Kompetenzzentrum Öffentliche IT

Forschung für den digitalen Staat

Jan Dennis Gumz, Dorian Wachsmann, Dorian Grosch

Das ÖFIT-Trendsonar Quanten-IKT

Gefördert durch:

Bundesministerium des Innern und für Heimat

Fraunhofer FOKUS

Impressum

Das Trendsonar interaktiv

Das Trendsonar Quanten-IKT ist auch in einer interaktiven Variante auf der Website des Kompetenzzentrums Öffentliche IT benutzbar. Durch das interaktive Trendsonar können Sie auf alle Informationen zu den behandelten Technologien online zugreifen. Darüber hinaus bietet Ihnen die interaktive Version die Möglichkeit, zwei Quanten-Technologien direkt miteinander zu vergleichen.

Das Trendsonar enthält Beschreibungen zu den analysierten Technologien sowie Einschätzungen von Expert:innen aus den Bereichen Quantencomputing und Quantenkommunikation. Einzusehen sind Bewertungen hinsichtlich Zukunftsfähigkeit, Reife- und Standardisierungsgrad sowie Angebot und Nachfrage. Zu jeder Technologie werden zudem quantitative Indikatoren zu Forschungsförderprogrammen, wissenschaftlichen Publikationen, Gründungen, Patenten, Suchanfragen sowie Sichtbarkeit in den Medien vorgestellt.

Das interaktive Trendsonar können Sie mit Smartphone, Tablet oder PC nutzen. Neben dem Trendsonar Quanten-IKT finden Sie auch unsere Trendsonare zu den Technologietrends aus den Bereichen Internet der Dinge, Künstliche Intelligenz und IT-Sicherheit unter:

www.oeffentliche-it.de/trendsonar

Autoren:
Jan Dennis Gumz, Dorian Wachsmann, Dorian Grosch

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: 978-3-948582-18-0

1. Auflage Januar 2023

Das letzte Abrufdatum der Onlinequellen in den Fußnoten ist der 12.01.2023.

Bildnachweis

Seite	Autoren	Quelle	geändert am:
1	Kanenori	pixabay	Collage (9.1.2023)
1	ID 5892437	pixabay	Collage (9.1.2023)
10	ID 4311868	pixabay	Collage (9.1.2023)
10	bjoisten	pixabay	Collage (9.1.2023)
15	ID 4311868	pixabay	Collage (9.1.2023)
15	ajoheyho	pixabay	Collage (9.1.2023)
21	confused_me	pixabay	Collage (10.1.2023)
21	ErikTanghe	pixabay	Collage (10.1.2023)
27	Ralphs_Fotos	pixabay	Collage (10.1.2023)
27	Fotoworkshop4You	pixabay	Collage (10.1.2023)
32	PollyDot	pixabay	Collage (10.1.2023)
32	aiamkay	pixabay	Collage (10.1.2023)
39	Hans	pixabay	Collage (11.1.2023)
39	dimitrisvetsikas1969	pixabay	Collage (11.1.2023)

Danksagung:
Wir möchten uns bei allen Expert:innen bedanken, die durch ihre wertvollen Einschätzungen und zielführenden Diskussionen mit ihrem Fachwissen zu dieser Publikation beigetragen haben. Namentlich bedanken möchten wir uns bei Sebastian Bock, Dr. Kevin Füchsel, Dr. Christoph Grzeschik, Prof. Dr. Gerhard Hellstern, Prof. Dr. Jörg Hettel, Simon Sebastian Hunt, Prof. Dr. Bettina Just, Christian Koch, Dr. Annka Liepold, Prof. Dr. Marian Margraf, Dr. Daniel Scherer, Dr. Michael Stemmer, Dr. Nikolay Tcholtchev, Prof. Dr. Matthias Troyer, Johannes Verst, Friedrich Wagner sowie Benedict Wenzel.

Icons für Infografik: https://fontawesome.com/

1. Quanten-IKT – ein neues Paradigma

Die Idee einer Informations- und Kommunikationstechnologie, deren Funktionsweise und Eigenschaften stark auf Prinzipien der Quantenphysik basieren, hat ihre Wurzeln in den 1980er Jahren. Nachdem Überlegungen hierzu lange überwiegend theoretischer Natur waren, hat die technische Entwicklung in den letzten Jahren Fahrt aufgenommen. Die Rechenleistung von Quantencomputern wächst in kurzen Abständen und die mit Quantenkommunikation überbrückten Distanzen nehmen zu. Technologie-Giganten haben sich ehrgeizige Ziele für die weitere Entwicklung gesteckt, weltweit werden finanzielle Ressourcen zur Verfügung gestellt und Initiativen gegründet.

Beim Quantencomputing und bei der Quantenkommunikation werden quantenphysikalische Effekte gezielt für die Informationsverarbeitung genutzt. Aufgrund dieser Effekte funktioniert Quanten-IKT anders als klassische IKT und ist deshalb auch nicht als nächste Entwicklungsstufe derselben anzusehen. Sie steht zudem nicht zwangsläufig in Konkurrenz zu klassischer IKT und soll und wird diese nicht generell ablösen. Während klassische IKT in vielen Anwendungsbereichen stark ist, verspricht Quanten-IKT in anderen Bereichen erhebliche Leistungssprünge. Zum Beispiel lassen sich Quantensysteme nur schlecht mit klassischen Rechnern simulieren. Bei Quantenrechnern könnte dies anders sein, was zum Beispiel Verbesserungen bei chemischen Verfahren zur Folge haben könnte. Die breite Praxistauglichkeit von Quanten-IKT steht aktuell noch aus. Hierfür sind Fortschritte in verschiedenen Bereichen wie etwa Architektur und Software erforderlich. Trotzdem ist die Auseinandersetzung mit Quanten-IKT schon heute relevant, da Durchbrüche schnell erhebliche Auswirkungen haben können, zum Beispiel auf die Sicherheit etablierter kryptografischer Verfahren.

Anfang 2022 hat ÖFIT Funktionsweise, Stärken, Schwächen und Herausforderungen von Quanten-IKT in einem White Paper beleuchtet. Nun folgt mit dem Trendsonar eine Bewertung der wichtigsten Trends aus dem Technologiefeld hinsichtlich verschiedener Dimensionen. Quanten-IKT befindet sich in einer früheren Entwicklungsphase als Technologiefelder wie etwa das Internet der Dinge oder Künstliche Intelligenz, die Gegenstand bisheriger Trendsonare waren, deshalb ist die Ungewissheit hier größer. Dies bedeutet zum Beispiel, dass sich auch Expert:innen mit der Bewertung von Technologien schwertun und dass für Auswertungen relevante Daten nicht immer im ausreichenden Maße verfügbar sind. Während es dies im Hinterkopf zu behalten gilt, kann eine systematische Vorgehensweise, wie sie dem ÖFIT-Trendsonar zugrunde liegt, trotzdem als entscheidungsunterstützende Orientierungshilfe zu Stand und möglicher zukünftiger Entwicklung von Trends dienen und Ausgangspunkt eines Monitorings sein.

Das ÖFIT-Trendsonar Quanten-IKT bietet eine Übersicht über fünf wesentliche Bereiche des Technologiefeldes, von möglichen Anwendungen über Ansätze für die grundlegenden Informationseinheiten hin zu Systemkomponenten, Architekturen und Software. Dabei wurden über 30 Technologien hinsichtlich gegenwärtiger Technologiereife, Entwicklung und Zukunftsaussichten analysiert. Während einige der Technologien in Konkurrenz miteinander stehen, bauen viele Technologien innerhalb der fünf Bereiche und über diese hinweg aufeinander auf, sodass sich praktischer Nutzen erst durch das Zusammenspiel mehrerer Technologien ergeben kann. Das ÖFIT-Trendsonar Quanten-IKT richtet sich an Entscheidungsträger:innen aus Politik, Wirtschaft und Verwaltung, sowie an alle technisch Interessierten.

Inhalt

2. Das Trendsonar im Überblick

Für dieses ÖFIT-Trendsonar haben wir in einem mehrstufigen Prozess (siehe Anhang A) Technologien aus dem Forschungsfeld Quantencomputing und Quantenkommunikation identifiziert. Die 33 wichtigsten Technologien wurden für die Publikation ausgewählt und werden nachfolgend vorgestellt. Das Trendsonar bietet Ihnen eine Übersicht und Analyse wichtiger derzeitiger und zukünftiger Technologien in den Bereichen:

- Anwendungen
- Qubits
- Systemkomponenten
- Architektur
- Software

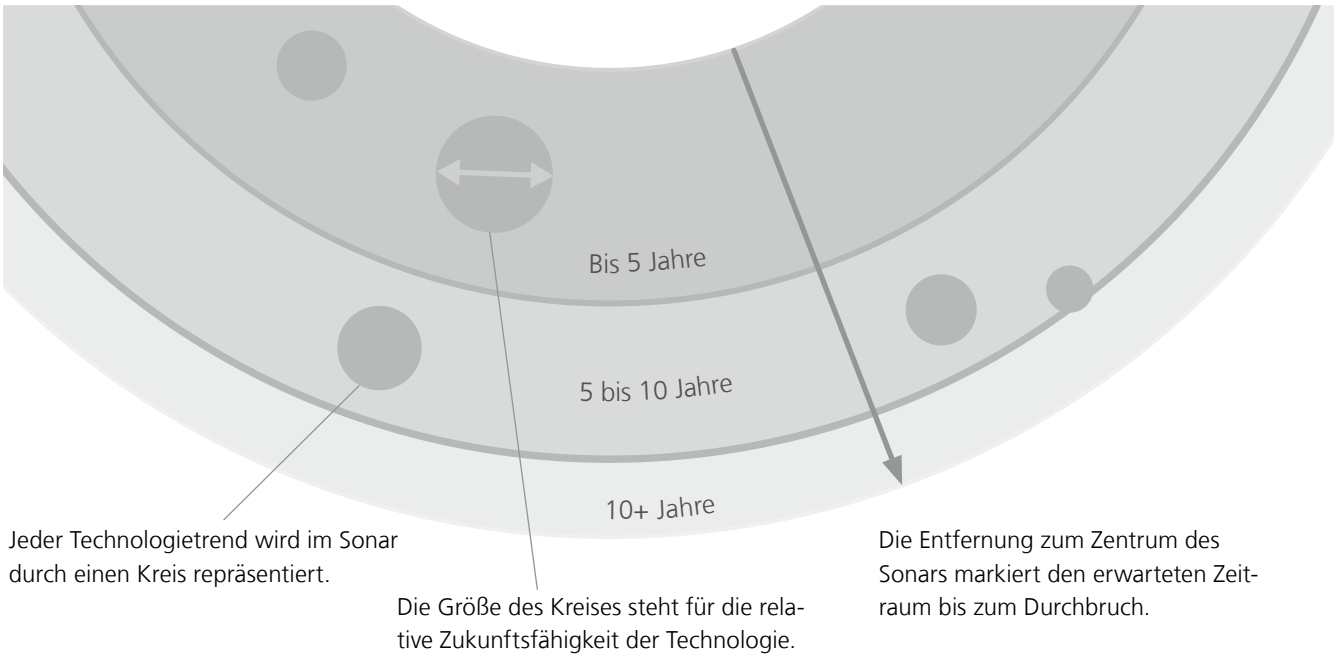
Die vorgestellten Technologien lassen sich in ihrem tatsächlichen Einsatz nicht immer klar genau einem der fünf Bereiche zuordnen, letztere helfen jedoch bei der Orientierung im hochdynamischen Feld der Quanten-IKT. Jede Technologie wurde bei der Analyse anhand mehrerer Charakteristika bewertet.

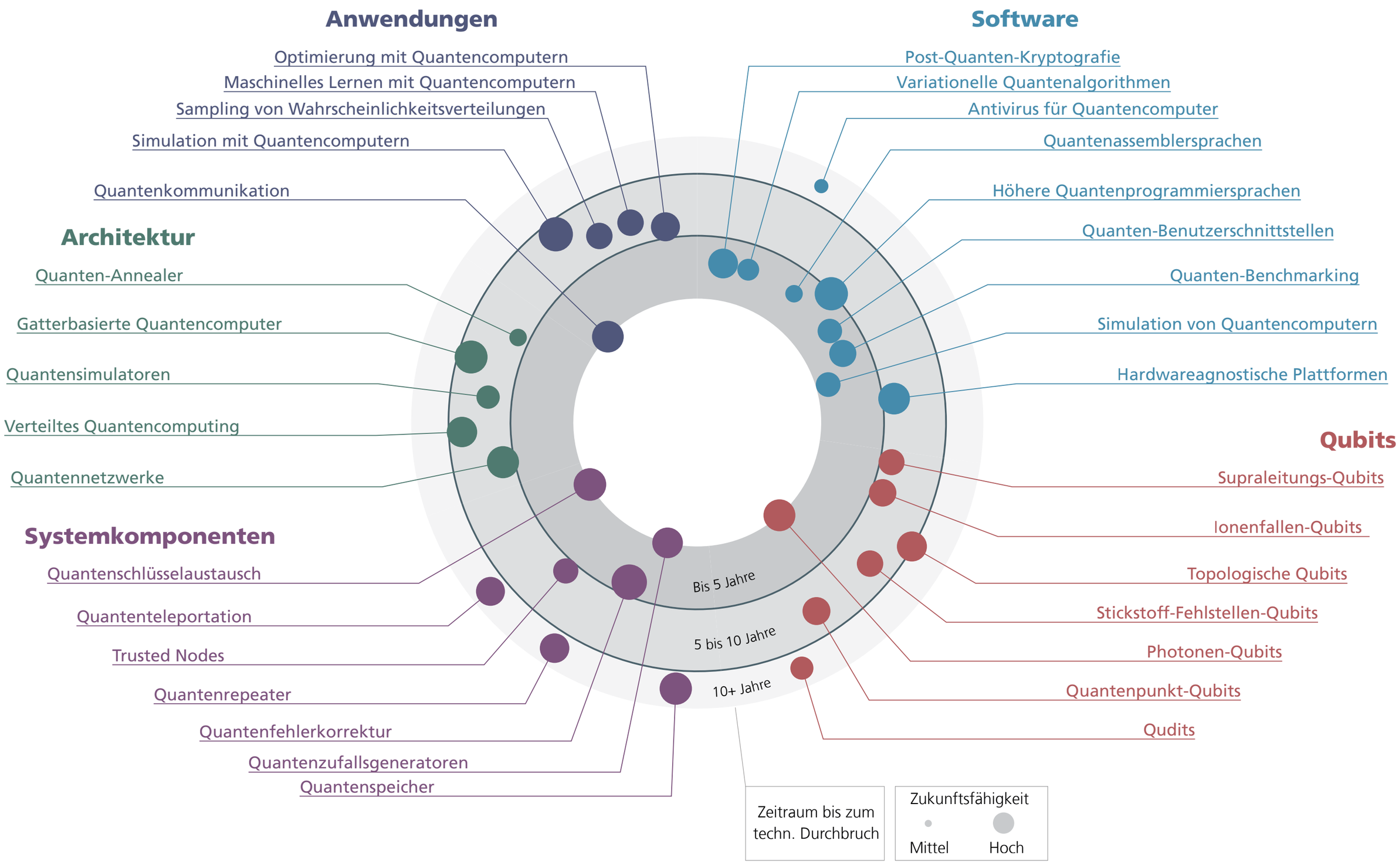
Die zentralen Bewertungskriterien sind die Zukunftsfähigkeit und der Zeitraum bis zum erwarteten Durchbruch der Technologie (siehe Abbildung 1):

Die **Zukunftsfähigkeit** gibt an, wie hoch das Potenzial der Technologie ist. Je größer der Wert ist, desto mehr versprechen sich Expert:innen von dieser Technologie. Die Dimension Zukunftsfähigkeit wird im Abschnitt »Das Trendsonar im Detail« ausführlicher beschrieben.

