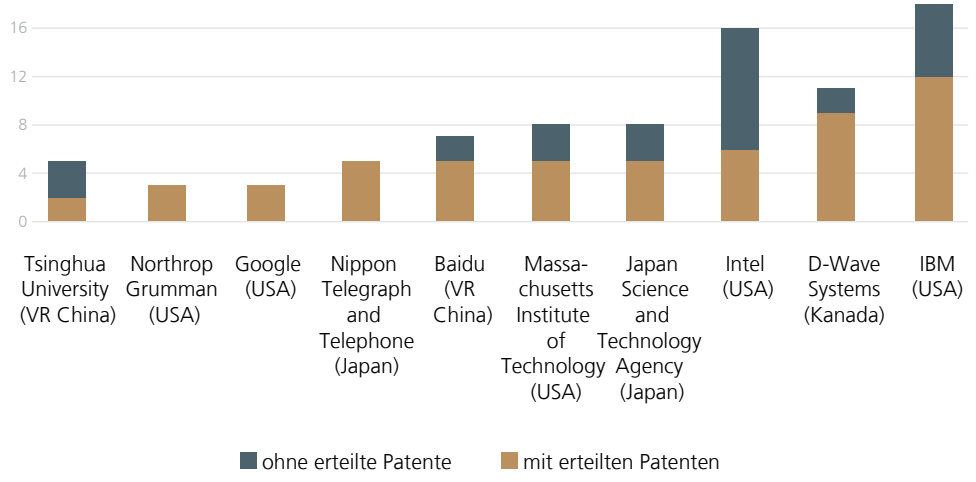


Abbildung 10: Patentfamilien zu supraleitenden Qubits

Inhaber von Patentfamilien mit Prioritätsjahr von 2001 bis 2020, sortiert nach Familien, für die mindestens ein Patent erteilt wurde. Die Berechnung erfolgte auf Basis von PatBase-Daten. Stand: 17.11.2021.

Abbildung 11: Wissenschaftliche Artikel zu Qubits mit Stickstoff-Fehlstellen

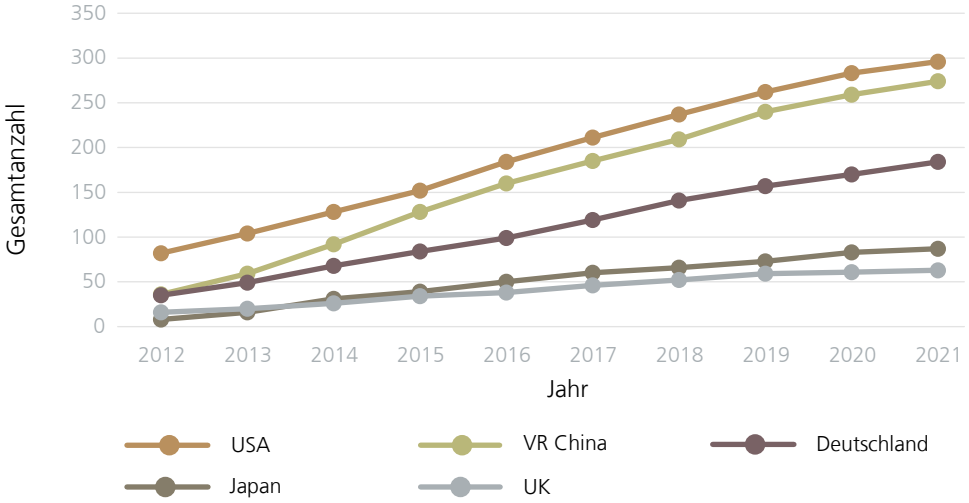
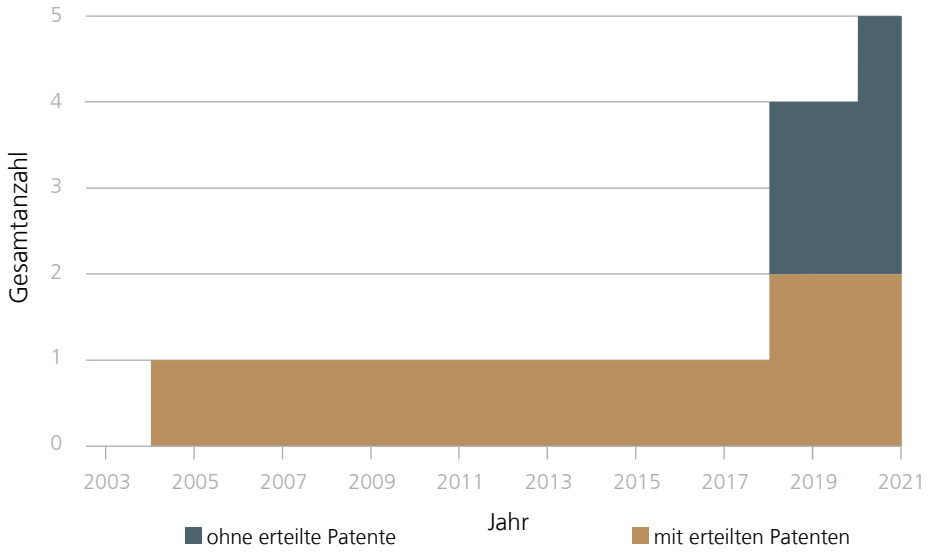


Abbildung 12: Patentfamilien zu Qubits mit Stickstoff-Fehlstellen



5.2. FÖRDERUNG UND INITIATIVEN

International investieren viele Technologiegrößen massiv in Quanteninformationstechnologie. Auch von öffentlichen Stellen werden weltweit umfangreiche finanzielle Ressourcen bereitgestellt, um Quantentechnologien voranzutreiben und skalierbare Quantenrechner und Quantennetzwerke sowie zugehörige Infrastruktur und nutzbare Softwareunterstützung zu entwickeln: So fördern die EU-Staaten und die Europäische Kommission beispielsweise über zehn Jahre im Rahmen der »Quantum Flagship Initiative«[21] vier Felder im Bereich Quantentechnologie mit einer Milliarde Euro. Die Bundesregierung will auf Basis ihrer »Quantencomputing Roadmap 2021« national weitere zwei Milliarden Euro in die Quantencomputing-Forschung investieren, um einen deutschen Quantenrechner zu bauen und Quantentechnologie von der Grundlagenforschung hin zu marktfähigen Anwendungen zu entwickeln.[22] In den

[21] Mehr Informationen unter https://qt.eu/about/. Zuletzt abgerufen am 20.10.2021.

[22] Mehr Informationen unter https://www.bundesregierung.de/breg-de/suche/quantencomputing-1836542 und https://www.quantentechnologien.de/qt-in-deutschland/programm.html. Zuletzt abgerufen am 20.10.2021.

letzten Jahren wurden größere Institute, Exzellenzinitiativen und Kooperationen gebildet, die sich der Forschung zum Thema Quantentechnologien widmen.

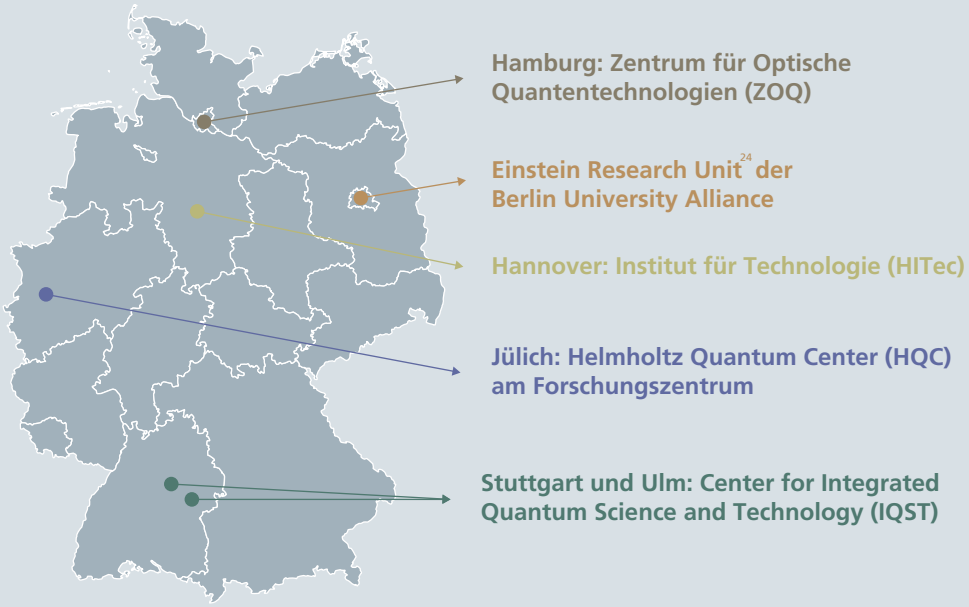
5.2.1 Ausblick

Europa und Deutschland sind mit ihrer langen wissenschaftlichen Tradition in der Quantenphysik und einer starken Quantentechnologieforschung in keiner schlechten Ausgangsposition, den Schritt aus der Grundlagenforschung zur Anwendung maßgeblich mitzugestalten. In Projekten wie z. B. PlanQK[23], zum Aufbau einer Plattform und eines Ökosystems für Quanten-KI, oder JUNIQ, als »Jülicher Nutzer-Infrastruktur für Quantencomputing« und mit weiteren Quantencomputing-Initiativen soll die technologische Basis für die Entwicklung von Quantentechnologien mit einem niederschwelligen Zugang für die Nutzung durch die Industrie, z. B. für Quanten-KI-Anwendungen, geschaffen werden. Um wettbewerbsfähig und souverän bezüglich Quanten-IKT zu sein, muss allerdings der Schritt zur Wertschöpfung gelingen. Wie in Kapitel 5.1 beschrieben, sind andere Staaten hier weiter.

[23] Mehr Informationen unter https://planqk.de. Zuletzt abgerufen am 20.10.2021.

Exkurs: Initiativen & Netzwerke in Deutschland und Europa

In den letzten Jahren wurden größere Institute, Exzellenzinitiativen und Kooperationen gebildet, die sich der Forschung zum Thema Quantentechnologien widmen. Zu den Instituten und Forschungszentren gehören beispielsweise:



Zu den Initiativen und Netzwerken gehört zum Beispiel die vom BMBF geförderte Initiative QuNET, bei der es unter Beteiligung der Fraunhofer-Institute IOF und HHI, der DLR und des Max-Planck-Institutes für die Physik des Lichts um die Weiterentwicklung von Quantenkommunikation geht.

Des Weiteren organisiert Bitkom jährlich den »Quantum Summit«. Partner sind z. B. die Fraunhofer-Gesellschaft, Atos und Fujitsu. Hier geht es um Wissensaustausch und Vernetzung zu Quantentechnologien allgemein.

[24] »Perspectives of a quantum digital transformation: Near-term quantum computational devices and quantum processors«

Das Konsortium OpenQKD[25] will mit Tests, Demonstratoren und Standards die Grundlage für ein gesamteuropäisches Netzwerk zum Quanten-Schlüsselaustausch legen. Mitglieder sind z. B. die Deutsche Telekom, BT, das Max-Planck-Institut für die Physik des Lichts, das Deutsche Zentrum für Luft- und Raumfahrt, Toshiba und die Universität Genf.

Das Quantum Business Network[26] (kurz QBN) beschäftigt sich in der Breite mit Quantentechnologien. Zu den Mitgliedern zählen drei Fraunhofer-Institute (AISEC, IAF, IPMS), europäische Start-ups wie Cambridge Quantum Computing (Fokus auf Software für Quantencomputer), ParityQC (Fokus auf Architektur für Quantenrechner), Quantum Optics Jena (Fokus auf Photonenquellen und optische Systeme) und kiutra (Fokus auf Kühlsysteme als »Enabling Technology«).

Im Rahmen der Initiative zu Quantentechnologien der Fraunhofer-Gesellschaft[27] wurde 2021 zusammen mit IBM ein IBM Q System One in Betrieb genommen. Die Fraunhofer-Gesellschaft koordiniert auf dieser technologischen Basis ein nationales Kompetenznetzwerk für Quantencomputing mit den Zielen Weiterentwicklung und Transfer anwendungsorientierter Quantencomputerstrategien – und zwar unter Wahrung der Datenhoheit und unter Einhaltung europäischer Vorschriften zum Umgang mit Daten.

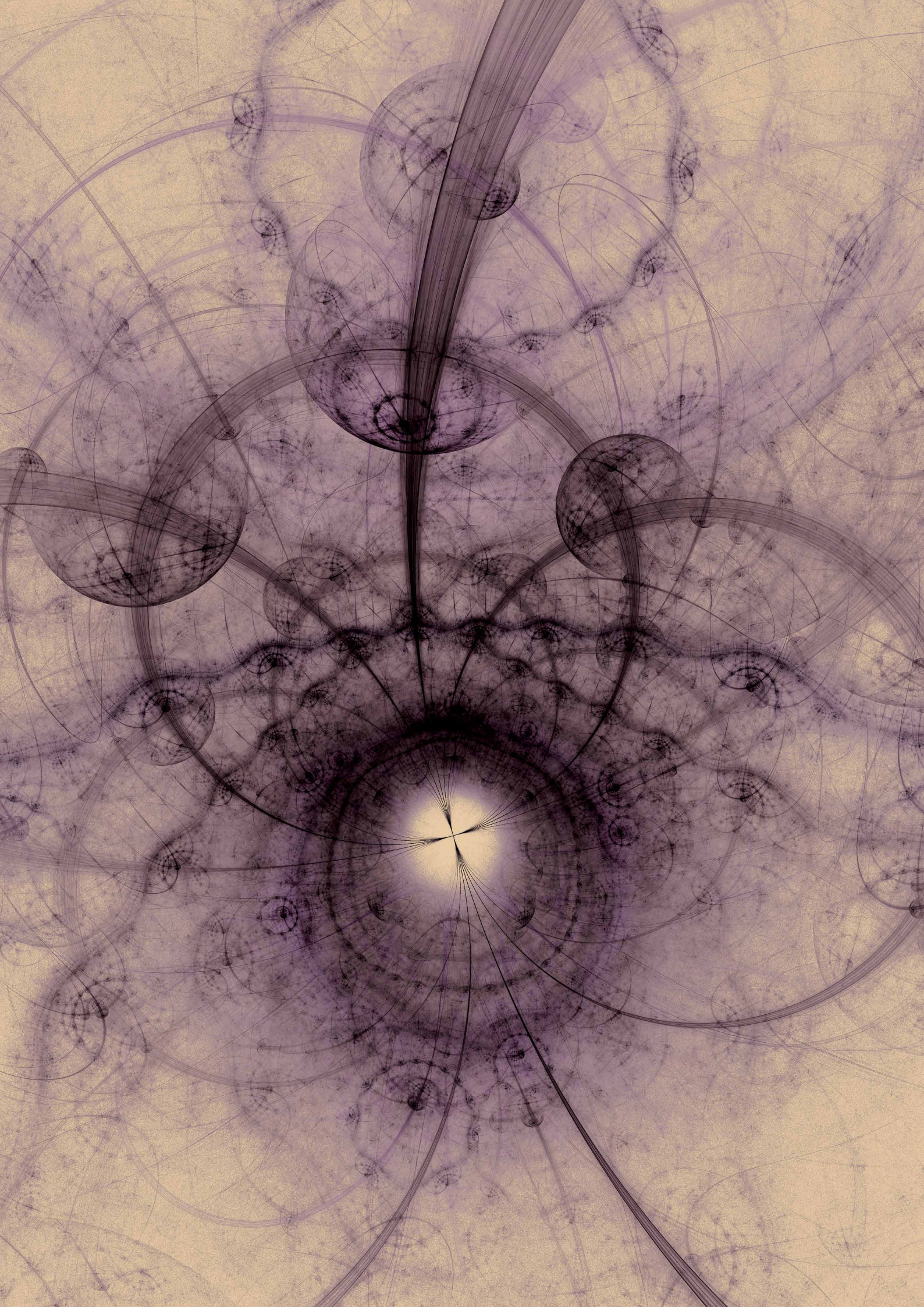
Des Weiteren wird im Rahmen der von der EU geförderten Initiative »OpenSuperQ«[28] ein europäischer Quantencomputer auf Basis supraleitender Qubits entwickelt. Ein Exemplar des Quantencomputers soll am Forschungszentrum Jülich betrieben werden, ein weiteres später von der ETH Zürich.

[25] Mehr Informationen unter https://openqkd.eu/.
Zuletzt abgerufen am 19.08.2021.

[26] https://quantumbusinessnetwork.de/. Zuletzt abgerufen am 9.12.2021.

[27] Mehr Informationen unter https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/quantentechnologie.html.
Zuletzt abgerufen am 20.10.2021.

[28] Mehr Informationen unter https://opensuperq.eu.
Zuletzt abgerufen am 20.10.2021.



6. HERAUSFORDERUNGEN

Auf dem Weg zur weitreichend praxistauglichen Quanten-IKT unter Berücksichtigung deutscher und europäischer Interessen sind noch erhebliche Hindernisse zu bewältigen. Herausforderungen ergeben sich dabei auf verschiedenen Ebenen. Auf der technischen Ebene sind z. B. noch Hardwarelimitationen zu überwinden. Aus politischer Sicht muss die Wettbewerbsfähigkeit und Souveränität Deutschlands und Europas bei der möglichen Schlüsseltechnologie Quanten-IKT angesichts starker Konkurrenz (siehe Kapitel 5.1) langfristig gewährleistet werden. In diesem Kapitel werden einige dieser Herausforderungen und Lösungsansätze vorgestellt.

6.1. TECHNISCHE HÜRDEN

6.1.1 Hürden bei Quantencomputern

Quantenalgorithmen zur Lösung praxisnaher Probleme benötigen in der Regel viele Qubits, die ihren Zustand über einen längeren Zeitraum stabil halten können. Im Vergleich zu diesen Anforderungen gelten heutige Quantencomputer als klein und fehleranfällig – wir befinden uns in der sogenannten NISQ-Ära *(Noisy Intermediate-Scale Quantum Computing)*. Dies limitiert die Möglichkeiten heutiger Quantencomputer. Die Anzahl an verfügbaren Qubits bestimmt die Größe des Problems, das in den Quantencomputer eingelesen werden kann, wie auch die Größe der Lösung, die nach der Berechnung ausgelesen werden kann. In der Forschung spricht man dabei von der *algorithmischen Breite*. Analog dazu bezeichnet die *algorithmische Tiefe*, wie viele Operationen hintereinander ausgeführt werden können, ohne dass die Zustände der einzelnen Qubits kollabieren (Dekohärenz[29]). Die algorithmische Tiefe wird maßgeblich durch die Stabilität der einzelnen Qubits bestimmt. Eine weitere Beschränkung heutiger Systeme stellt die Genauigkeit *(Fidelity[30])* der Qubits dar. Diese wird hauptsächlich durch die Art und Weise bestimmt, wie die Qubits technisch implementiert sind.