Der **Zeitraum bis zum technologischen Durchbruch** ist eine Einschätzung, wie lange es noch dauern wird, bis die Technologie selbst oder als Teil eines größeren Systems nachweislich zuverlässig, robust, klassischen Alternativen zumindest ebenbürtig, nützlich und nutzbar ist. Dabei handelt es sich um eine vorsichtig optimistische Einschätzung, das heißt, sie entspricht Werten aus dem unteren Bereich des realistischen Zeitrahmens bis zum Durchbruch.

Abbildung 1: Schematische Darstellung des Sonars

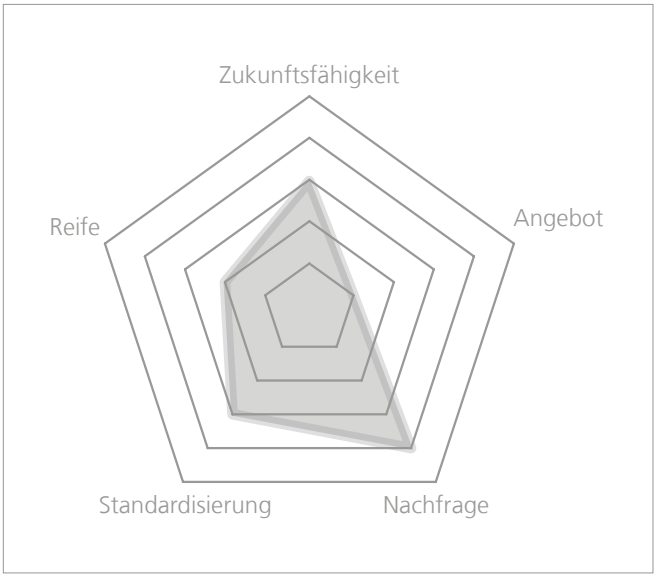



Anwendungen
Optimierung mit Quantencomputern
Maschinelles Lernen mit Quantencomputern
Sampling von Wahrscheinlichkeitsverteilungen
Simulation mit Quantencomputern
Quantenkommunikation
Software
Post-Quanten-Kryptografie
Variationelle Quantenalgorithmen
Antivirus für Quantencomputer
Quantenassemblersprachen
Höhere Quantenprogrammiersprachen
Quanten-Benutzerschnittstellen
Quanten-Benchmarking
Simulation von Quantencomputern
Hardwareagnostische Plattformen
Architektur
Quanten-Annealer
Gatterbasierte Quantencomputer
Quantensimulatoren
Verteiltes Quantencomputing
Quantennetzwerke
Qubits
Supraleitungs-Qubits
Ionenfallen-Qubits
Topologische Qubits
Stickstoff-Fehlstellen-Qubits
Photonen-Qubits
Quantenpunkt-Qubits
Qudits
Systemkomponenten
Quantenschlüsselaustausch
Quantenteleportation
Trusted Nodes
Quantenrepeater
Quantenfehlerkorrektur
Quantenzufallsgeneratoren
Quantenspeicher
Bis 5 Jahre
5 bis 10 Jahre
10+ Jahre
Zeitraum bis zum techn. Durchbruch
Zukunftsfähigkeit
Mittel
Hoch

3. Das Trendsonar im Detail

Der Überblick wird durch weiterführende Bewertungen der einzelnen Technologien ergänzt. Um den Einsatz von Quanten-Technologien in der Praxis einzuschätzen, müssen zu den zukunftsbezogenen Aspekten auch weitere Bewertungsdimensionen aufgenommen werden. Dazu wurden die Verfügbarkeit entsprechender Produkte (Angebotsseite), das Interesse an diesen Produkten (Nachfrageseite), der Entwicklungsstand (Reifegrad) und der Standardisierungsgrad der Technologie erhoben. Dadurch werden Einsichten zur aktuellen Marktstruktur und zur Nutzbarkeit von Technologien in bestehenden Systemen ermöglicht. Diese zukunfts- und praxisrelevanzbezogene Einschätzung der Technologietrends wurde von Expert:innen aus dem Bereich der Quantentechnologieforschung vorgenommen. Die fünf Bewertungsdimensionen sind jeweils in Form eines Netzdiagramms visualisiert (siehe Abbildung 2).

Abbildung 2: Schematische Darstellung der Expert:innenbewertung



Der Expert:innenanalyse sind quantitative Kenngrößen zur Seite gestellt. Hierzu wurden Daten aus Forschungsförderprogrammen auf Bundes- und EU-Ebene, aus einer Datensammlung zu Start-ups, aus Patent- und wissenschaftlichen Literaturdatenbanken, aus Suchmaschinenanfragen und aus Medienanalyse-Tools herangezogen.

Anzahl nationaler und europäischer **Forschungsförderungsprogramme**	●●● hoch (> 999) ●●● mittel (100 – 999) ●●● gering (0 – 99)
Entwicklung wissenschaftlicher **Publikationen** 2013 – 2017 verglichen mit 2018 – 2022	↗–↘ Anstieg ↗–↘ Abnahme ↗–↘ gleichbleibend ✓✕ Daten unzureichend
Anzahl innovationsorientierter **Gründungen** seit 2011	●●● hoch (> 19) ●●● mittel (10 – 19) ●●● gering (0 – 9)
Entwicklung von **Suchanfragen** zwischen 2013 – 2017 verglichen mit 2018 – 2022	↗–↘ Anstieg ↗–↘ Abnahme ↗–↘ gleichbleibend ✓✕ Daten nicht vorhanden
Anzahl der **Patentfamilien** mit mindestens einem erteilten Patent	●●● hoch (> 99) ●●● mittel (10 – 99) ●●● gering (0 – 9)
Anzahl der Erwähnungen in journalistischen **Medien** zwischen 2017 und 2022	●●● hoch (> 999) ●●● mittel (100 – 999) ●●● gering (0 – 99)

Die Expert:inneneinschätzungen und die quantitativen Indikatoren beleuchten die Eigenschaften der ausgewählten Technologien aus zwei verschiedenen Perspektiven. Dabei ist beispielsweise die quantitative Erhebung von Gründungen ein Indikator für das Angebot einer Technologie am Markt und eine hohe Zukunftsfähigkeit wird durch die Anzahl an Forschungsförderungsprogrammen gespiegelt. Durch die gemeinsame Betrachtung von Expert:innenbewertungen und quantitativen Indikatoren lassen sich Strategien für die Anwendung der thematisierten Technologien entwerfen.

Zukunftsfähigkeit

Der Wert der Kenngröße Zukunftsfähigkeit reflektiert das Potenzial einer Technologie. Ein hoher Wert bedeutet, dass die Chance besteht, dass die Technologie zukünftig weit verbreitet sein wird, dass sie eine wesentliche Rolle innerhalb des Quanten-IKT-Ökosystems spielt oder für disruptive Veränderungen sorgt. Ist der Wert niedrig, lässt sich dies so interpretieren, dass die maximal erreichbare Bedeutung der Technologie als eher niedrig angesehen wird. Anzumerken ist, dass die Zukunftsfähigkeit nicht angibt, ob das Potenzial einer Technologie zukünftig tatsächlich ausgeschöpft wird. So werden derzeit zum Beispiel viele verschiedene Qubit-Typen entwickelt. Es ist gut denkbar, dass sich im Laufe der Zeit einige wenige Typen zulasten von Alternativen als De-facto-Standard etablieren werden.

Reife

Der Wert der Kenngröße Reife beschreibt den geschätzten Entwicklungsgrad einer Technologie. Je höher die Einschätzung, desto ausgereifter ist die Technologie nach Meinung der Expert:innen. Ein hoher Reifegrad ist ein Indikator dafür, dass der technologische Durchbruch bald erfolgen könnte, wobei andere Faktoren wie etwa Forschungsförderung, Nachfrage und erwartete Marktgröße auch Einfluss auf diese Zeitspanne haben können.

Angebot

Der Wert der Kenngröße Angebot bildet die Verfügbarkeit von Produkten ab, die auf der Technologie basieren. Je höher der Wert, desto vielfältiger ist die Angebotslage.

Nachfrage

Der Wert der Kenngröße Nachfrage bildet das aktuelle Interesse an einer Technologie seitens potenzieller Kund:innen ab. Je größer der Wert, desto höher die Nachfrage.

Standardisierung

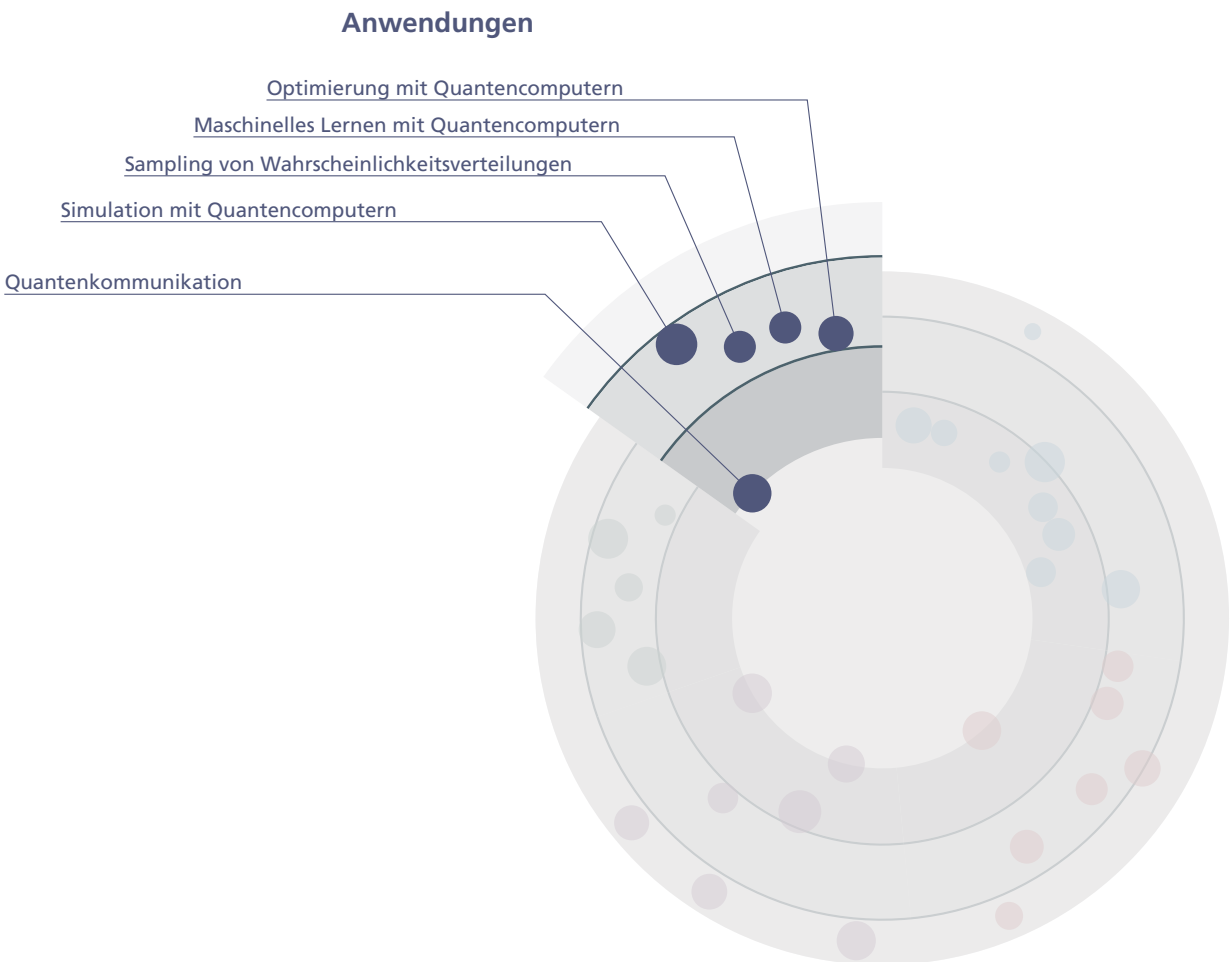
Der Wert der Kenngröße Standardisierung spiegelt die Einschätzung zum Standardisierungsgrad einer Technologie wider. Je höher der Wert, desto ausgereifter und etablierter sind verfügbare Standards. Standardisierung trägt zu höherer Qualität und zu verbesserter Interoperabilität bei.

Im Netzdiagramm wird für jede der fünf Dimensionen der arithmetische Mittelwert der Bewertungen durch die Expert:innen dargestellt. Bei einem noch jungen Technologiefeld wie der Quanten-IKT bestehen viele Unsicherheiten und entsprechend können sich auch Expert:innen uneins sein. In Anhang B befindet sich eine Tabelle für die Technologien des Trendsonars, in der zusätzlich zum Mittelwert für die fünf Dimensionen auch die jeweilige Standardabweichung bei den Expert:inneneinschätzungen hinterlegt ist. Je größer die Standardabweichung im Vergleich zum Mittelwert ausfällt, desto heterogener das Meinungsbild.

Die Zukunftsfähigkeit der betrachteten Technologien wird von den befragten Expert:innen im Allgemeinen als hoch eingeschätzt. Tatsächlich sind sich die Expert:innen in diesem Punkt auch am ehesten einig. Die Abweichungen in den Einschätzungen sind bei der Zukunftsfähigkeit zumeist geringer als bei den anderen Dimensionen. Generell wird der Status quo bei Reife, Angebot und Nachfrage als mittelmäßig bis etwas darunter eingeschätzt. Dabei wird die Nachfrage durchschnittlich zumeist höher bewertet als das Angebot, was ein Indiz für das Wachstumspotenzial des Marktes sein könnte. Der Standardisierungsgrad der Technologien wird im Mittel als gering bewertet. Dies deckt sich auch mit den Rechercheergebnissen: Im Gegensatz zu früheren Ausgaben des Trendsonars zu anderen Technologiefeldern wurde der quantitative Indikator zu Normen und Normentwürfen diesmal nicht berücksichtigt, da die Datengrundlage nicht ausreichend war.

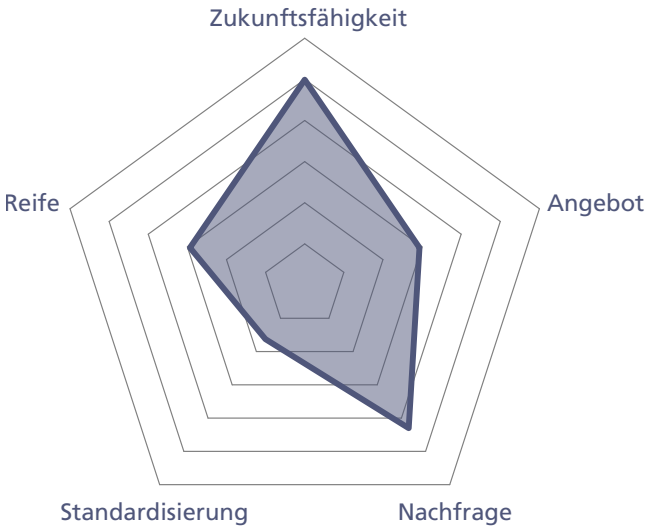
3.1 Anwendungen

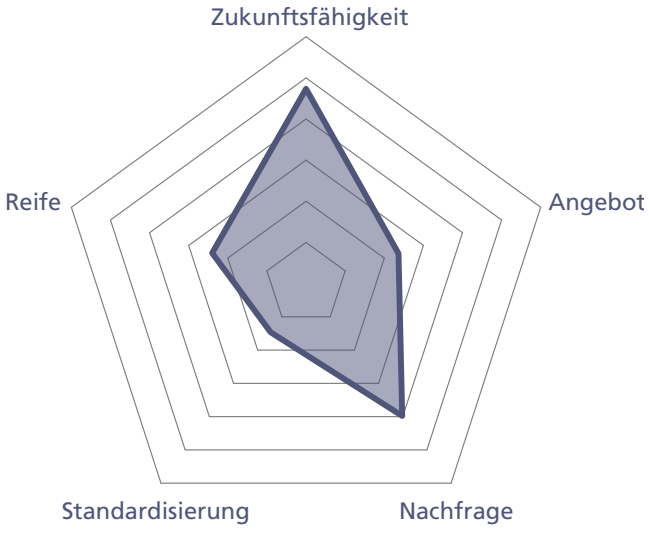
Dieser Abschnitt beschreibt Anwendungen, welche sich aus Kombinationen verschiedener Technologien aus den Abschnitten Qubits, Systemkomponenten, Architektur und Software ergeben. Bei diesen Anwendungen könnte Quanten-IKT Vorteile gegenüber klassischer IKT besitzen und so zum Beispiel die wirtschaftliche Verwertung ermöglichen.



Optimierung mit Quantencomputern

Quantencomputer können zur Lösung mathematischer Optimierungsprobleme eingesetzt werden. Dabei stehen insbesondere Probleme aus der kombinatorischen Optimierung im Fokus. Derartige Probleme sind zum Beispiel im Bereich der Logistik von großer Bedeutung. Zur Lösung kombinatorischer Optimierungsprobleme existieren bereits verschiedene Algorithmen für Quantenrechner.



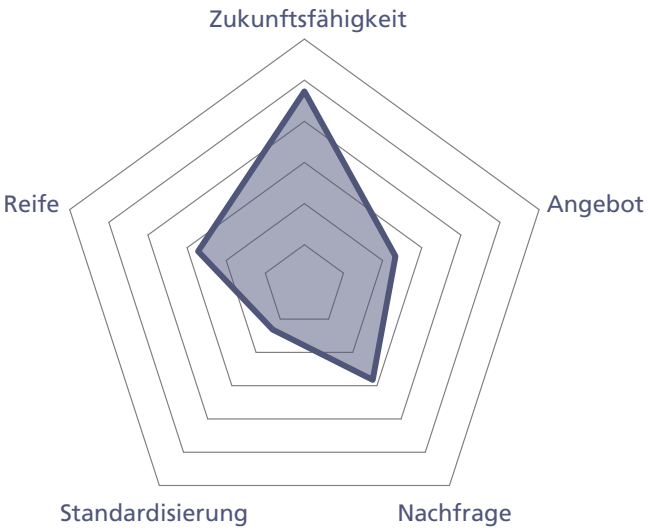


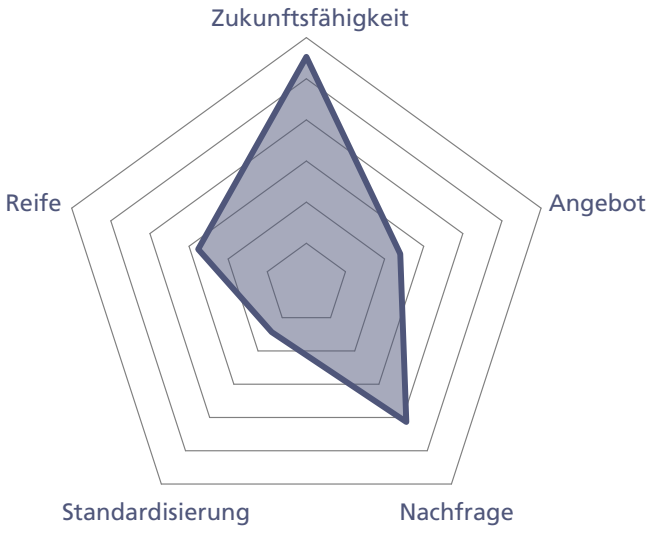
Maschinelles Lernen mit Quantencomputern

Quantencomputer können im Bereich des Maschinellen Lernens eingesetzt werden. Hierbei kommen oft hybride Algorithmen zum Einsatz, die Teilprozesse an klassische Computer und Quantencomputer verteilen, je nachdem, welcher Computertyp geeigneter für eine Teilaufgabe ist. Insgesamt sollen viele Techniken des Maschinellen Lernens dadurch leistungsfähiger werden.

Sampling von Wahrscheinlichkeitsverteilungen

Die Stichprobenziehung von Wahrscheinlichkeitsverteilungen ist unter anderem relevant für Simulationen, Maschinelles Lernen und statistische Physik. Je nach Wahrscheinlichkeitsverteilung kann dies jedoch mit klassischen Rechnern sehr schwierig sein. Zumindest für einige Wahrscheinlichkeitsverteilungen, etwa die Boltzmann-Verteilung, scheinen Quantencomputer in bisherigen Tests deutlich effizienter zu sein.



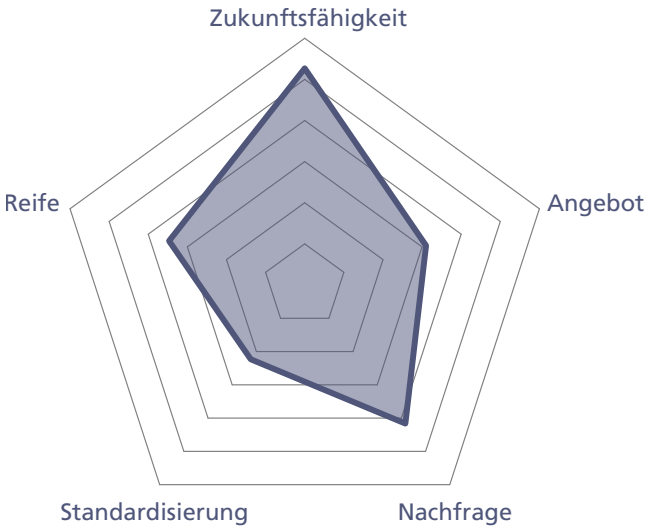


Simulation mit Quantencomputern

Klassische Computer kommen bei der Simulation von Quantensystemen recht schnell an ihre Grenzen. Bei Quantencomputern ist dies anders, da es sich hierbei auch um Quantensysteme handelt. Simulationen von Quantensystemen sind zum Beispiel für Herstellungsverfahren chemischer Stoffe und die Entwicklung von Medikamenten relevant. Außerdem existieren Quantenalgorithmen, die Simulationen von Systemen der klassischen Physik (zum Beispiel Wärmeleitung und Strömungen) ermöglichen.

Quantenkommunikation

Quanten-IKT bietet die Chance, Kommunikationstechnik auf ein bisher unerreichtes Sicherheitslevel zu heben. Dafür können zum Beispiel Protokolle zum Quantenschlüsselaustausch und Protokolle zur Quantenteleportation eingesetzt werden. Nach einem Quantenschlüsselaustausch werden Nutzdaten dann verschlüsselt auf klassischen Kanälen übertragen. Theoretisch besteht aber auch die Möglichkeit, bei der Übertragung von Nutzdaten Quanteneffekte zu nutzen. Bei der Quantenteleportation geht es um die Übertragung von Quanteninformation, also die Übertragung des Zustands eines Quantensystems.




Forschungsförderung


Publikationen


Gründungen

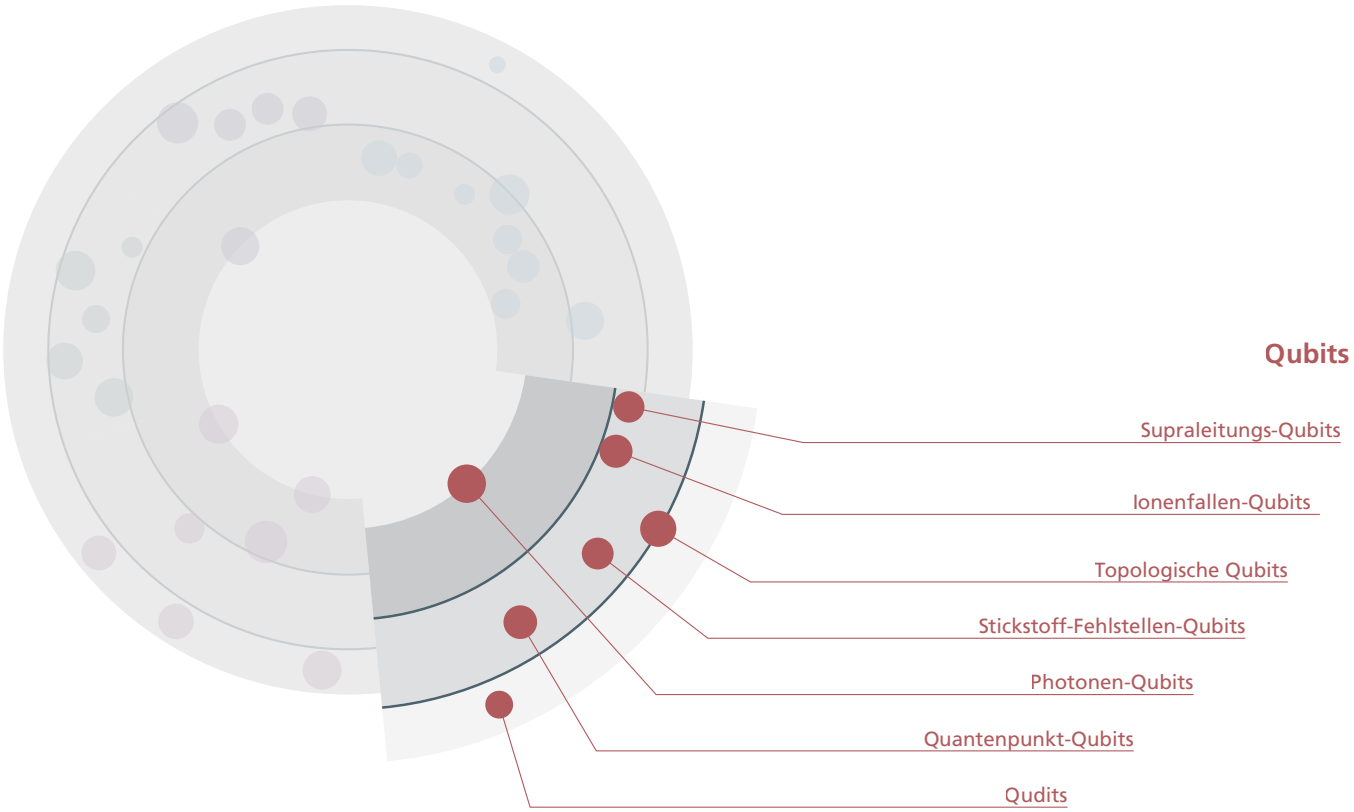

Suchanfragen


Patente


News

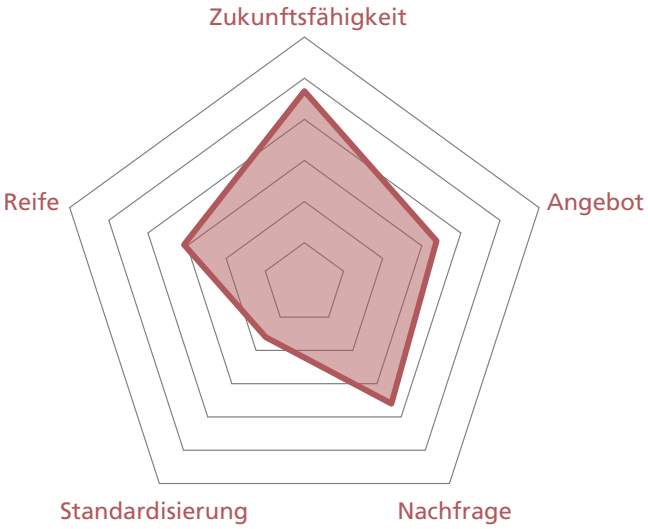
3.2 Qubits

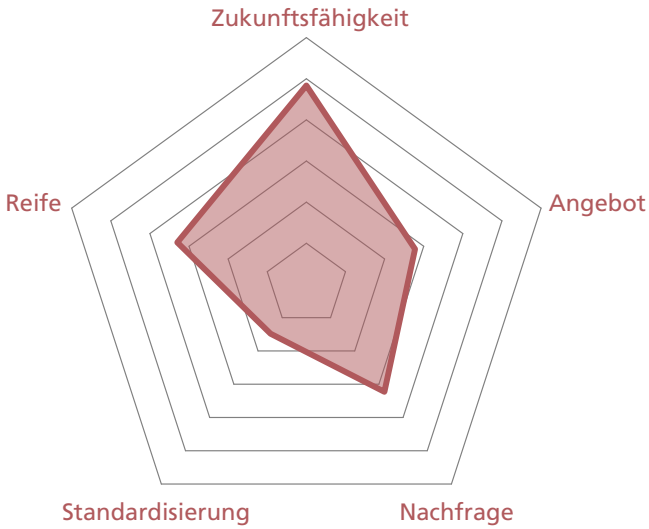
Analog zum klassischen Bit existiert auch in der Quanten-IKT eine kleinste Informationseinheit: Das Quantenbit, kurz Qubit, oder in verallgemeinerter Form das Qudit. Ein Qubit kann neben den Basiszuständen 0 und 1 auch Überlagerungen dieser Zustände annehmen, was ein grundsätzlicher Unterschied zum klassischen Bit ist. Qubits können versendet werden und so zum Informationsaustausch genutzt werden. Ebenso können mehrere Qubits zu einem Register zusammengefasst werden und so als Speicher eines Quantenprozessors dienen. Es existieren verschiedene Möglichkeiten, um Qubits physikalisch umzusetzen. Verschiedene Ansätze können dabei ganz unterschiedliche Vor- und Nachteile haben, etwa bezüglich der Fehleranfälligkeit oder der Skalierbarkeit, wobei bisher kein Ansatz den anderen durchweg überlegen ist. In diesem Abschnitt werden die wesentlichen Ansätze vorgestellt.