Die Forschung verfolgt im Wesentlichen zwei Wege, um die Fehleranfälligkeit von Qubits zu reduzieren und ihre Stabilität zu erhöhen. Zum einen wird an technischen Lösungen geforscht, wie z. B. neuen Konstruktionsweisen für Qubits. Zum anderen wird an Verfahren zur Quantenfehlerkorrektur gearbeitet. Dabei werden mehrere physische Qubits zu einem logischen Qubit zusammengefasst, d. h. sie verhalten sich im Algorithmus wie ein einzelnes, fehlerkorrigiertes Qubit. Wie viele physische Qubits zur Erstellung eines logischen Qubits erforderlich sind, hängt z. B. von der zugrundeliegenden Qubit-Konstruktionsweise ab und reicht von etwa 13 bis hin zu Millionen von physischen Qubits.[31] Um also einen Quantencomputer mit einer praxisreifen Anzahl an logischen Qubits zu erreichen, ist auf Hardwareebene eine deutlich größere Anzahl an physischen Qubits erforderlich. Dabei werden die Kosten pro Qubit auf ca. 10.000 US-Dollar geschätzt[32]. Ein wesentliches Problem bei der Skalierung der Qubitzahlen stellt zudem die Hitzeentwicklung durch den Einsatz von Mikrowellenstrahlung zur Manipulation der einzelnen Qubits dar.[33] Für einige Qubittypen sind Temperaturen nahe dem absoluten Nullpunkt erforderlich, damit die Quantenzustände nicht kollabieren und damit das Ergebnis des ausgeführten Quantenalgorithmus verfälschen. Damit Quantenrechner funktionieren, müssen sie generell gut gegenüber Umwelteinflüssen abgeschirmt werden. Daher sind auch technische Hürden bei »unterstützenden« Technologien bedeutend für die Skalierbarkeit von Quantencomputern: Beispielsweise haben existierende Apparate zur Kühlung von Qubits einen sehr hohen Energiebedarf und obwohl die Quantenprozessoren selbst sehr klein sind, erfordert die restliche Technik derzeit außerordentlich viel Grundfläche. An Fortschritten bei sogenannten »Quantum Enabling Technologies« wird gearbeitet. Für die Skalierung ist zudem die durch Quantenkommunikation gegebene Möglichkeit des in Kapitel 3.5 beschriebenen verteilten Quantencomputings relevant.

[29] Durch Interaktion mit der Umwelt verändert sich der Zustand eines Quantensystems. Im Falle eines Quantencomputers bedeutet das, dass die mittels Qubits gespeicherte Information verloren geht. Mehr dazu z. B. unter https://blogs.scientificamerican.com/observations/decoherence-is-a-problem-for-quantum-computing-but/. Zuletzt abgerufen am 23.11.2021.

[30] Fidelity ist ein Maß für Ähnlichkeit von Quantenzuständen. Es wird z. B. genutzt, um zu bestimmen, wie »sauber« ein Quantengatter arbeitet, also wie nahe der durch ein reales Quantengatter erzeugter Quantenzustand dem theoretisch erwarteten Quantenzustand kommt.

[31] Mehr Informationen dazu z. B. unter https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap.
Zuletzt abgerufen am 20.10.2021.

[32] John Levy: »1 million qubit quantum computers: moving beyond the current «brute force" strategy«. https://seeqc.com/blog/1-million-qubit-quantum-computers-moving-beyond-the-current-brute-force-strategy/.
Zuletzt abgerufen am 20.10.2021.

[33] John Levy: »1 million qubit quantum computers: moving beyond the current «brute force" strategy«. https://seeqc.com/blog/1-million-qubit-quantum-computers-moving-beyond-the-current-brute-force-strategy/.
Zuletzt abgerufen am 20.10.2021.

Eine weitere Hürde ist die Notwendigkeit hochgenauer Messinstrumente. Denn selbst wenn die einzelnen Qubits eine gute Stabilität und hohe Genauigkeit aufweisen, kann die abschließende Messung der Qubitzustände die Ergebnisse stark verfälschen. Heutige Quantencomputer verwenden als Messinstrumentarium eine ganze Reihe von einzelnen Geräten, die immer wieder neu kalibriert und aufeinander abgestimmt werden müssen. Dieses Verfahren ist fehleranfällig und skaliert voraussichtlich schlecht für zukünftige Quantencomputer mit hohen Qubitzahlen.[34] Diese Hürde ist auch für die Quantenkommunikation relevant, da Qubits hier nach der Übertragung vom Sender zum Empfänger gemessen werden.

6.1.2 Hürden bei der Quantenkommunikation

Quantenkommunikation ist technologisch weiter fortgeschritten als Quantencomputing. Protokolle und Anwendungen aus der Quantenkommunikation befinden sich teilweise noch in der Laborphase, werden teilweise aber auch schon seit Längerem praktisch eingesetzt. Letzteres trifft zum Beispiel auf den Quanten-Schlüsselaustausch zu. Die dabei überbrückten Distanzen sind allerdings noch eher gering. Die Dekohärenz von Qubits macht die Überwindung großer Distanzen zu einer großen Herausforderung. Um das Potenzial der Quantenkommunikation auszuschöpfen, braucht es große und stabile Quantennetzwerke, vielleicht sogar ein Quanteninternet. Genau an diesem Prozess der Skalierung von Quantennetzwerken wird daher hart gearbeitet. Technische Lösungen können z. B. sogenannte Quantenrepeater oder Trusted Nodes sein. Quantenrepeater basieren auf der Verschränkung und »erneuern« in gewisser Weise den Zustand eines versendeten Qubits. Trusted Nodes sind kein Quantenbauteil im eigentlichen Sinn. Auch sie sollen die Sendereichweite von Daten erhöhen, ihnen muss allerdings vertraut werden, da hier die per Qubits übertragene Information einsehbar ist, d. h. die Informationsübertragung ist in diesem Fall nicht inhärent abhörsicher. Zudem funktioniert die Übertragung von Daten bei der Quantenkommunikation entweder auf dem direkten Weg durch die Luft (z. B. Satellit zu Stationen auf der Erdoberfläche) oder per Glasfaserkabel. Die weit verbreiteten Kupferleitungen sind hier im Gegensatz zur klassischen Kommunikationstechnologie technisch beispielsweise nicht geeignet, d. h. zum Aufbau von großen Quantennetzwerken sind neben Know-how, Sende- und Empfangsgeräten sowie Zwischenstationen auch noch viele, gut verteilte Verbindungsstrecken erforderlich.

6.2. QUANTENPROGRAMMIERSPRACHEN, ZUGÄNGE, PLATTFORMEN

Trotz der zahlreichen Fortschritte in den letzten Jahren im Bereich Quantencomputing und ersten Meldungen zum Erreichen des Quantenvorteils, ist die Nutzung und Programmierung - selbst bei ausgereifter Hard- und Software – im Vergleich zur klassischen Informatik noch sehr komplex. Diese Komplexität kommt daher, dass die Quantenprogramme bisheriger Sprachen in der Regel aus elementaren Anweisungen für Quantencomputer, den sogenannten Quantengattern, bestehen. Diese Anweisungen erinnern an Maschinencode und Assemblersprache aus den Anfängen der klassischen IKT. Dementsprechend sind umfangreiche Kenntnisse zu Quantenmechanik und linearer Algebra notwendig, um Quantenprogramme zu schreiben. Und selbst für ausgewiesene Experten wird die Komplexität der Quantenprogramme mit steigender Anzahl an Qubits zu groß, um die Anweisungen noch manuell zu setzen. Um diese Komplexität zu verringern, muss der Schritt weg von einer Maschinencode-ähnlichen Programmierung hin zu einer Formulierung durch eine höhere Programmiersprache getan werden. Dazu gibt es erste Initiativen, die jedoch aufgrund der Eigenschaften von Quantencomputern von den gewohnten klassischen Paradigmen abweichen und entsprechend eine vergleichsweise hohe Einstiegshürde haben. Einige dieser Ansätze werden in der Infobox näher beleuchtet.

Um Quantencomputer in der Praxis nutzen zu können, müssen neben den Quantenprogrammiersprachen auch Plattformen bereitgestellt werden, über die ein einfacher Zugriff auf Quantencomputer verschiedener Anbieter möglich ist. Im Idealfall bieten diese Plattformen auch direkt einen Leistungsvergleich der verfügbaren Quantencomputer, sodass Nutzer:innen das für sie passende Modell wählen können. In der Praxis kann das so aussehen, dass ein Programm direkt auf einer Onlineplattform entwickelt und dann über diese Plattform an den entsprechenden Quantenrechner weitergegeben wird. Damit es auf diesem auch ausgeführt werden kann, muss das Quantenprogramm in Steuerpulse übersetzt werden. Diese Aufgabe übernehmen Compiler und Firmware, deren komplexe Abläufe und Programmierung jedoch vor den Anwender:innen versteckt werden. Für die Nutzer:innen ist dann nur das vom Quantencomputer berechnete Ergebnis sichtbar.

[34] Matt Swayne (2020): »TQD Spotlight: Zurich Instruments' Quantum Analyzer Aimed at Real-time Multi-Qubit Readout«. https://thequantumdaily.com/2020/10/12/tqd-spotlight-zurich-instruments-quantum-analyzer-aimed-at-real-time-multi-qubit-readout/. Zuletzt abgerufen am 20.10.2021.

Exkurs: Beispiele für existierende Software-Frameworks, -plattformen & Programmiersprachen

tket von Cambridge Quantum Computing ist ein Software-Framework mit einem Compiler und sehr effizienten Optimierungen. Die Bedienung ist dagegen noch sehr kleinschrittig. Ein Projekt, welches darüber hinausgeht, ist die Hochsprache Silq der ETH Zürich. Silq beinhaltet bereits einige Eigenschaften einer höheren Programmiersprache, bietet aber keinen Compiler und auch keine Möglichkeit, Programme nach einer Übersetzung auf physikalischen Backends auszuführen, d. h., Silq kann derzeit nur auf speziellen Simulatoren eingesetzt werden. Weil Quantenfehlerkorrektur noch sehr hardwarenah erfolgt, steht Silq dementsprechend auch nicht auf einem quantenfehlerkorrigierten Fundament.