Supraleitungs-Qubits

Elektronische Schaltkreise weisen bei Temperaturen nahe am absoluten Nullpunkt quantentypische Eigenschaften auf und bilden so die physikalische Basis für diesen Qubittyp. Es gibt verschiedene Varianten von supraleitenden Qubits (Charge Qubit, Flux Qubit, Phase Qubit). Dass es bereits bewährte Prozesse für die Massenproduktion von elektronischen Schaltkreisen gibt, könnte einen Vorteil hinsichtlich der Skalierbarkeit bedeuten.



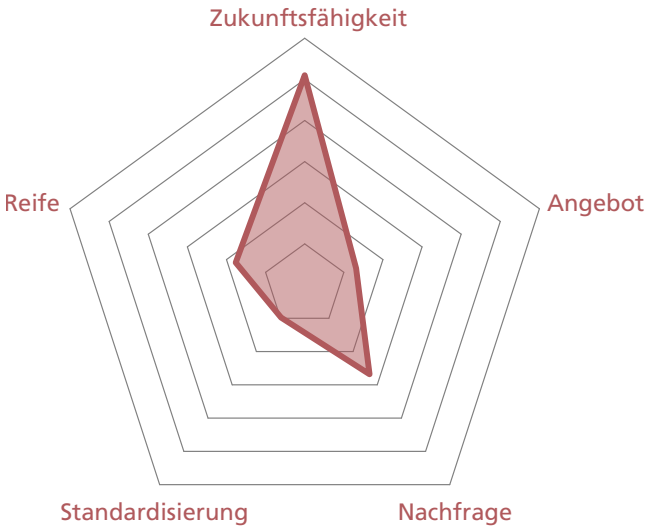


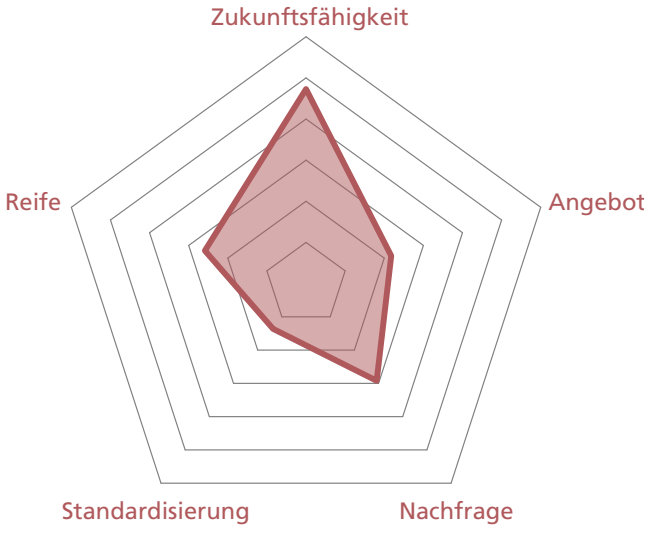
Ionenfallen-Qubits

Es handelt sich hierbei um einen Qubittyp, der auf Ionenfallen basiert. Ionen sind Atome, bei denen die Anzahl der Elektronen nicht mit der Anzahl der Protonen übereinstimmt. Deshalb sind Ionen elektrisch geladen. In Ionenfallen werden solche Ionen innerhalb einer Vakuumkammer mittels elektromagnetischer Felder positioniert. Ein Vorteil bei Ionenfallen-Qubits ist, dass die Fehlerrate bei der Anwendung von Gattern auf diese Qubits sehr gering ist.

Topologische Qubits

Hierbei handelt es sich um einen auf Anionen und Hybridmaterialien basierenden Ansatz zur Konstruktion von Qubits. Eine Stärke topologischer Qubits ist, dass sie robuster gegenüber Störungen durch Umwelteinflüsse sind als andere Qubittypen.



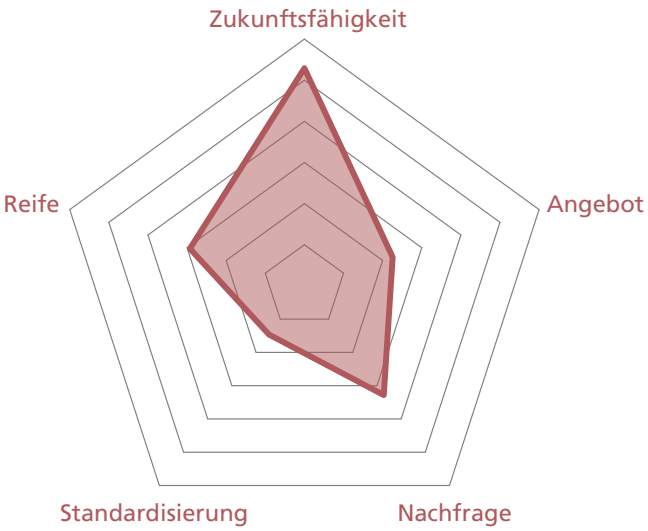


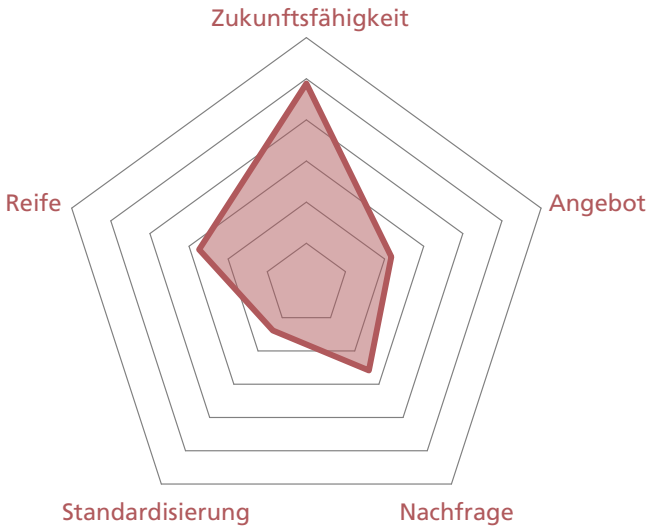
Stickstoff-Fehlstellen-Qubits

Diamanten sind im Wesentlichen Gitter aus Kohlenstoffatomen. Diese lassen sich gezielt verunreinigen, sodass zwei benachbarte Kohlenstoffatome im Gitter durch ein Stickstoffatom und eine Fehlstelle (also eine Lücke in der Gitterstruktur) ersetzt werden. Dies wird als Stickstoff-Fehlstellen-Zentrum (englisch nitrogen-vacancy-center) bezeichnet und lässt sich als physikalische Grundlage zur Konstruktion von Qubits nutzen. Neben Quantencomputing lässt sich dieser Qubittyp auch für sehr feine Messtechnik (Quantensensorik) nutzen.

Photonen-Qubits

Photonen-Qubits basieren auf den quantenphysikalischen Eigenschaften von Photonen. Besonders geeignet ist dieser Qubittyp für Quantenkommunikation, da sich Photonen mit Lichtgeschwindigkeit fortbewegen und existierende Infrastruktur nutzen können, also beispielsweise per Glasfaser übertragbar sind.



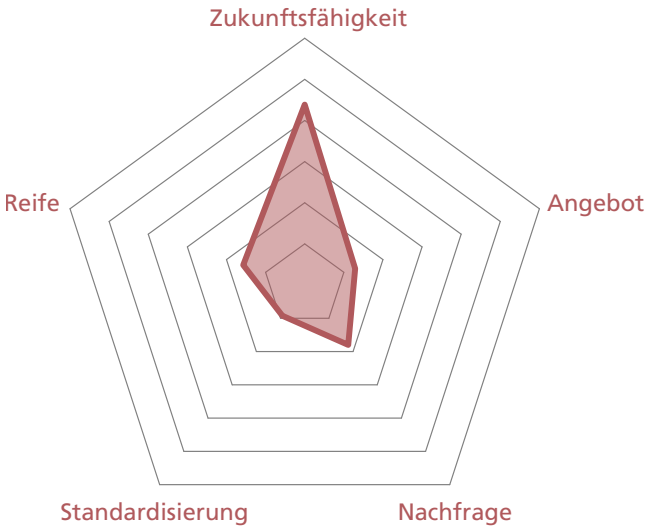


Quantenpunkt-Qubits

Quantenpunkte sind (künstliche) Partikel in Nanometergröße, bei denen Ladungsträger (Elektronen) so stark in ihren Bewegungsmöglichkeiten eingeschränkt sind, dass ihre Energie nur noch diskrete Level annimmt. Dies kann als Basis für Qubits genutzt werden. Quantenpunkte sind nicht nur für Quanten-IKT interessant, sondern werden auch als Grundlage für Bildschirme verwendet.

Qudits

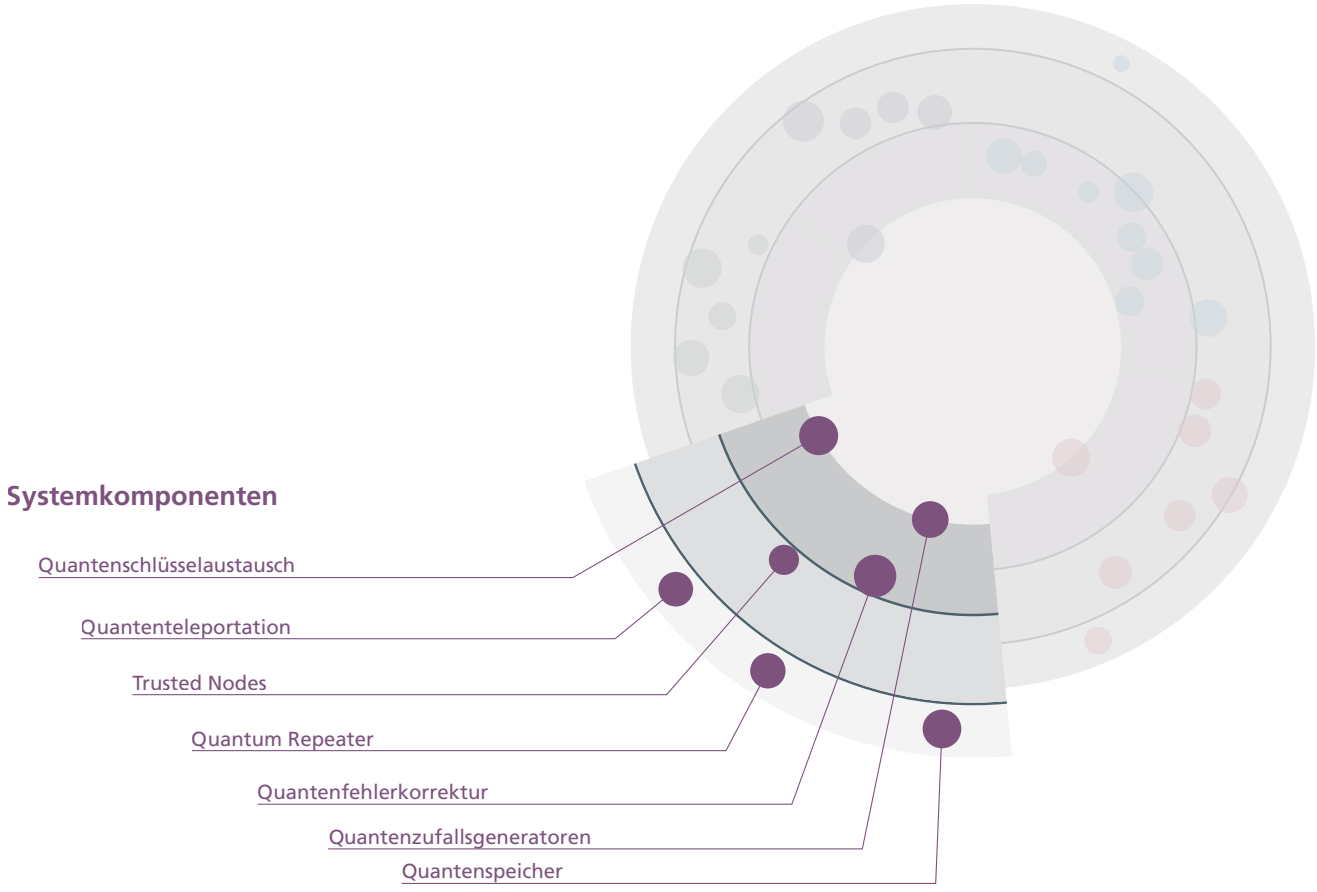
Als kleinste Informationseinheit kommen bei Quantencomputern zumeist Qubits zum Einsatz. Für ein Qubit lassen sich zwei unterschiedliche Zustände messen, die dann 0 bzw. 1 repräsentieren. Es ist das Quanten-Äquivalent zum binären Bit. Tatsächlich lassen sich allerdings auch Quantensysteme konstruieren, für die mehr als zwei Zustände messbar sind. Zum Beispiel das Qutrit mit drei messbaren Zuständen 0, 1 und 2. Als Oberbegriff für solche Quanteninformationseinheiten mit mehr als zwei messbaren Zuständen wird der Begriff Qudit verwendet. Qudits könnten zum Beispiel Computer ermöglichen, deren Funktionsweise im Gegensatz zu klassischen Rechnern nicht auf dem Binärsystem basiert.



Forschungsförderung | Publikationen | Gründungen | Suchanfragen | Patente | News

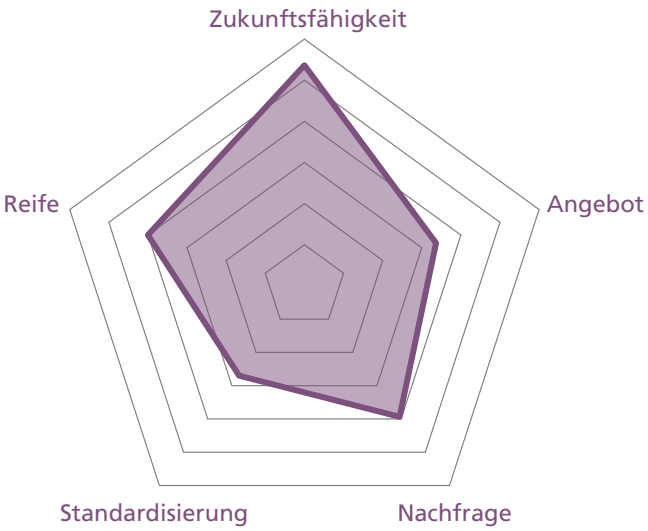
3.3 Systemkomponenten

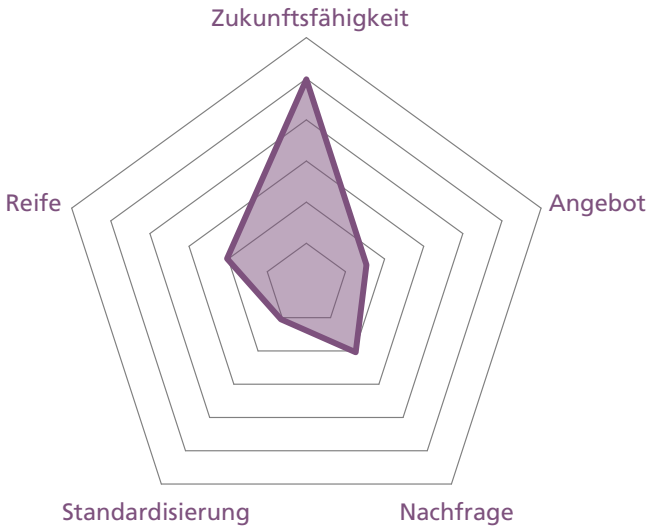
Systeme wie etwa Quantenrechner oder Quantennetzwerke bestehen aus vielen Komponenten, die die Funktionstüchtigkeit des Gesamtsystems erst ermöglichen. In diesem Abschnitt werden wesentliche Komponenten betrachtet, mit Ausnahme von Qubits, die in einem eigenen Abschnitt behandelt werden.



Quantenschlüsselaustausch

Um sicher verschlüsselt zu kommunizieren, ist ein Schlüssel erforderlich, der für alle bis auf die Kommunikationsparteien geheim ist. Die Generierung und der Austausch eines Schlüssels muss daher so gestaltet werden, dass der Schlüssel nicht durch Dritte abgehört werden kann. Quanteneffekte können für Kommunikation so genutzt werden, dass Abhörversuche aufgrund von Naturgesetzen nicht verborgen werden können. Ursache dafür ist, dass mit einem Abhörversuch auch eine Veränderung der übertragenen Information erfolgt und diese Änderungen auch nachvollziehbar ist. Es existieren Protokolle, die dies für den Austausch von Schlüsseln nutzen. Gab es bei einem Schlüsselaustausch keinen Abhörversuch, so können die Schlüssel verwendet werden. Andernfalls wird der Vorgang wiederholt, bis Schlüssel ausgetauscht wurden, die nicht abgehört wurden.



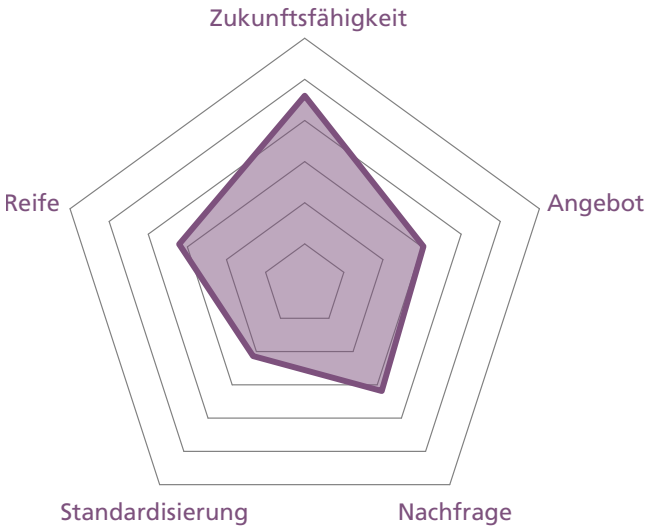


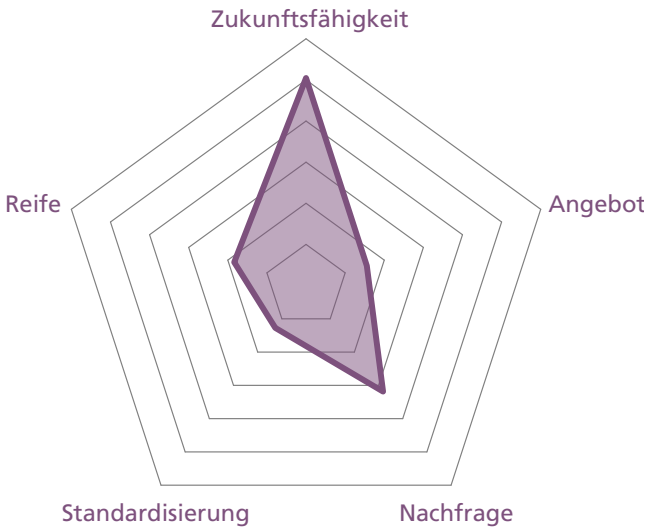
Quantenteleportation

Quantenteleportation beschreibt die Übertragung des Zustands eines Qubits auf ein theoretisch beliebig weit entferntes Qubit. Dabei wird das Phänomen der Verschränkung genutzt, bei dem die zwei Qubits ein gemeinsames Qubitsystem bilden statt zweier getrennter. Um dies zur Übertragung von Information zu nutzen, ist ein ergänzender klassischer Kanal erforderlich. Quantenteleportation lässt sich für die abhörsichere Kommunikation nutzen, aber auch für verteiltes Quantencomputing.

Trusted Nodes

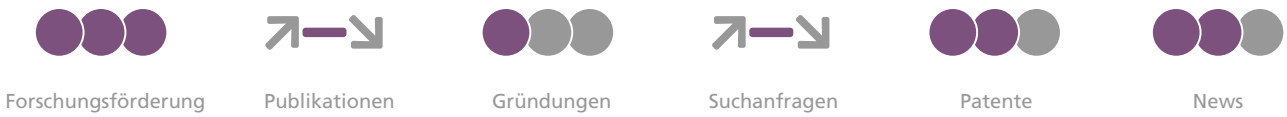
Um über große Distanzen mithilfe von Quanteneffekten abhörsicher zu kommunizieren, braucht es Zwischenstationen, da die Reichweite von Quantenkommunikation aufgrund von Signalverlusten in Abhängigkeit von der Distanz begrenzt ist. Eine Möglichkeit für solche Zwischenstationen sind Trusted Nodes. In diesen Knotenpunkten wird die gesendete Information von ihrer (reichweitenbegrenzten) Quantenform in Bitfolgen übersetzt und dann neu in Quantenform übersetzt, bevor sie weitergesendet wird. Während die Information so zwar auf den Strecken zwischen den Knotenpunkten sicher ist, ist dies in den Knotenpunkten selbst nicht der Fall, da sie hier in Bitform vorliegt. Daher muss der Zugang zu den Knotenpunkten gut geschützt sein, damit diesen Punkten und folglich auch dem Quantennetzwerk tatsächlich vertraut werden kann.





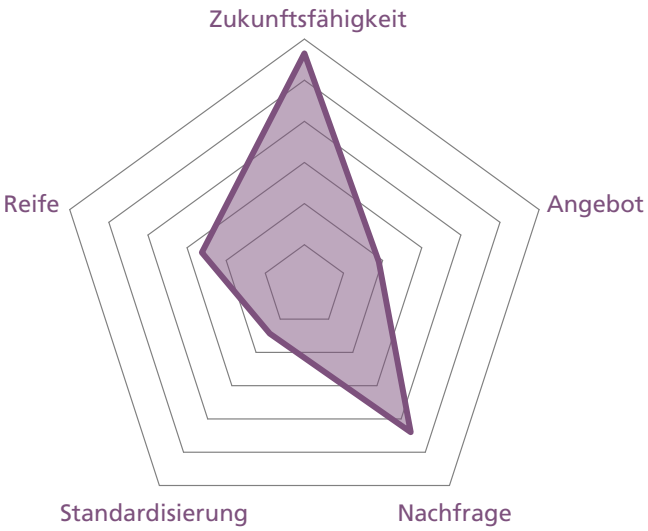
Quantenrepeater

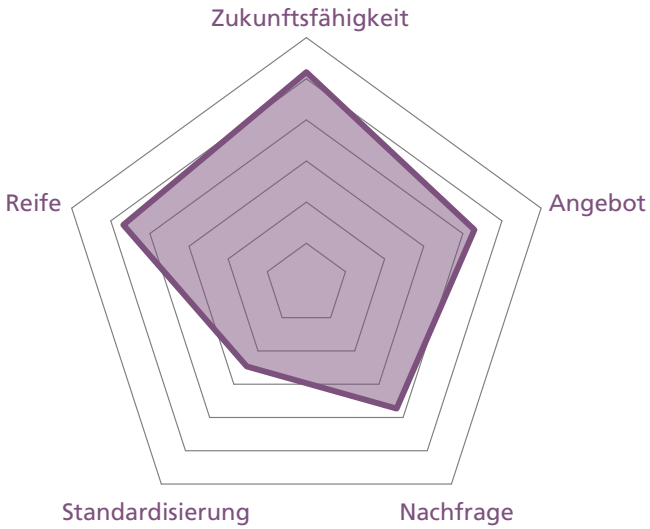
Quantenrepeater sind eine andere Form von Zwischenstationen, um über größere Distanzen mittels Quanteneffekten abhörsicher zu kommunizieren, und stellen somit eine Alternative zu Trusted Nodes dar. Quantenrepeater beinhalten Quantenspeicher und funktionieren mittels Quantenteleportation. Dadurch ist ihre Konstruktion zwar technisch anspruchsvoller als die von Trusted Nodes, die übertragene Information liegt jedoch auch innerhalb der Zwischenstationen nicht als les- und kopierbare Bitform sondern in Form von Quantenzuständen vor.



Quantenfehlerkorrektur

Quanteninformations- und kommunikationstechnologie ist hochgradig fehleranfällig, etwa aufgrund von unbeabsichtigter Wechselwirkung mit der Umgebung. Auch bei klassischer IKT treten Fehler auf, die in der Regel mithilfe von Kopien von Information korrigiert werden. Die Anfertigung von Kopien ist bei der Quanten-IKT aufgrund physikalischer Eigenschaften (»No-Cloning-Theorem«) jedoch nicht möglich. Unter Quantenfehlerkorrektur versteht man Quanten-IKT-spezifische Verfahren, um Fehler zu bemerken und korrigieren zu können. Dabei werden mehrere Qubits zu einem logischen Qubit zusammengefasst und anhand von Messergebnissen bestimmte Fehlertypen erkannt und korrigiert.



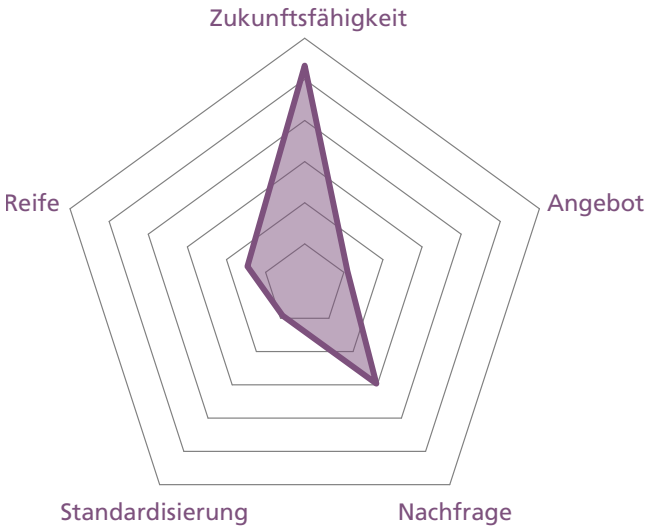


Quantenzufallsgeneratoren

Quantenzufallsgeneratoren nutzen echt zufällige Quanteneffekte, um Zufallszahlen zu generieren. Zufallszahlen sind in vielen Bereichen von Interesse, beispielsweise in der Kryptografie und für Simulationen. Die durch viele andere Generatortypen erzeugten Zahlen sind entweder nur scheinbar zufällig (Pseudozufallszahlen) oder werden durch einen Prozess generiert, dessen Zufälligkeit zumindest nicht widerlegt ist. Weil es in der Quantenphysik inhärent zufällige Prozesse gibt, können durch hierauf basierende Generatoren echte Zufallszahlen erzeugt werden.

Quantenspeicher

Derzeit speichern Qubits Information in der Regel nur sehr kurzfristig, oft zu kurz, um praktische Anwendungen zu ermöglichen. Quantenspeicher sollen längeres Zwischenspeichern ermöglichen. Als Teil von Quantenrepeatern könnten so größere Quantenkommunikationsnetzwerke ermöglicht werden. Zudem könnten auf Quantencomputern Probleme in praxisrelevanter Größe bearbeitbar werden.