Die wohl momentan etablierteste Plattform als Schnittstelle zu einem Quantencomputer-Backend ist IBMs Qiskit. Der Programmierstil ist bisher meist Assembler-artig, entwickelt sich durch spezielle Anwendungsmodule, zum Beispiel für Machine Learning oder naturwissenschaftliche Simulationen, jedoch mehr und mehr zu einer Sprache, die für Spezialist:innen aus den entsprechenden Fachbereichen nutzbar ist. Zu Qiskit ähnliche Entwicklungen sind etwa Braket (Amazon), Q# (Microsoft) oder Cirq (Google). Eine Sonderstellung nimmt das Framework Ocean ein, da dieses für die Quanten-Annealer von D-Wave und nicht für gatterbasierte Quantencomputer konzipiert wurde.

Als Entwicklungsplattform, die auch den Zugriff auf Hardware verschiedener Anbieter ermöglicht, ist Strangeworks hervorzuheben. Über diese Plattform ist es möglich, Quantenprogramme in fast allen oben genannten Sprachen zu entwickeln und diese auch auf den dazugehörigen Backends ausführen zu lassen. Eine höhere Quantenprogrammiersprache oder einen Vergleich verschiedener Hardwareansätze bietet jedoch auch Strangeworks nicht. Auch Interoperabilität, hier das Schreiben von Quantenprogrammen in einem bestimmten Software-Framework und das Ausführen auf anderen, nicht dafür vorgesehen Backends, ist bisher nicht gegeben.

6.2.1 Offene Probleme

Die meisten der aktuell genutzten Software-Frameworks werden von großen US-amerikanischen Firmen entwickelt. Ergänzt werden diese z. B. durch Angebote aus Kanada, Großbritannien und der Schweiz. Um die Souveränität und damit auch Datenhoheit bei der zukünftigen Nutzung von Quantencomputern für die mittelständische Wirtschaft in Deutschland und Europa zu gewährleisten, ist die Entwicklung von Open-Source-Software-Frameworks, bestehend aus Quantenprogrammiersprachen, dazugehörigen Compilern, Schnittstellen zur Quantenfirmware und zu Quantenmiddleware zu empfehlen.

Betrachtet man die gegenwärtigen kommerziellen Angebote, bieten im Wesentlichen einige wenige große Firmen ein für ihre Hardware optimiertes Software-Framework. Möchte ein Unternehmen einen Quantencomputer nutzen, da es für einen konkreten Anwendungsfall einen Vorteil identifizieren konnte, muss es sich für eines der Software-Frameworks entscheiden und das zu lösende Problem auf dieses adaptieren. Das birgt aber die Gefahr eines Vendor Lock-in. Möchte das Unternehmen einen Quantencomputer eines anderen Anbieters nutzen, weil dieser Computer sich schneller entwickelt hat oder für das Problem besser geeignet ist, muss in der Regel das Software-Framework gewechselt werden. Der gesamte Quellcode muss angepasst werden, was gerade für kleinere und mittelständische Unternehmen, die in Deutschland eine sehr wichtige wirtschaftliche Rolle einnehmen, finanziell und personell kaum zu leisten ist. Standardisierte Schnittstellen zwischen Quantenmiddleware, Quantenfirmware und Quantencompilern können dabei helfen, diesen Vendor Lock-in zu vermeiden, indem sie eine universelle Anbindung mehrerer Hardwarearchitekturen an ein Software-Framework ermöglichen. Solche Schnittstellen könnten im Rahmen von Standardisierungsaktivitäten in offenen Verfahren konzipiert und verfeinert werden.

Ein weiteres offenes Problem besteht in den aktuell etablierten Assembler-artigen Sprachen, die den Programmieralltag sehr repetitiv und kleinschrittig gestalten. Zudem sind Funktionen zum automatisierten Speichermanagement oder zur automatisierten Quantenfehlerkorrektur in den Paketen führender Anbieter nicht vorhanden. Solche Aufgaben müssen derzeit von Entwickler:innen manuell gehandhabt werden und erfordern häufig die Auseinandersetzung mit einzelnen (physischen) Qubits. Dies verlangsamt die Softwareentwicklung und steigert die Wahrscheinlichkeit von Fehlern bei der Programmierung.

Zudem sind sehr gute quantenphysikalische Kenntnisse erforderlich, was zu einer hohen Einstiegshürde beiträgt. Entsprechend existieren nur wenige erfahrene Quantenprogrammierer:innen weltweit. Damit Quantencomputing langfristig möglichst vielen Unternehmen einen Mehrwert bietet, ist es (neben der Hardwareentwicklung) von höchster Priorität, auch Nicht-Quantenphysiker:innen den Umgang mit Quantencomputern zu ermöglichen. Die Lösung besteht in der Entwicklung einer höheren Quantenprogrammiersprache, die viele der kleinschrittigen Elemente automatisiert. Diese Sprache ist bestenfalls leicht zugänglich und an etablierte Paradigmen angelehnt. So könnten interessierte klassische Entwickler:innen dazu befähigt werden, mit vergleichsweise wenig Beratung und Schulung Quantenprogramme selbst zu schreiben, sodass letztendlich das Potential von Quantencomputern in der Breite genutzt werden kann.

Neben der Entwicklung der Software ist natürlich auch ein Zugriff auf die Hardware notwendig. Damit Nutzer:innen das für ihr Problem am besten passende System wählen können, wäre eine Plattform erforderlich, die den Zugriff auf verschiedene Systeme verschiedener Anbieter ermöglicht und einen Leistungsvergleich (Benchmarking) dieser Systeme bietet. Dazu gehört auch eine interoperable Quantenprogrammiersprache, sodass in dieser Sprache geschriebene Programme auf einer Vielzahl verschiedener Quantencomputer ausgeführt werden können. Eine solche Plattform und eine derartige Sprache existieren aktuell noch nicht.

6.3. FACHKRÄFTE, WISSEN, BILDUNG

6.3.1 Erforderliche Kenntnisse

Quanten-IKT unterscheidet sich grundsätzlich von klassischer IKT. Daher erfordert Quanten-IKT auch andere Fähigkeiten und Kenntnisse. Sowohl die Kombination als auch das Level der erforderlichen Fähigkeiten und Kenntnisse ist dabei rollenabhängig. An dieser Stelle wird dies aus den Perspektiven von Entscheider:innen aus Wirtschaft oder öffentlicher Verwaltung einerseits und von Fachkräften für Quantensoftware und -hardware andererseits betrachten.

Entscheider:innen benötigen keine ausgeprägten quantenphysikalischen oder mathematischen Kenntnisse. Die Kenntnisse sollten lediglich ausreichen, um Stärken, Schwächen und Potenziale von Quanten-IKT einschätzen zu können. Darüber hinaus sollten Entscheider:innen einen Überblick über den Stand der Technik, gängige Anwendungsszenarien und Einschätzungen zur zukünftigen Entwicklung haben. Kurzum: Entscheider:innen sollten die Fähigkeit haben, die Frage beantworten zu können, welche Auswirkungen praxisreife Quanten-IKT auf ihre Organisation haben würde. Dies betrifft z. B. Chancen für Wettbewerbsvorteile bis hin zur Bedrohung der Funktionstüchtigkeit der Organisation. Aufgrund des disruptiven Potenzials (z. B. beschrieben in Kapitel 3) der Quanten-IKT sollten Entscheider:innen diese Frage so früh wie möglich, am besten schon heute, beantworten können. Wenn abgewartet wird, bis die Praxisreife bei Quanten-IKT erreicht ist, wird es in vielen Fällen schon zu spät sein. Dies betrifft zum Beispiel Daten, die langfristig geheim gehalten werden müssen, also etwa Geschäftsgeheimnisse oder personenbezogene Daten. Angriffe unter Einsatz von Quantencomputern bedrohen nämlich gängige Verschlüsselungsverfahren, weshalb schnellstmögliches Handeln erforderlich ist. Dies wird in Kapitel 6.4 dargelegt.

Fachkräfte sollen Hardware und Software weiterentwickeln, um Performanz, Fehleranfälligkeit und Skalierbarkeit von Quanten-IKT zu verbessern. Im Hardwarebereich bedeutet dies z. B., dass an der Weiterentwicklung von Qubits sowie von Geräten, die die Messung, Kontrolle und Stabilität von Quanten-IKT ermöglichen, gearbeitet wird. Der Softwarebereich umfasst den Entwurf, die Implementierung und das Testen von Algorithmen und Protokollen. Die Quanten-Softwareentwicklung erfolgt dabei (noch) sehr nah an der Hardware anstatt auf einem höheren Abstraktionslevel (siehe Kapitel 6.2). Dies bedeutet, dass Fachkräfte in der Quanten-IKT neben Informatikkenntnissen je nach Aufgabengebiet solide bis hervorragende Kenntnisse im Bereich der Elektrotechnik und Quantenphysik haben müssen.[35] Zur Beschreibung und zum Verständnis der quantenphysikalischen Vorgänge sind dabei mathematische Kenntnisse aus den Bereichen der linearen Algebra und der Wahrscheinlichkeitstheorie erforderlich. Letztendlich ist also eine große Schnittmenge an Kenntnissen aus traditionell eher getrennten wissenschaftlichen Disziplinen vonnöten. Gefragt sind zudem praktische Erfahrungen im Bereich physikalischer Laborexperimente sowie im Umgang mit realer, also nicht durch klassische IKT simulierter Quanten-IKT. Als junge Technologie bietet die Quanten-IKT noch viele unbewältigte und komplexe Hürden, weshalb eine ausgeprägte Problemlösungsfähigkeit wichtig ist. Fachkräfte arbeiten zudem häufig mit Personen zusammen, deren Fachwissen weniger ausgeprägt ist oder die einen komplett anderen Ausbildungshintergrund haben. Dementsprechend müssen

[35] Als Nachweis der Qualifikation wird hier oftmals ein Doktortitel im Bereich Quantenphysik erwartet.