Forschungsförderung


Publikationen


Gründungen

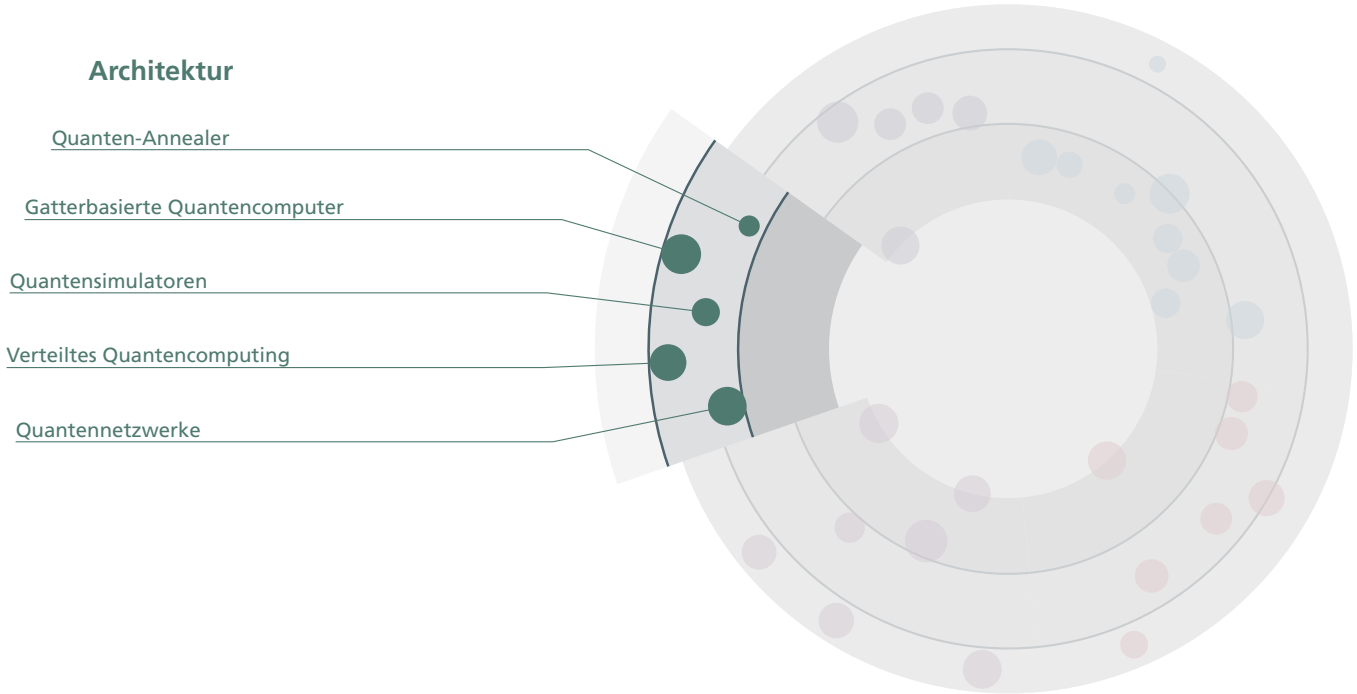

Suchanfragen


Patente


News

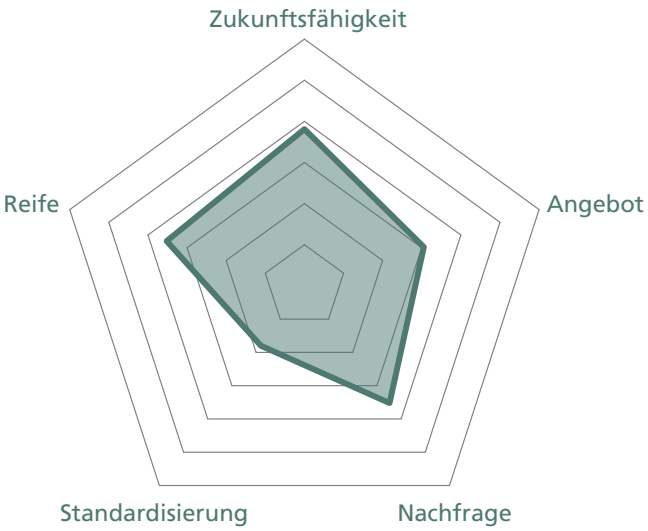
3.4 Architektur

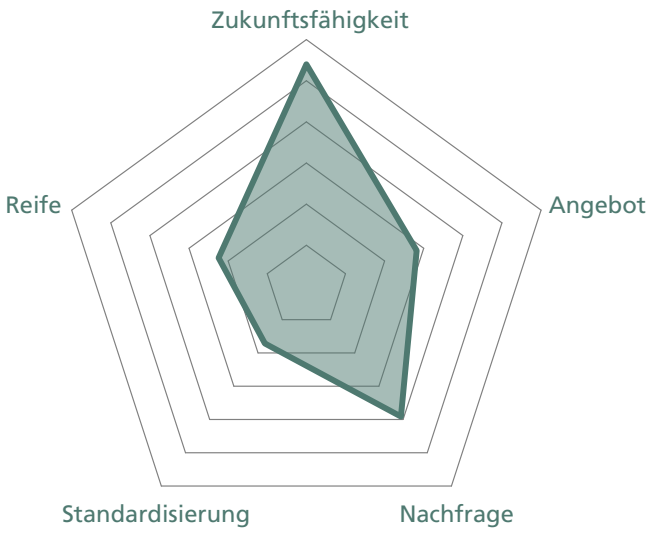
Diskussionen zu Quantentechnologie für die Informationsverarbeitung und -übermittlung fokussieren sich oftmals auf Quantencomputing und insbesondere gatterbasierte Quantenrechner. Tatsächlich existieren aber auch andere Architekturansätze, die einige Aufgaben, etwa Simulationen, möglicherweise früher, besser oder überhaupt erst erfüllen können oder wesentlich für die Skalierung von gatterbasierten Quantenrechnern sein könnten. Dieser Abschnitt stellt einige dieser Ansätze vor.



Quanten-Annealer

Bei Quanten-Annealern handelt es sich um einen Quantencomputertyp, dessen Funktionsweise auf der natürlichen Evolution von Quantensystemen über die Zeit hinweg basiert. Dieser Prozess der Systemevolution wird als Quanten-Annealing bezeichnet. Bei einem Quanten-Annealer erfolgt also kein algorithmisches Abarbeiten kleiner Schritte, stattdessen wird ein System in einen bestimmten Anfangszustand versetzt, um dann dem Annealing-Prozess überlassen zu werden, der das System verändert. Abschließend erfolgt eine Messung des Endzustands des Systems. Populär ist dieser Computertyp vor allem bei der Lösung mathematischer Optimierungsaufgaben. Der Anfangszustand entspricht dabei der Menge aller validen Lösungen des Problems und der Endzustand genau einer Lösung, die optimal ist oder der optimalen Lösung zumindest sehr nahekommt.



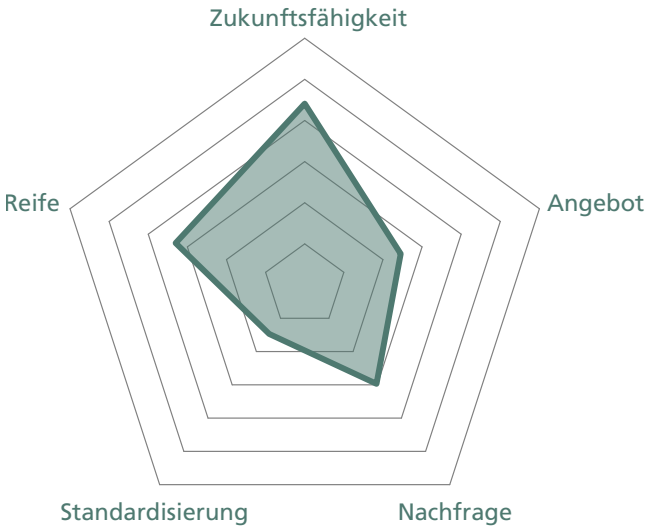


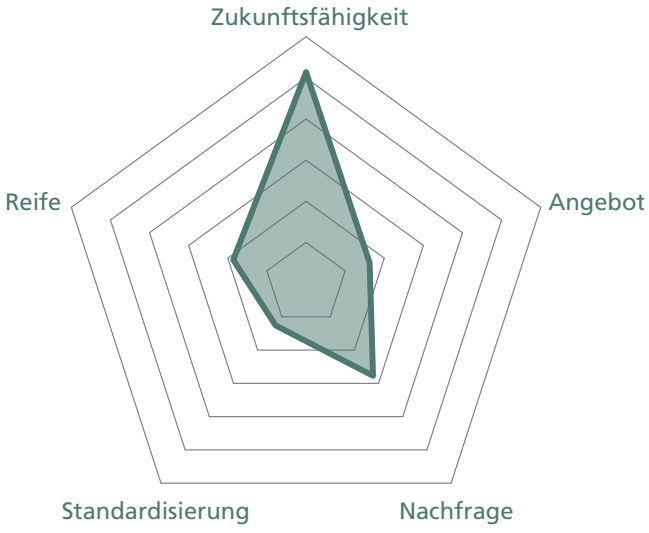
Gatterbasierte Quantencomputer

Die Funktionsweise gatterbasierter Quantencomputer ähnelt der eines klassischen Computers. Sie bestehen aus Registern von Qubits, auf die eine kleine Menge unterschiedlicher Gatter, etwa logischer Operationen, angewendet werden kann. Programme geben dann vor, welche Gatter in welcher Reihenfolge angewendet werden. Gatterbasierte Quantenrechner sind universell einsetzbar und im Vergleich zu anderen Quantencomputertypen einfacher zu programmieren.

Quantensimulatoren

Bei Quantensystemen handelt es sich um physikalische Systeme, die aus Quantenobjekten, etwa Molekülen und Elektronen, bestehen und deren Verhalten sich nur mithilfe der Quantenphysik erklären lässt. Die Beschreibung und die Simulation des Verhaltens solcher Quantensysteme ist zum Beispiel für chemische Prozesse in der Industrie relevant. Viele Quantensysteme lassen sich jedoch nur unzureichend durch klassische Rechner simulieren, da die Berücksichtigung von Quanteneffekten zu viel Rechenleistung erfordert. Quantensimulatoren sind spezielle Maschinen, mit denen sich diese Systeme leichter modellieren und simulieren lassen, da sie Quanteneffekte schon von Haus aus beinhalten. Aufgrund der starken Spezialisierung sind sie aber nicht so vielseitig einsetzbar wie etwa gatterbasierte Quantenrechner.



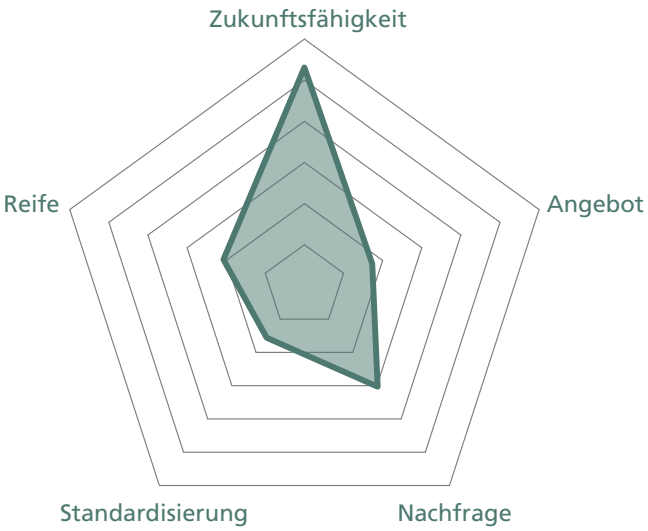


Verteiltes Quantencomputing

Leistungsfähige Quantencomputer brauchen viele Qubits. Allerdings ist es schwierig, einzelne Quantenprozessoren mit ausreichend vielen Qubits zu bauen. Beim verteilten Quantencomputing wird das Phänomen der Quantenteleportation genutzt, um viele kleine Quantenprozessoren zu verknüpfen, sodass sie sich, obwohl physisch getrennt, wie ein einziges System verhalten, das dann zur Lösung von Problemen eingesetzt werden kann.

Quantennetzwerke

Quantennetzwerke (auch: Quanteninternet) beschreiben die Verbindung vieler einzelner Übertragungskanäle und Quantenprozessoren zu einem Netzwerk, sodass über große Distanzen und mit vielen Parteien Information in Quantenform ausgetauscht werden kann. Quantennetzwerke ermöglichen so Quantenkommunikation im großen Maßstab, aber auch verteiltes Quantencomputing.