Fachkräfte die Fähigkeit haben, die komplizierten Inhalte und Ergebnisse ihrer Arbeit zielgruppengerecht und verständlich zu kommunizieren.

6.3.2 Fachkräftemangel?

Fachkräfte im Bereich der Quanten-IKT müssen über einen bisher ungewöhnlichen und daher seltenen Mix von Fähigkeiten und Kenntnissen verfügen. Aufgrund des sich abzeichnenden Wachstums der Branche[36] liegt es daher nahe, dass es bei den verfügbaren Fachkräften zu einem Engpass kommen könnte. Dementsprechend ist es auch nicht verwunderlich, dass innerhalb der Quanten-IKT-Branche von einem steigenden Fachkräftemangel ausgegangenen wird.[37] Verlässliche Zahlen hierzu sind allerdings Mangelware, weshalb an dieser Stelle Forschungsbedarf besteht. Hierbei sollten nicht nur die Anzahl und die Entwicklung der offenen Stellen erfasst werden, sondern auch, welche Fähigkeiten und Kenntnisse in welcher Mischung gefragt sind und was potenziellen Arbeitnehmer:innen geboten wird, z. B. bezüglich Gehalt, Benefits und Verträgen ohne Befristung.

6.3.3 Bildung und Bildungsangebote

Die erforderliche Mischung aus Kenntnissen wird innerhalb etablierter und weit verbreiteter Bildungsangebote (z. B. den Studienfächern Informatik und Physik) nicht geboten. Diese Kenntnisse werden derzeit daher noch oft in Eigeninitiative erworben, was keine gute Basis ist, um einem möglichen Fachkräftemangel vorzubeugen. In den letzten Jahren sind einige Ausbildungsmöglichkeiten zu Quanten-IKT entstanden. Zum Beispiel bieten die TU München und die Ludwig-Maximilians-Universität München seit 2020 gemeinsam den Masterstudiengang »Quantum Science & Technology« an.[38] Die Universität des Saarlandes bietet seit 2019 den Bachelorstudiengang »Quantum Engineering« an, 2020 folgte der Masterstudiengang.[39] Im Jahr 2019 vereinbarten das Forschungszentrum Jülich und Google eine Partnerschaft, welche unter anderem die Ausbildung von Fachkräften zum Ziel hat.[40] Des Weiteren bietet die Staatliche Universität Sankt Petersburg Kurse zu Quantencomputing auf der Onlinelernplattform Coursera an.[41]

Neben Ausbildungsangeboten sind auch Weiterbildungsmöglichkeiten für interessierte Fachkräfte gefragt. Bildungsangebote sollten bestenfalls modular aufgebaut sein, sodass sich Fachkräfte abhängig von ihren bestehenden Kenntnissen, also etwa ihrer ursprünglichen Fachrichtung, zielführend weiterbilden können. Parallel dazu besteht, wie in Kapitel 6.2 beschrieben, auch die Möglichkeit, höhere Quantenprogrammiersprachen zu entwickeln, um so z. B. klassischen Softwareentwickler:innen entgegen zu kommen.

Damit zukünftige Fachkräfte Erfahrung sammeln können, sind zudem freie oder zumindest kostengünstige Zugänge zu Quantenhardware erforderlich. Aufgrund dessen, dass die Programmierung dieser Hardware je nach Anbieter unterschiedlich funktioniert (siehe Kapitel 6.2), ist hier insbesondere der Zugang zu Hardware einer Bandbreite von Anbietern gefragt.

Die Aus- und Weiterbildung von Fachkräften alleine wird aus deutscher und europäischer Perspektive jedoch nicht reichen. Um eine Talentabwanderung zu verhindern, müssen auch Anreize geschaffen werden, um einheimische Fachkräfte zu halten und eventuell auch außereuropäische Fachkräfte zu gewinnen. Dies kann z. B. über Gehalt, aber auch über Freiheiten in der Arbeitsgestaltung, langfristiger Forschungsperspektive (angekurbelt etwa durch langfristige Förderung), Offenheit von Vorgesetzten sowie interessante und vielfältige Arbeitsinhalte (etwa durch eine gewisse Breite bei der Forschung zu und Entwicklung von Quanten-IKT) erfolgen.

---

[36] Beispielsweise nachvollziehbar anhand des prognostizierten Marktvolumens unter https://www.bcg.com/publications/2019/quantum-computers-create-value-when. Zuletzt abgerufen am 20.10.2021.

[37] Beispielsweise:
1) MIT News (2019): »Q&A: The talent shortage in quantum computing«. https://news.mit.edu/2019/mit-william-oliver-qanda-talent-shortage-quantum-computing-0123. Zuletzt abgerufen am 23.08.2021.
2) VDI Technologiezentrum GmbH (2017): »Förderung von Quantentechnologien – Positionspapier der deutschen Industrie«. S. 25. https://www.photonikforschung.de/media/quantentechnologien/pdf/Quantentechnologie_bf.pdf. Zuletzt abgerufen am 23.08.2021.
3) ZDNet (2021): »Quantum computing's next big challenge: A quantum skills shortage«. https://www.zdnet.com/article/quantum-computings-next-challenge-finding-quantum-developers-and-fast/. Zuletzt abgerufen am 23.08.2021.

[38] FAZ (2021): »Wie man sich auf KI spezialisieren kann«. https://www.faz.net/aktuell/karriere-hochschule/wie-man-sich-auf-ki-spezialisieren-kann-17388612.html. Zuletzt abgerufen am 23.08.2021.

[39] Studienangebot der Universität des Saarlandes. Links: https://www.uni-saarland.de/studium/angebot/master/quantum-engineering.html bzw. https://www.uni-saarland.de/studium/angebot/bachelor/quantum-engineering.html. Zuletzt abgerufen am 23.08.2021.

[40] Forschungszentrum Jülich (2019): »Quantencomputer: Forschungszentrum Jülich und Google vereinbaren Partnerschaft«. https://www.fz-juelich.de/SharedDocs/Pressemitteilungen/UK/DE/2019/2019-07-08-quantencomputer-fzj-google.html. Abgerufen am 23.08.2021.

[41] https://de.coursera.org/specializations/quantum-computing-from-basics-to-the-cutting-edge. Zuletzt abgerufen am 23.08.2021.

Letztlich müssen Kenntnisse zur Quanten-IKT auch in die Entscheiderebene hineingetragen werden. Neben Publikationen wie der vorliegenden könnten sich hier auch auf die Bedürfnisse von Entscheider:innen zugeschnittene Vorträge und insbesondere Workshops eignen.

6.4. POST-QUANTEN-KRYPTOGRAFIE

Quantencomputer haben erhebliche Auswirkungen auf die Sicherheit heute eingesetzter kryptografischer Verfahren. Bei symmetrischen Verschlüsselungsverfahren (wie z.B. AES) reduziert sich die Schlüsselsuche durch einen von Lov Grover 1996 entwickelten Suchalgorithmus für Quantencomputer, die Sicherheit kann aber durch die Verdoppelung der Schlüssellänge wieder auf das ursprüngliche Niveau gehoben werden.

Viel stärker wirken sich Quantencomputer aber auf aktuell genutzte Public-Key-Verfahren aus. Ein von Peter Shor 1994 entwickelter Algorithmus bricht effizient kryptografische Verfahren, die auf dem Faktorisierungsproblem basieren (z.B. RSA-Verschlüsselung und RSA-Signatur). Mit einer ähnlichen Idee lassen sich auch Verfahren brechen, die auf dem Problem der Berechnung diskreter Logarithmen basieren (z.B. Signaturverfahren DSA, Verschlüsselungsverfahren Elgamal und Schlüsseleinigungsverfahren Diffie-Hellman). Eine Anpassung der Schlüssellänge wie bei symmetrischen Verfahren ist hier nicht möglich, weil diese soweit erhöht werden müsste, dass z. B. die Schlüsselgenerierung nicht mehr effizient durchführbar ist.

Damit werden nahezu alle der heute eingesetzten Public-Key-Verfahren (Signatur-, Schlüsselaustausch- und Verschlüsselungsverfahren) unsicher. Da die in symmetrischen Verfahren genutzten kryptografischen Schlüssel auf Basis der oben aufgeführten Public-Key-Verfahren vereinbart werden (authentisierte Schlüsselaustauschverfahren), ist auch die symmetrische Verschlüsselung betroffen. Angreifer könnten mithilfe von Quantencomputern die Sicherheit von Schlüsselaustauschverfahren aushebeln und so die kryptografischen Schlüssel extrahieren oder Man-in-the-Middle-Angriffe durchführen. Dies betrifft alle aktuell verwendeten kryptografisch abgesicherten Internetverbindungen (z. B. https-Verbindungen oder Virtual Private Networks (VPN)).

Die NSA warnt bereits vor den Auswirkungen von Quantencomputern und hat eine Migration hin zu quantencomputerresistenten Verfahren eingeleitet.[42] Auch das BSI hat sich des Themas angenommen.[43] Darüber hinaus hat das NIST im Jahr 2017 einen Standardisierungsprozess für quantencomputerresistente Verfahren gestartet, die ISO hat ebenfalls Aktivitäten begonnen.[44] Weiter fördert das BMBF Verbundprojekte zum Thema Post-Quanten-Kryptografie.[45]

Die meisten Expert:innen gehen davon aus, dass spätestens ab 2030 Quantencomputer existieren, die die heute eingesetzten Public-Key-Verfahren brechen. Seit den Veröffentlichungen des ehemaligen CIA-Mitarbeiters Edward Snowden ist bekannt, dass die amerikanischen Geheimdienste große Mengen an Internetkommunikation für eine spätere Auswertung speichern. Damit lassen sich die heute verwendeten Schlüsselaustauschverfahren später mittels Quantencomputer brechen und die darauf aufgebaute sichere Kommunikation nachträglich entschlüsseln. Gerade für Dokumente, für die die Vertraulichkeit über mehrere Jahre garantiert werden muss, besteht damit dringender Handlungsbedarf: Für langlebige Sicherheit müssten schon heute quantencomputerresistente Verfahren für den Schlüsselaustausch eingesetzt und die Schlüssellänge symmetrischer Verfahren auf 256 Bit hochgesetzt werden. Dies ist bisher nicht flächendeckend der Fall.

Die Gründe für die verspätete Umsetzung sind vielfältig. So ist der IT-Sicherheitsmarkt in Deutschland stark fragmentiert. Änderungen an Sicherheitsprodukten sind aufgrund der in der Regel notwendigen Zertifizierungsprozesse sehr kostenintensiv. Die deutschen Unternehmen der Sicherheitsindustrie sind damit nicht in der Lage, hier in Vorleistung zu gehen. Des Weiteren werden Sicherheitsprodukte, insbesondere Kryptohardware, nicht nur über Jahre, sondern häufig Jahrzehnte eingesetzt, auch weil ein Austausch aufgrund häufig fehlender Migrationsstrategien mit hohen Kosten verbunden ist (Stichwort Krypto-agilität). Außerdem besteht aktuell bei vielen Bedarfsträger:innen

[42] Tom Simonite (2016): »NSA Says It «Must Act Now" Against the Quantum Computing Threat«. https://www.technologyreview.com/2016/02/03/162433/nsa-says-it-must-act-now-against-the-quantum-computing-threat/. Zuletzt abgerufen am 20.10.2021.

[43] Weitere Informationen dazu unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Quantencomputing/entwicklungsstand-quantencomputer_node.html. Zuletzt abgerufen am 20.10.2021.

[44] Siehe etwa https://csrc.nist.gov/projects/post-quantum-cryptography. Zuletzt abgerufen am 20.10.2021.

[45] Siehe etwa https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk. Zuletzt abgerufen am 20.10.2021.

aus Wirtschaft und Verwaltung kein Bewusstsein für die Risiken durch Angriffe unter Einsatz von Quantencomputern (mehr zu erforderlichen Kenntnissen in Kapitel 6.3), weil die Existenz ausreichend großer Quantencomputer noch in der Zukunft liegt.

Dies alles hat dazu geführt, dass nicht rechtzeitig auf quantencomputerresistente Verfahren umgestellt wird. Häufig benötigen solche Aktualisierungen einen sehr langen Zeitraum. So wird z. B. in der Finanzbranche heute immer noch der Verschlüsselungsalgorithmus Triple-DES in einigen Komponenten eingesetzt, obwohl seit 2000 der Nachfolgestandard AES existiert und das BSI seit dieser Zeit dazu rät, Triple-DES durch AES zu ersetzen.

Um den Bedrohungen für die Kryptografie durch Angriffe mittels Quantencomputern begegnen zu können, sollten kurzfristig die folgenden Themen bearbeitet werden:

- Schaffung des Bewusstseins für die Bedrohung und die Risiken bei den Bedarfsträger:innen
- Auswahl bzw. Entwicklung geeigneter quantencomputerresistenter Verfahren für die Sicherheitsziele Vertraulichkeit, Authentizität und Integrität für unterschiedliche Einsatzzwecke
- Gezielte Nutzung der Ergebnisse aus den vom BMBF geförderten Verbundprojekten zur Post-Quantum-Kryptografie
- Analyse, bei welchen Bedarfsträgern Sicherheitsprodukte kurz-, mittel- und langfristig aktualisiert werden müssen und Erarbeitung einer Prioritätenliste
- Erarbeitung von Migrationsstrategien für unterschiedliche Einsatzzwecke, Sicherheitsniveaus und Prioritäten
- Erarbeitung und Veröffentlichung empfohlener Vorgehensweisen für unterschiedliche Anforderungen und Bereiche der kritischen Infrastrukturen

6.5. DEN ÜBERBLICK BEHALTEN

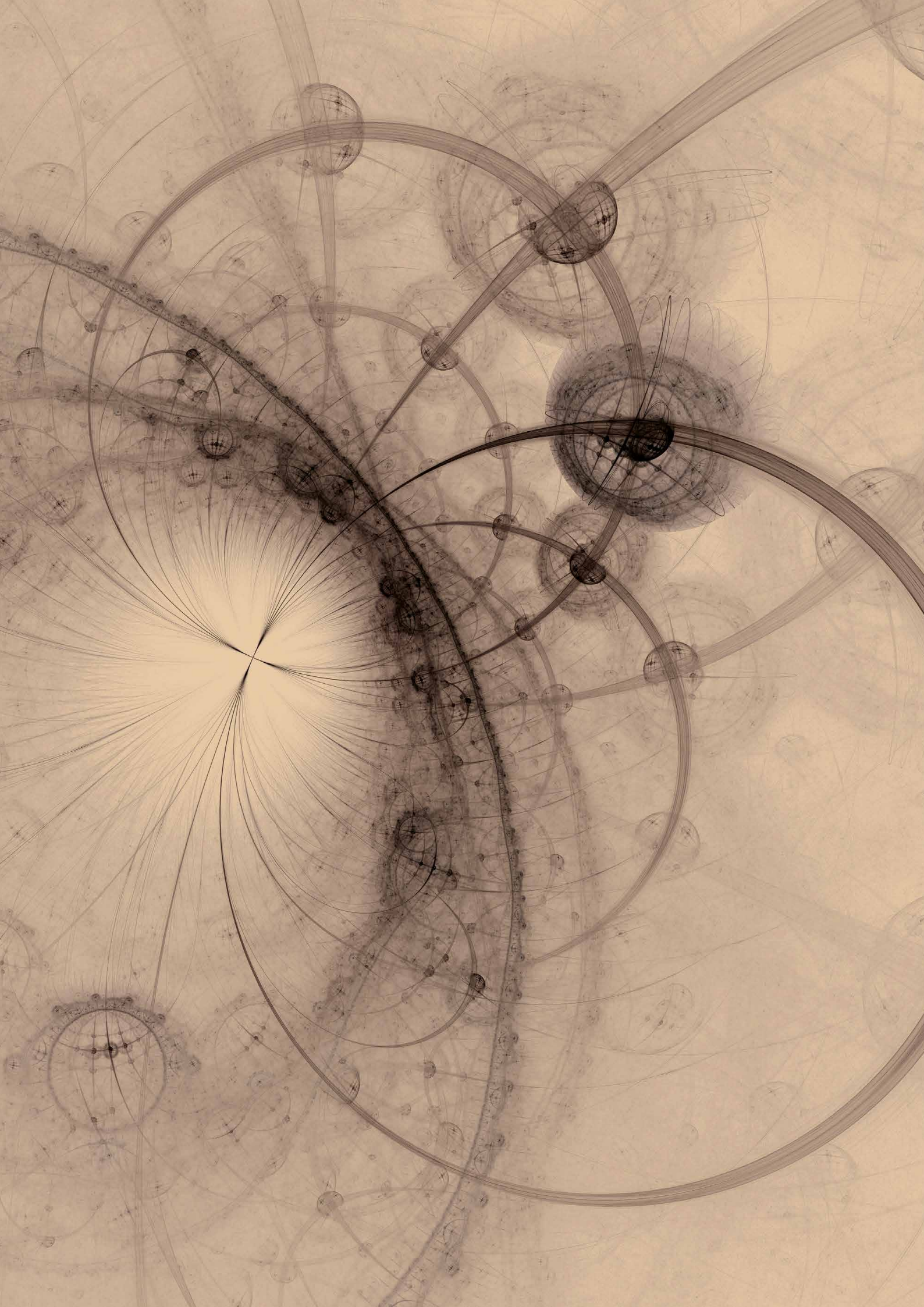
Quanten-IKT entwickelt sich rasch und parallel in verschiedenen Bereichen, von unterstützenden Technologien und Hardware über Algorithmen, Software, Plattformen, Bildungsangebote und Förderprogramme bis hin zu Unternehmensgründungen, Kooperationen und der Erschließung von Anwendungsbereichen. Dabei verfolgen unterschiedliche Akteure unterschiedliche Ansätze, etwa bezüglich der Programmiersprachen und der Qubitkonstruktionsweise. Entsprechend schwierig ist es, einen Gesamtüberblick zur Breite, zum technischen Stand und zu möglichen Entwicklungspfaden zu behalten.

Ein solcher Überblick ist ein Schlüssel, um eine Erfolg versprechende Strategie zu entwickeln, diese gegebenenfalls an veränderte Bedingungen anzupassen und einzelne Maßnahmen zu veranlassen. Dies ist zum Beispiel relevant, um zu ermitteln, wie konkurrenzfähig und souverän Deutschland und Europa bezüglich verschiedener Bereiche der Quanten-IKT sind und wo Handlungsbedarf besteht.