Forschungsförderung

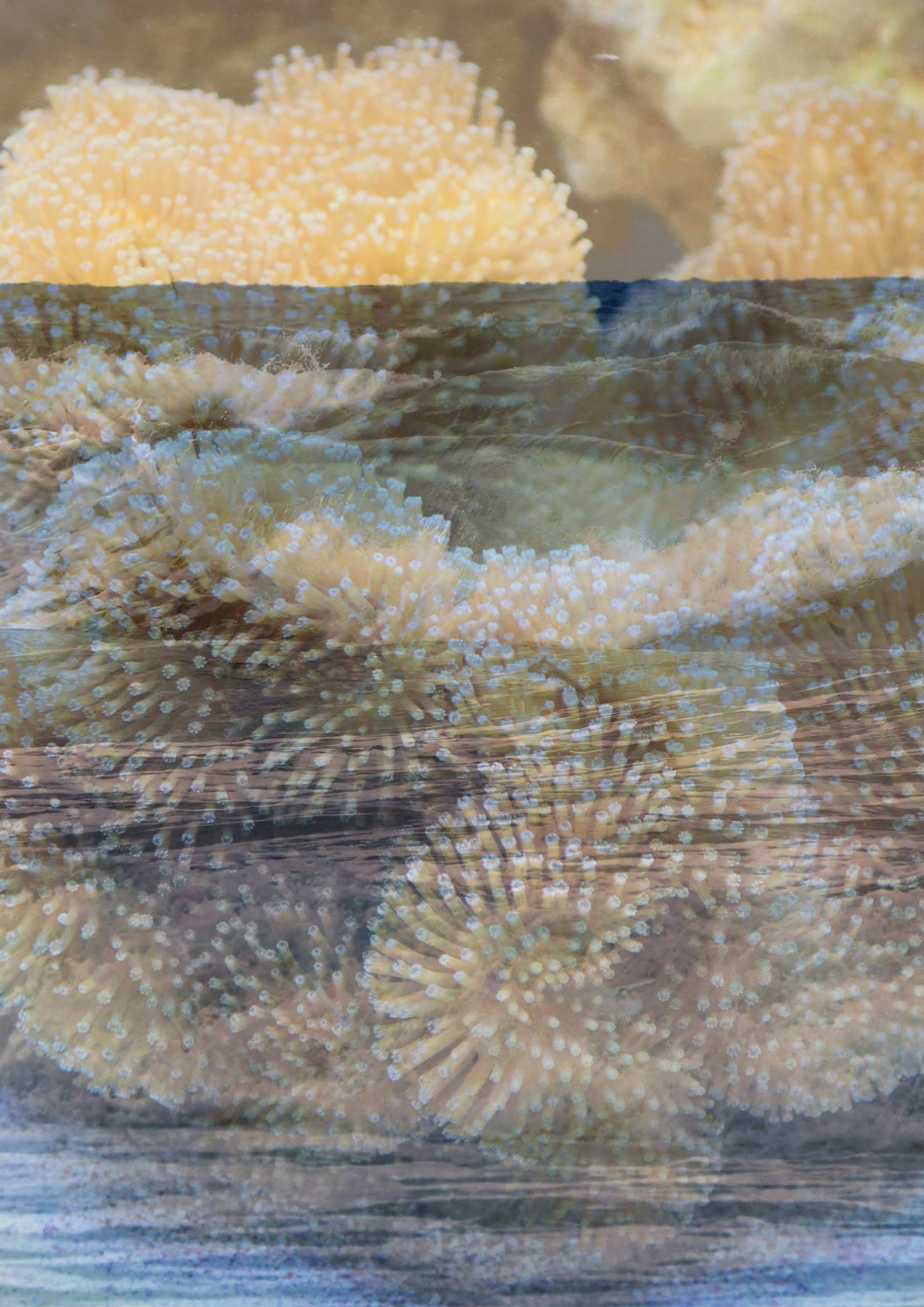

Publikationen


Gründungen


Suchanfragen

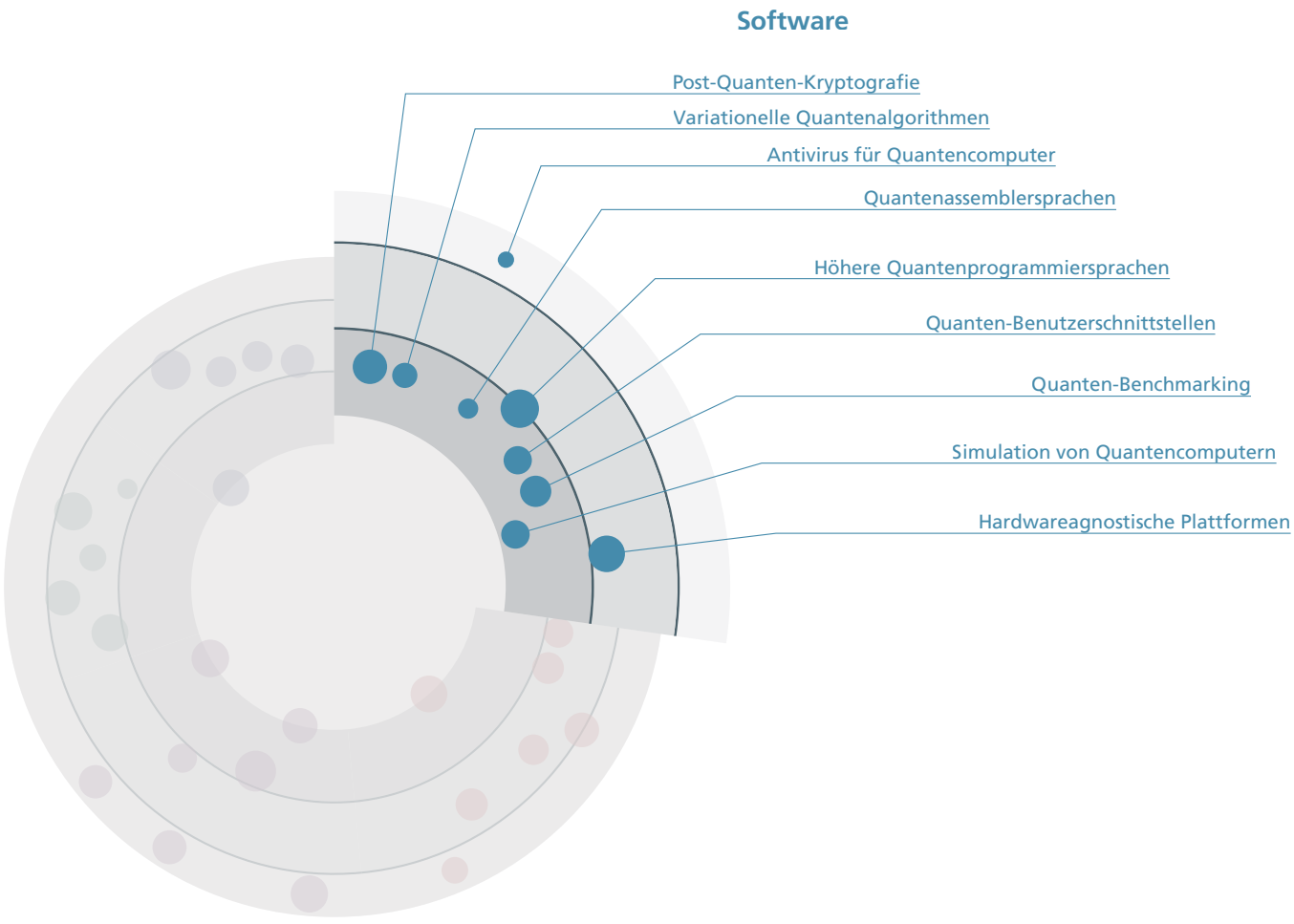

Patente


News



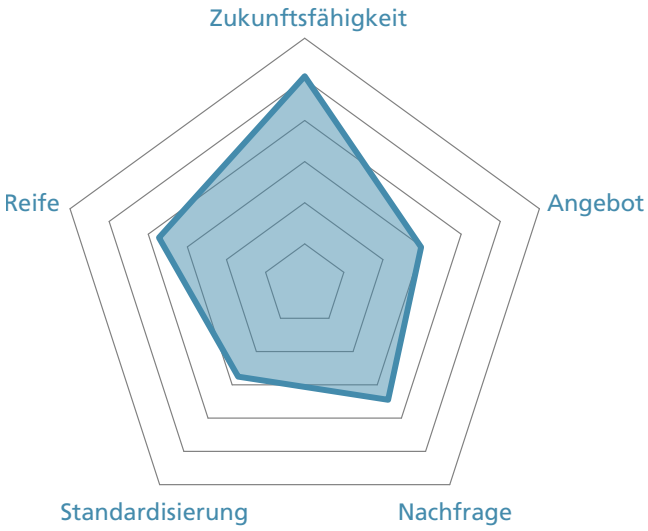
3.5 Software

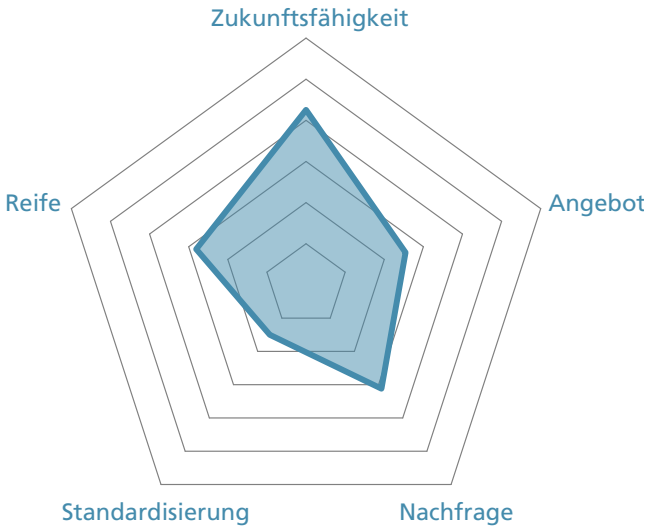
Quanten-IKT erfordert neue Software, und zwar sowohl für Quanten-IKT als auch für klassische IKT. Dies betrifft zum Beispiel Verschlüsselungen, die gegenüber Quantencomputern sicher sind, oder Sprachen und Schnittstellen, die Programmierbarkeit und Nutzbarkeit von Quanten-IKT ermöglichen. In diesem Abschnitt werden wesentliche Konzepte, Technologien und Verfahren zusammengefasst, die verschiedene Software-Bedarfe aus dem Umfeld der Quanten-IKT addressieren und teilweise erst gemeinsam die Funktionstüchtigkeit von Quanten-IKT ermöglichen.



Post-Quanten-Kryptografie

Post-Quanten-Kryptografie umfasst klassische kryptografische Verfahren, die nicht nur gegenüber klassischen Rechnern, sondern auch gegenüber Quantencomputern sicher sind. Die Sicherheit der heute weit verbreiteten Public-Key-Verfahren basiert auf mathematischen Aufgaben, zum Beispiel dem Faktorisierungsproblem, die sich nicht effizient mit klassischen Computern lösen lassen. Allerdings existieren Algorithmen für Quantencomputer, mit denen eine effiziente Lösung möglich ist, sobald Quantenrechner ausreichend leistungsfähig geworden sind. Daher sind die etablierten Public-Key-Verfahren nicht sicher gegenüber Quantencomputern, weshalb neue Verfahren erforderlich sind. Post-Quanten-Kryptografie war bereits Gegenstand des Trendsonars IT-Sicherheit aus dem Jahr 2016. Im Vergleich zeigt sich, dass Expert:innen die Technologie hinsichtlich der Dimensionen Standardisierung, Reife, Nachfrage und Angebot mittlerweile deutlich höher einschätzen, während die Zukunftsfähigkeit einen ähnlichen Wert aufweist.



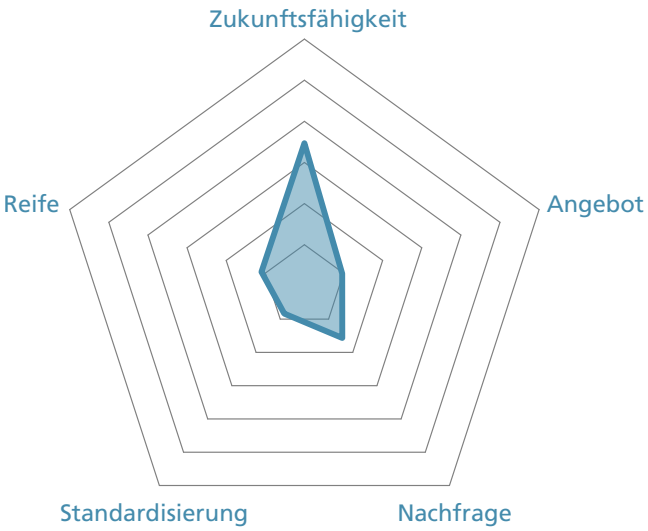


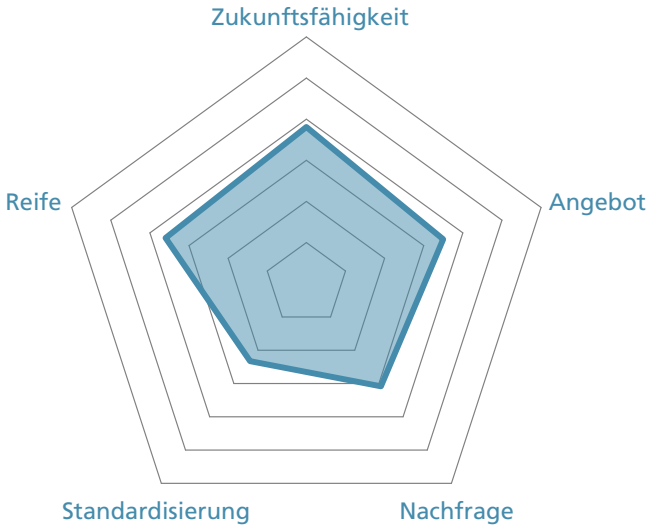
Variationelle Quantenalgorithmen

Bei variationellen Quantenalgorithmen handelt es sich um eine Menge von Methoden zur Lösung von Problemen mit Quantencomputern. Hierbei wird eine parametrisierbare Quantenschaltung genutzt. Für ein gegebenes Problem werden die Parameter mithilfe eines klassischen Rechners schrittweise optimiert. Das Vorgehen weist also Ähnlichkeiten zu klassischen Methoden der Optimierung und des Maschinellen Lernens auf. Es gilt als vielversprechender Kandidat, um schon während der NISQ-Ära (Noisy Intermediate-Scale Quantum Computing) Vorteile gegenüber klassischen Rechnern zu erreichen.

Antivirus für Quantencomputer

Sowohl Quantenkommunikationsnetzwerke als auch Quanten-Cloud-Hardware, die mehreren Nutzer:innen zur Verfügung steht (»Multi-Tenancy«), bieten Angriffsflächen. So sind zum Beispiel Fault-Injection-Angriffe möglich. Antivirus für Quantencomputer umfasst Methoden, die derartige Angriffe verhindern sollen, etwa indem Code vor der Ausführung auf verdächtige Muster untersucht wird.



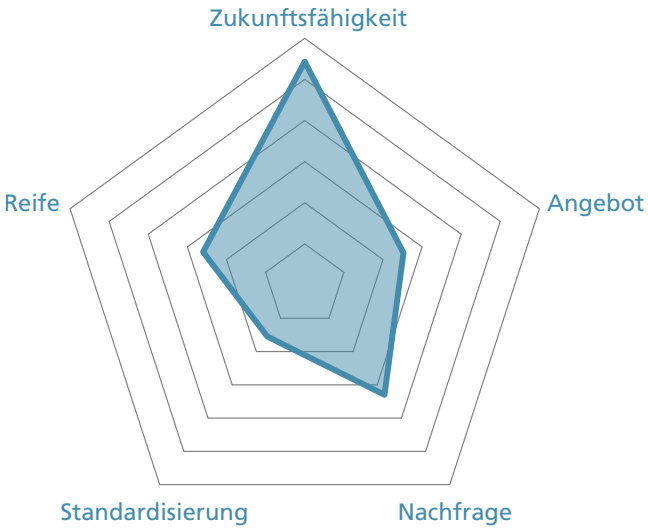


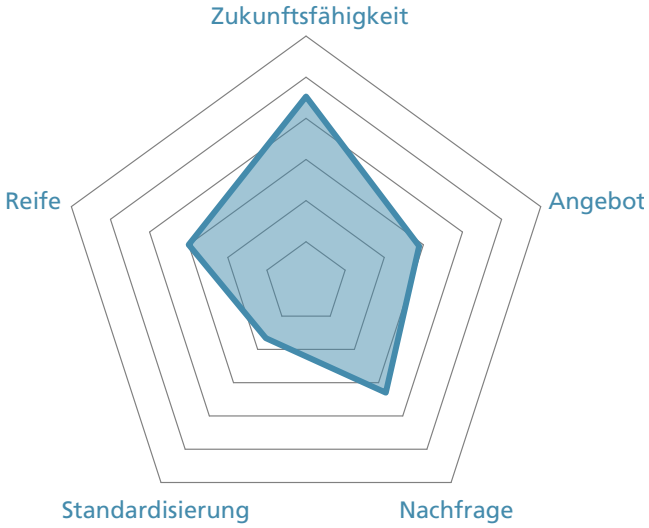
Quantenassemblersprachen

Bei Quantenassemblersprachen handelt es sich um relativ hardwarenahe Programmiersprachen für Quantencomputer, bei denen zum Beispiel spezifische Qubits angesprochen und teilweise auch Gatter kalibriert werden. Während dies vorteilhaft sein kann, um spezifische Quanten-Hardware optimal zu nutzen, kann nur in kleinen Schritten programmiert werden.

Höhere Quantenprogrammiersprachen

Hierbei handelt es sich um Programmiersprachen für Quantencomputer, die ein relativ hohes Abstraktionslevel haben im Vergleich zu zum Beispiel Assemblersprachen und Maschinencode. Dadurch sind sie ähnlich wie etwa Hochsprachen für klassische Rechner weniger hardwarenah und kleinschrittig und sollen so schnelleres und weniger fehleranfälliges Programmieren ermöglichen.



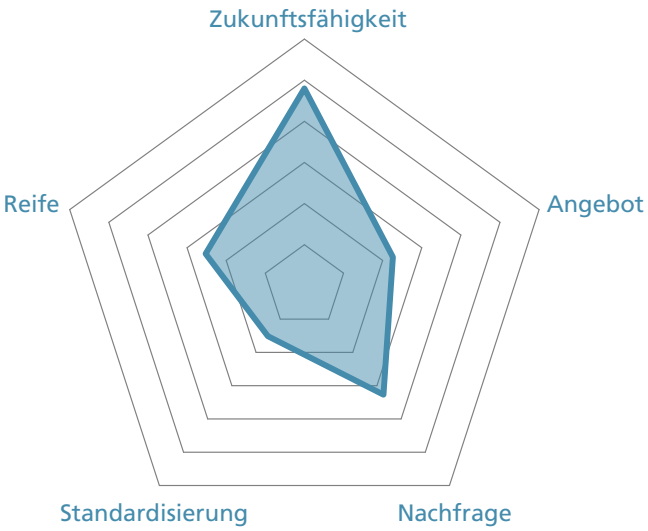


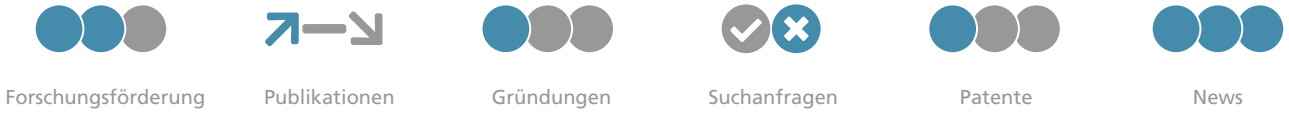
Quanten-Benutzerschnittstellen

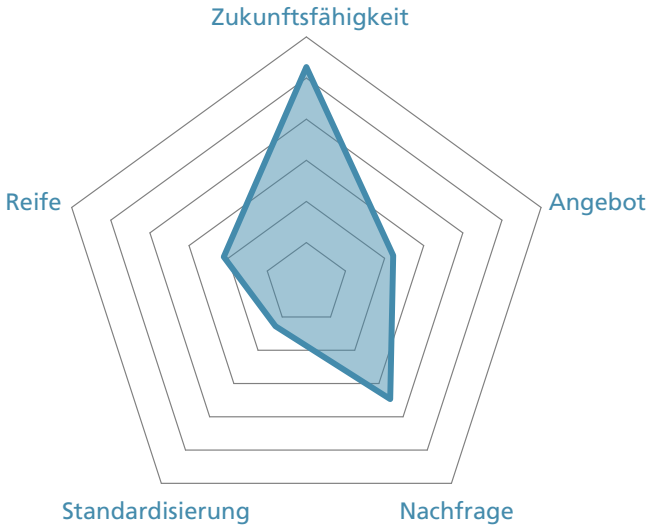
Solche Schnittstellen sollen die Arbeit mit Quantencomputern für Menschen vereinfachen. Dazu gehören in der Regel Möglichkeiten, Code einzugeben, eine grafische Visualisierung der konstruierten Quantenschaltung (eventuell mit Drag-&-Drop-Funktionalität), die Möglichkeit, den Code auf Simulatoren oder echten Quantenrechnern auszuführen, sowie eine (oftmals grafische) Aufbereitung der Ergebnisse.