Eine Lösungsmöglichkeit hierfür ist ein strategisches Monitoring, das mithilfe von Expert:innen entwickelt und durch quantitative Analysen gestützt wird. In regelmäßigen Abständen könnte so der Stand der Quanten-IKT weltweit, im europäischen Raum und in Deutschland anhand von Indikatoren ermittelt und verglichen werden. Gegenstände eines solchen Monitorings könnten z. B. sein:

- der derzeitige und zukünftige Fachkräftemangel (siehe auch Kapitel 6.3)
- existierende Software-Frameworks und ihre Eigenschaften
- aktueller Stand der Umstellung auf Post-Quanten-Kryptografie
- Qubitkonstruktionsweisen
- Patentlandschaft zu Quanten-IKT
- Pilotprojekte zur Anwendung von Quanten-IKT
- mögliche Anwendungen im öffentlichen Sektor

Die Ergebnisse eines solchen Monitorings könnten in erster Linie politischen Entscheidungsträger:innen bei strategischen Entscheidungen helfen, aber auch die Umsetzung von Quanten-IKT-Projekten erleichtern. Denkbar wäre zudem, die Ergebnisse öffentlich zur Verfügung zu stellen, sodass sich gerade kleine und mittelständische Unternehmen, für die ein solches Monitoring in Eigenregie zu aufwändig wäre, informieren und Chancen ergreifen können.



7. ENTWICKLUNGSPERSPEKTIVE

7.0.1 Reife der Technologie

Aus den vorangegangenen Kapiteln wird deutlich, dass Quantencomputing und Quantenkommunikation zur Lösung bestimmter Problemklassen nicht nur in der Theorie klassischen Rechnermodellen und Übertragungstechniken überlegen sind, sondern erwartet wird, dass sich dies auch für konkrete und relevante Anwendungen nutzbar machen lässt. Gestützt wird diese Erwartung u. a. durch erste, noch konstruierte Beispiele, die unter dem Stichpunkt »Quantum Supremacy«[46] bereits den Nachweis einer Überlegenheit des Quantencomputing für eine bestimmte Problemstellung in der Praxis behaupten. Im Falle der Quantenkommunikation existieren überdies zum sicheren Schlüsselaustausch (Quantum Key Distribution) sogar bereits erste kommerzielle Lösungen, allerdings sind die dabei überbrückbaren Distanzen noch gering (siehe auch Abschnitt 3.4), während solche Einschränkungen bei klassischer Kommunikation praktisch nicht existieren.

Als mögliche Schlüsseltechnologie betrachtet, befindet sich die Quanten-IKT bislang noch in einem frühen Stadium. Die Laborphase ist zwar bereits fortgeschritten und zeigt mehr und mehr Erfolge, dauert aber an. Erste Anwendungen der Quantenkommunikation finden bereits ihren Weg in die Praxis, Anwendungen des Quantencomputings und eine breitere Verfügbarkeit und Nutzbarkeit kommerzieller Lösungen werden erwartet, stehen aber noch aus. Erste kommerziell nutzbare Quantencomputer stehen mittlerweile zur Verfügung, womit die Schwelle für hierauf aufbauende Forschungs- und Entwicklungsaktivitäten gesenkt und die Verbreitung des Know-how zur Quanten-IKT insgesamt gefördert wird.

Technische Herausforderungen liegen insbesondere in der noch geringen Anzahl von Qubits und deren Genauigkeit (Fidelity) sowie dem Rauschen, der Dekohärenz und der hohen Störanfälligkeit – man spricht hier von der sogenannten NISQ-Ära des Quantencomputings (Noisy Intermediate-Scale Quantum Computing). Bei der Quantenkommunikation ist die Reichweite der weitgehend fehlerfreien Übermittlung von Qubits noch begrenzt, die Skalierung zu Netzwerken ist hier eine zentrale Herausforderung. Im Wesentlichen sind es diese Einschränkungen, die praxisrelevante Anwendungen derzeit noch verhindern.

7.0.2 Abschätzung der weiteren Entwicklung

Die »Roadmap Quantencomputing« des Expertenrats der Bundesregierung zum Thema Quantencomputing[47] geht von der Realisierbarkeit erster praxisrelevanter Anwendungen in fünf bis zehn Jahren und einer breiteren Spanne von Anwendung in

[46] Zu Quantum Supremacy siehe z.B. https://de.wikipedia.org/wiki/Quantenüberlegenheit. Zuletzt abgerufen am 12.01.2022.

[47] VDI/BMBF: »Roadmap Quantencomputing« vom Januar 2021. https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Roadmap-Quantencomputing-bf-C1.pdf. Zuletzt abgerufen am 12.01.2022.

System	Ausbaustufe	Anzahl Qubits	Jahr
IBM Q System One	Falcon	27	2019
IBM Q System One	Hummingbird	65	2020
IBM Q System One	Eagle	127	2021
IBM Q System One	Osprey	433	2022
Next family of IBM Quantum systems	Condor	1121	2023
Next family of IBM Quantum systems	(large scale systems)	1.000.000	nach 2023

Tabelle 2: IBMs Roadmap für Quantencomputing

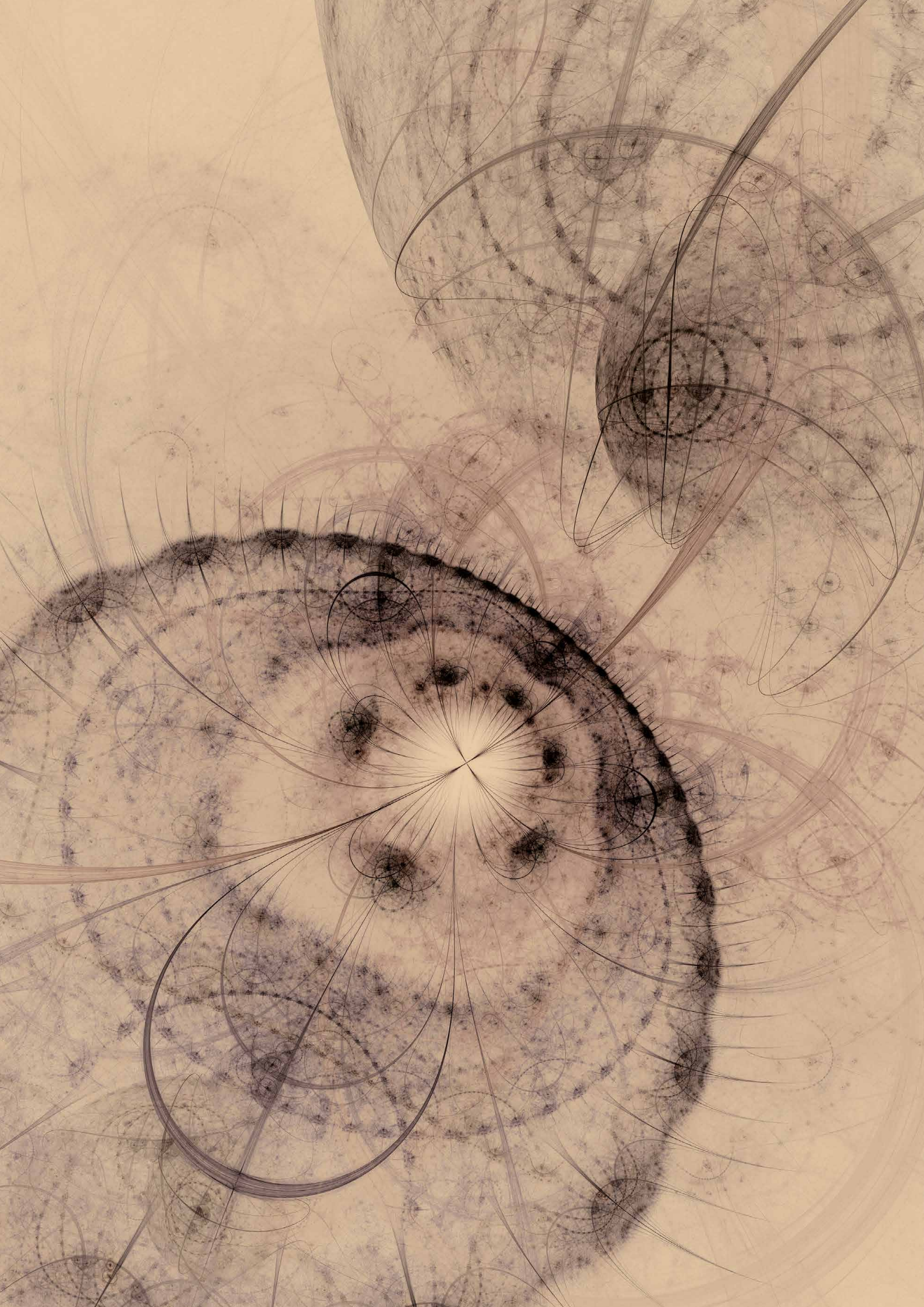
zehn bis fünfzehn Jahren aus. Als erster Schritt in diese Richtung wird hierzu u. a. der kurzfristige Aufbau eines umfassenden Ökosystems und fokussierter Strukturen für das Quantencomputing in Deutschland innerhalb der nächsten fünf Jahre vorgeschlagen. Aus dieser und weiteren Einschätzungen lässt sich ablesen, dass in Expertenkreisen derzeit mit einer breiteren praxisrelevanten Verfügbarkeit von Anwendungen des Quantencomputing in etwa zehn bis zwanzig Jahren gerechnet wird.

Hardware-seitig geben die Roadmaps der Hersteller von Quantenrechnern Hinweise auf die erwarteten Fortschritte der zugrunde liegenden Technologie. Hier ist insbesondere die Anzahl der Qubits ein entscheidender – wenn auch nicht der einzige – Parameter.[48] Das erste, im Juni 2021 in Deutschland eingeführte IBM Quantum System One (Falcon) aus 2019 verfügt beispielsweise über 27 Qubits. Der Sycamore-Quantenprozessor von Google verfügt ebenfalls seit 2019 bereits über 53 Qubits. Am Beispiel der IBM-Roadmap[49] für das Quantum System One lässt sich zudem ein Eindruck von bereits im Einsatz befindlichen (Falcon), vorgestellten (Hummingbird, Eagle) und zukünftig geplanten Ausbaustufen (Osprey, Condor) gewinnen (siehe Tabelle 2).

Hieran ist erkennbar, dass Hersteller von einem Durchbruch bei der Erhöhung der realisierbaren Qubitanzahl pro Quantenrechner ausgehen – die IBM-Roadmap lässt beispielsweise auf ein erwartetes exponentielles Wachstum in den nächsten Jahren schließen. Realisiert sich die Erwartung von Quantenprozessoren mit Tausenden oder Millionen von Qubits in absehbarerer Zeit, so kommen breite Anwendungen der Quanten-IKT tatsächlich bald in greifbare Nähe.

[48] Eine weitere ebenso wichtige Kennzahl ist beispielsweise die Genauigkeit (Fidelity, siehe auch Kapitel 6.1).

[49] https://www.datacenter-insider.de/ibm-enthuellt-roadmap-fuer-quantum-computing-software-a-1001849/. Zuletzt abgerufen am 12.01.2022.



8. HANDLUNGSEMPFEHLUNGEN

Post-Quanten-Kryptografie jetzt weiterentwickeln und frühestmöglich umsteigen.

Viele der derzeit etablierten kryptografischen Verfahren werden bei Fortentwicklung von Quantencomputern zukünftig nicht mehr sicher sein. Es ist sogar möglich, aktuellen Datenverkehr aufzuzeichnen und zu speichern, um die Daten zu entschlüsseln, sobald die technischen Möglichkeiten der Quantencomputer weit genug fortgeschritten sind. Auch kurzfristige Durchbrüche in der Quanten-IKT sind möglich. Es ist daher ratsam, die Entwicklung von Post-Quanten-Kryptografie voranzutreiben und die Ergebnisse frühestmöglich einzusetzen. Derartige Verfahren, die sowohl für klassische als auch quantenmechanische Rechner schwer zu überwinden sind, lassen sich mit klassischen Computern umsetzen.

Ökosystem aufbauen.

Um die Stärken Deutschlands und Europas in der Grundlagenforschung auch in Wertschöpfung umsetzen zu können, sollte ein Ökosystem für Quanten-IKT aufgebaut werden. Dazu bedarf es der Unterstützung wirtschaftlicher Aktivität im Bereich Quanten-IKT. Insbesondere KMUs, die zwar das Domänenwissen, aber keine Forschungs- und Bildungsmittel für solche innovativen, aber auch risikobehafteten Technologien besitzen, können von einer regen Zusammenarbeit mit den Expert:innen aus Forschungseinrichtungen und dem Zugang zu Plattformen für Quanten-IKT-Wissen profitieren. Diese Vernetzung von Wissenschaft und Wirtschaft gilt es in Zukunft im Rahmen von Forschungs- und Innovationsförderprogrammen weiter auszubauen. Zudem ist eine ausreichende Anzahl niedrigschwelliger Zugänge zu Quanten-IKT und zu klassischer IKT, die Quanten-IKT simuliert, erforderlich, damit experimentiert werden kann, Kenntnisse ausgebaut werden können und Algorithmen entwickelt und getestet werden können.

Wissen schaffen und teilen.

Um dem wachsenden Bedarf nach Kompetenzen zu begegnen, müssen Bildungsmöglichkeiten geschaffen werden. Das betrifft zum einen Ausbildungen, also Studiengänge und/oder -module, die das relevante Wissen aus Physik, Mathematik, Elektrotechnik und Informatik bündeln. Allerdings reicht es nicht aus, mehrere Jahre abzuwarten, bis die ersten Quanten-IKTler:innen ausgebildet wurden. Es ist daher sinnvoll, unterstützend dazu auch Weiterbildungsmaßnahmen zu ergreifen, die z. B. Informatiker:innen den Einstieg ermöglichen. Bei Entscheider:innen in öffentlicher Verwaltung und Wirtschaft sollten ebenfalls Kompetenzen aufgebaut werden, auch wenn hier nicht die gleiche Tiefe wie bei Fachkräften erforderlich ist. Hier geht es eher um einen guten Überblick über die Quanten-IKT-Landschaft.

Standardisierung vorantreiben.

Ein Erfolgsfaktor wird sein, die noch zu entwickelnden Standards zum Quantencomputing in Einklang mit den existierenden Standards im breiten Cloud- und KI-Markt zu bringen, um so unter anderem Kompatibilität, Erweiterbarkeit, Austausch und Vergleichbarkeit der Quantensoftware zu gewährleisten und eine leichtere Integration in gängige Werkzeuge und Anwendungen zu ermöglichen. Generell sind Standards für Schnittstellen etc. erforderlich für die Wettbewerbsfähigkeit und Souveränität, um z. B. Vendor-Lock-in-Effekte zu verhindern. Darüber hinaus werden Standards für die Schlüsselindikatoren gebraucht, die für das einheitliche Benchmarking, die Evaluation und die Qualitätssicherung von quantenbasierten Systemen verwendet werden sollen. Ein Hebel der öffentlichen Hand kann eine gezielte Förderpolitik sein, bei der z. B. die Verwendung offener Standards eine Rahmenbedingung von Projekten ist.

Marktlücken suchen und nutzen.

Es existieren Hardwareansätze, bei denen Akteure außerhalb Europas sich bereits Vorsprünge erarbeitet und mit entsprechenden Patenten gefestigt haben. Gleichzeitig gibt es noch viele Ansätze, die bislang in geringem Ausmaß verfolgt wurden, wie etwa die Konstruktion von Qubits auf Basis von Kunstdiamanten. Hier und in anderen Bereichen ist Deutschland stark in der Grundlagenforschung. Solche Ansätze stellen Chancen dar, Marktanteile zu erobern.

Anwendungsmöglichkeiten im öffentlichen Sektor identifizieren und erschließen.

Generell befindet sich die Wirtschaft im Zusammenhang mit Quanten-IKT gerade in einer Phase des Ausprobierens, bei der geeignete Anwendungsfelder konkret bestimmt werden sollen. Der öffentliche Sektor sollte hier mitmischen und mögliche Anwendungen (z. B. als Teil eines strategischen Monitorings)

identifizieren und zugehörige Pilotprojekte starten. Hierbei geht es nicht nur darum, wie Quanten-IKT dem öffentlichen Sektor nutzen kann. Aus strategischer Sicht sollte der öffentliche Sektor auch als früher Anwender von Quanten-IKT als Treiber der deutschen und europäischen Quanten-IKT auftreten. Dies ist insbesondere vor dem Hintergrund von Interesse, dass sich Deutschland oftmals schwertut, exzellente Grundlagenforschung in Wertschöpfung umzusetzen. Ein solcher Trend ist auch bei der Quanten-IKT beobachtbar. Gerade bei einer noch mit Unsicherheit behafteten Technologie mit längerem Weg zur Praxisreife wie der Quanten-IKT kann der öffentliche Sektor helfen, Plätze im Wettbewerb gutzumachen bzw. den Anschluss zu halten.

Strategisch handeln.

Bei der Entwicklung von Quanten-IKT kann es durchaus zu Rückschlägen oder zwischenzeitlichem Stillstand kommen. Die Bereitschaft, dies zu akzeptieren und sich langfristig zu engagieren, kann entscheidend sein für zukünftige Marktverhältnisse. Daher sind Durchhaltevermögen und ein gewisses Maß an Flexibilität in der deutschen und europäischen Wirtschaft, Forschung und Politik gefragt, natürlich verbunden mit entsprechenden Förderungen. Zudem sollte bei der Entwicklung von Quanten-IKT gesamtheitlich vorgegangen werden. Das bedeutet z. B., dass sich nicht frühzeitig auf einzelne Konstruktionsweisen für Qubits konzentriert wird, sondern dass sich Europa hier breit aufstellt, um nicht in Sackgassen zu landen. Neben der Hardware sollten auch Algorithmen und Software weiterentwickelt werden. Zudem müssen Potenziale der Quanten-IKT weiter ausgelotet werden, d. h. Anwendungsfälle müssen identifiziert werden, in denen Quanten-IKT tatsächlich für deutliche Fortschritte sorgen kann.

Monitoring und strategische Vorausschau etablieren.

Quanten-IKT ist eine sich dynamisch entwickelnde Technologie auf dem Weg zur Praxisreife. Um die zukünftige Entwicklung und die damit verbundenen Auswirkungen einschätzen zu können, sollte der aktuelle Stand der Quanten-IKT kontinuierlich und systematisch (z. B. über Indikatoren) in Gesamtheit erfasst werden. Dies umfasst Themen von Steuerungstechnik und Qubitkonstruktionsweisen über Fehlerkorrektur bis hin zu Software und Plattformen. Auf Basis eines solchen Monitorings sollte zudem eine regelmäßige – z. B. jährliche – strategische Vorausschau etabliert werden. Aus europäischer Perspektive können zusammen mit Expert:innen auf Basis des aktuellen Stands wahrscheinliche Entwicklungen der Technologien und des Umfelds erarbeitet werden, z. B. durch Planspiele. Dies soll dazu dienen, um z. B. mögliche Monopole, die die Wettbewerbsfähigkeit der eigenen Wirtschaft behindern, und Abhängigkeiten, die die staatliche Handlungsfähigkeit erheblich einschränken, vorausschauend aufzudecken und durch geeignete Maßnahmen zu vermeiden.

KONTAKT

Jan Dennis Gumz
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-948582-12-8

22I01