Quanten-Benchmarking

Quanten-Benchmarking ermöglicht Vergleiche verschiedener Hard- und Softwareansätze, etwa bezüglich der Rechengeschwindigkeit und Effizienz. Dadurch können zum Beispiel Fortschritte bei der Entwicklung von Quanten-IKT messbar gemacht oder die passende Hard- oder Software für eine bestimmte Anwendung identifiziert werden. Beim Benchmarking im Bereich Quantencomputing bestehen allerdings verschiedene Herausforderungen, wie etwa die starke Unterschiedlichkeit der Hard- und Softwareansätze.





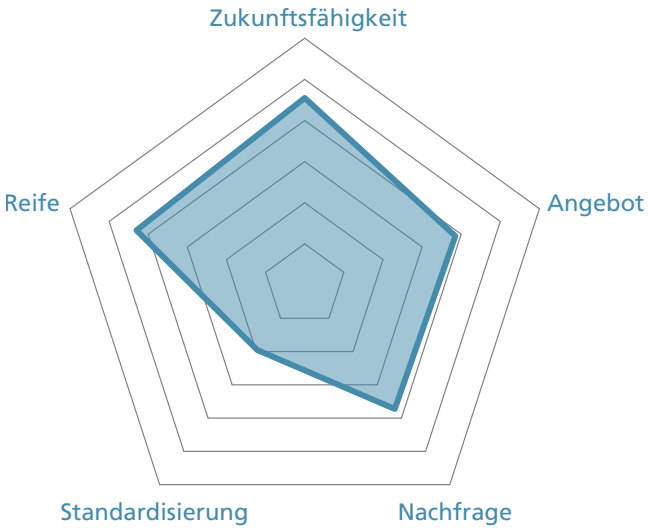


Hardwareagnostische Plattformen

Konkurrierende Hardwareansätze im Bereich Quantencomputing unterscheiden sich mitunter stark und erfordern oft spezifische Anpassungen etwa von Code. Hardwareagnostische Plattformen sollen Anwendungen und Softwareentwicklung aus Sicht der Nutzer:innen stärker von der Hardware entkoppeln und so die Nutzung erleichtern. Dazu wird zum Beispiel nutzergenerierter Code automatisch für Hardware optimiert. Idealerweise bieten solche Plattformen auch höhere Quantenprogrammiersprachen und aussagekräftige Leistungsvergleiche für Quanten-IKT-Systeme.

Simulation von Quantencomputern

Klassische Rechner können Quantencomputer mit geringer Größe simulieren. Dabei ist es möglich, sowohl fehleranfällige als auch bisher nicht existierende »perfekte« Quantencomputer zu simulieren. Klassische Rechner können dadurch bei der Entwicklung und beim Testen von Algorithmen für Quantencomputer und beim Erlernen des Umgangs mit Quantenrechnern helfen.




Forschungsförderung


Publikationen


Gründungen


Suchanfragen


Patente


News

4. Zukunft der Quanten-IKT

Das Technologiefeld Quanten-IKT ist noch jung und die Weiterentwicklung stellt eine große Herausforderung dar. Entsprechend fällt der Reifegrad vieler Technologien gering aus und der praktische Nutzen ist zumeist begrenzt. Die Expert:innenbefragung stützt dies: Die durchschnittlichen Werte für Reife- und Standardisierungsgrad sowie Angebot sind niedrig. Dass sich Quanten-IKT in einer frühen Phase befindet, zeigt auch der Vergleich mit den Ergebnissen der ÖFIT-Trendsonare zu Künstlicher Intelligenz und dem Internet der Dinge. Die Durchschnittswerte für die Dimensionen Angebot, Reife und Standardisierung fielen dort klar höher aus.

Quanten-IKT besitzt großes Potenzial. Dies zeigt sich auch durch die zumeist hohen Werte für die Dimension Zukunftsfähigkeit. Gleichzeitig herrscht derzeit aber auch Ungewissheit hinsichtlich der weiteren Entwicklung. Um diese Entwicklung mitzusteuern und bereit zu sein für Durchbrüche, kann ein Monitoring hilfreich sein. Publikationen wie das ÖFIT-Trendsonar, aber auch die Roadmaps von Anbietern können ein Ausgangspunkt sein, um regelmäßig – zum Beispiel jährlich – den Stand von Technologien zu erfassen. So lässt sich zum Beispiel nachvollziehen, ob die erwartete Entwicklungsgeschwindigkeit einer Technologie realisiert wird. Aufgrund dessen, dass verschiedene Technologien innerhalb der Quanten-IKT voneinander abhängig sind, ist ein gesamtheitliches Monitoring sinnvoll.

Während bei der Mehrheit der Quanten-IKT-Technologien der Durchbruch noch mehrere Jahre entfernt ist, existieren auch Ausnahmen. Dies gilt zum Beispiel für Quantenzufallsgeneratoren, die bereits 2020 Bestandteil von in Südkorea verkauften Smartphones waren. Es existieren bereits einige kleine Netzwerke, die genutzt werden, um mithilfe von Quantenschlüsselaustausch die Übertragung besonders schützenswerter Information abzusichern. Daraus folgt, dass bei Photonenqubits im Bereich der Quantenkommunikation bereits der technologische Durchbruch geglückt ist. Für eine Verwendung im Bereich des Computings gilt dies aber nicht. Generell ist der Kommunikationsbereich der Quanten-IKT etwas weiter fortgeschritten als der Computingbereich.

Der technologische Durchbruch einer Technologie kann aus unterschiedlichen Gründen von anderen Technologien abhängig sein. So kann eine Technologie zum Beispiel eine für die Funktionstüchtigkeit einer anderen Technologie unverzichtbare Komponente sein, eine kleinere Version einer anderen Technologie darstellen oder die Nutzbarkeit in großem Maße erhöhen. Zwei Langzeitziele der Quanten-IKT sind die Entwicklung großer, fehlertoleranter Universalquantenrechner und weltweiter Quantenkommunikationsnetzwerke. Die Quantenrechner sollen eine Vielfalt von Problemen bearbeiten können und dabei aufgrund ihrer Größe und Fehlertoleranz tatsächlich auch erhebliche Vorteile gegenüber klassischen Rechnern bei der Lösung praktisch relevanter Probleme bieten. Die Quantenkommunikationsnetzwerke sollen ein Quanteninternet bilden, also den Informationsaustausch zwischen vielen verschiedenen und weltweit verteilten Kommunikationsparteien mit Quanteneffekten zuverlässig absichern. Für die zwei Langzeitziele wurden die Abhängigkeiten zwischen Technologien visualisiert ergänzt um eine Schätzung des Jahres, ab dem der technologische Durchbruch erfolgen könnte (siehe Abbildung 3).

Um zum Beispiel große, fehlertolerante Universalquantencomputer zu erreichen, sind unter anderem technologische Durchbrüche bei der Quantenfehlerkorrektur und bei gatterbasierten Quantenrechnern erforderlich. Um einen Durchbruch bei gatterbasierten Quantenrechnern zu ermöglichen, ist dann wiederum ein gewisser technologischer Reifegrad bei Qubits notwendig.

Die Entwicklung von Quantennetzwerken mittlerer Größe, also etwa von Netzwerken, die mehrere Großstädte innerhalb eines Landes verbinden, ist ein Zwischenschritt bei der Skalierung solcher Netzwerke zu einem Quanteninternet. Netzwerke mittlerer Größe können aber bereits den Quantenschlüsselaustausch für Kommunikationsparteien in vielen verschiedenen Städten ermöglichen.

Die Verdeutlichung von Abhängigkeiten zwischen einzelnen Technologien erleichtert es, den aktuellen Entwicklungsstand von Quanten-IKT einzuschätzen und mögliche Entwicklungspfade zu analysieren. So lässt sich die Unsicherheit bezüglich der zukünftigen Entwicklung der Quanten-IKT ein Stück weit reduzieren.

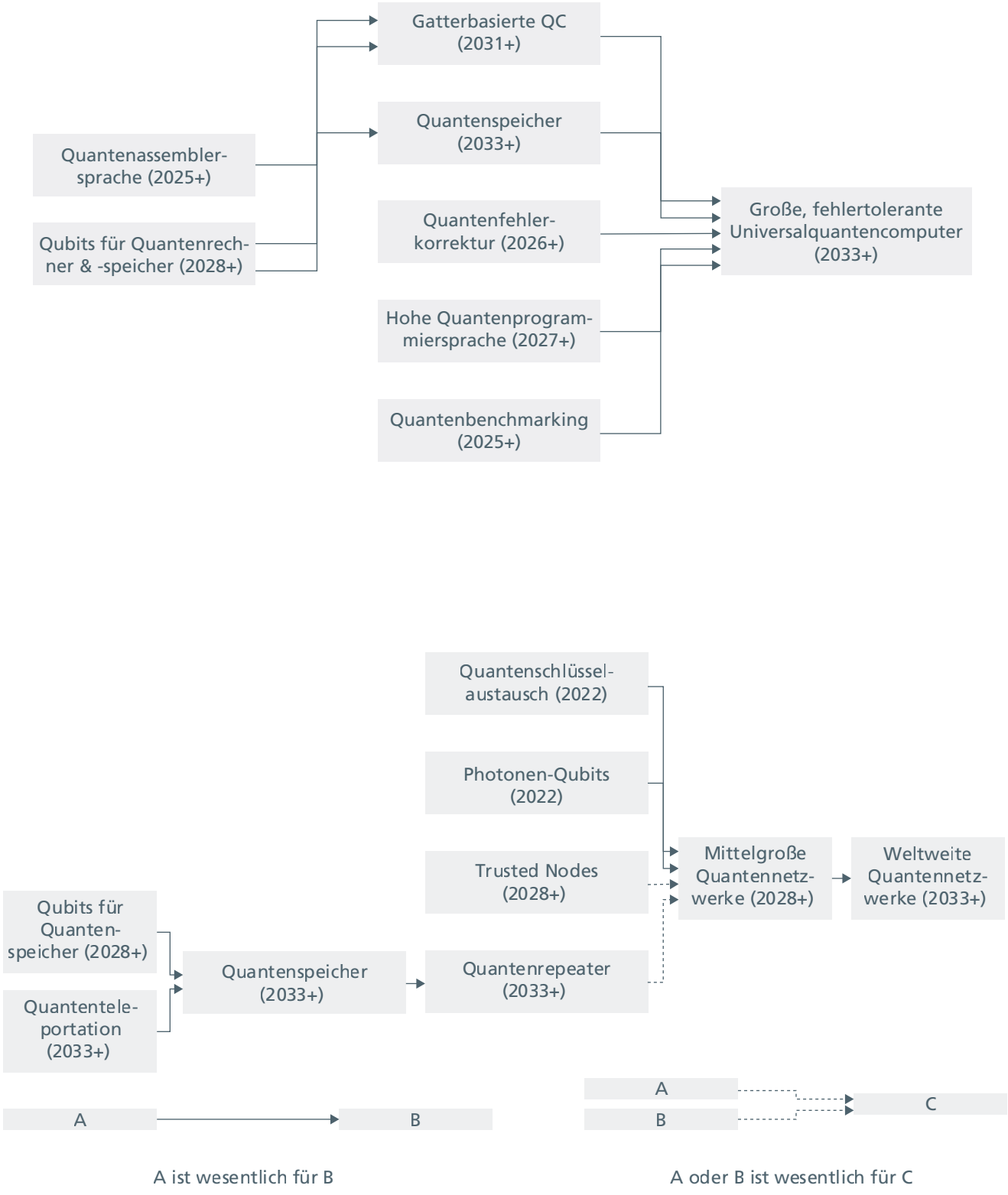


Abbildung 3: Abhängigkeiten zwischen Quanten-IKT-Technologien

Anhang A: Methodische Anmerkungen

Die ÖFIT-Trendsonare basieren auf einem einheitlichen methodischen Vorgehen. Die Identifikation und Analyse der Technologietrends im Bereich Quanten-IKT erfolgte durch qualitative Methoden, die durch quantitative Analysen flankiert wurden. Den Kern bilden qualitative Bewertungen durch Expert:innen aus Forschung und Anwendung in den Bereichen Quantencomputing und -kommunikation, die durch quantitative Ergebnisse ergänzt wurden.

Die initiale Auswahl **relevanter Trends** ergab sich aus Vorarbeiten für das Anfang 2022 erschienene ÖFIT-Whitepaper Quanten-IKT sowie einer Recherche zu in den letzten beiden Jahren auf dem Preprintserver arXiv erschienenen Publikationen zum Thema Quanten-IKT. Ergänzt durch die unten näher beschriebenen quantitativen Indikatoren wurden diese Technologietrends kategorisiert und bezüglich ihrer Relevanz bewertet.

Im nächsten Schritt wurden die Trends mithilfe eines Online-Fragebogens hinsichtlich der Dimensionen **Zukunftsfähigkeit, Reife, Angebot, Nachfrage** und **Standardisierung** auf einer Skala von eins bis zehn durch Expert:innen aus dem Bereich Quanten-IKT bewertet.

Bei der Dimension **Zeitraum bis zum technologischen Durchbruch** handelt es sich um eine Schätzung mit mehreren Einflussfaktoren. Eine Grundlage waren existierende Schätzungen des aktuellen Technology Readiness Levels (abgekürzt auch TRL) und der Zeitspanne bis zum Durchbruch in Studien sowie in Roadmaps genannte Ziele für Technologien. Auch die Einschätzung des aktuellen Reifegrades aus der Expert:innenumfrage wurde zurate gezogen. Zwischen einzelnen Technologien existieren Abhängigkeiten. Derartige Abhängigkeiten zwischen Technologien, beispielhaft dargelegt im vorigen Abschnitt, wurden berücksichtigt, um eine konsistente Modellierung der Dimension zu erreichen.

Die quantitativen Ergänzungen stützen sich auf die Ergebnisse von Suchanfragen bei verschiedenen Datenbanken. Bei allen Suchanfragen wurde eine Stichwortsuche durchgeführt, in der auch Synonyme und gängige Abkürzungen in deutscher und englischer Sprache berücksichtigt wurden.

Für die Daten aus den **Forschungsförderprogrammen** wurden Forschungsprojekte der Deutschen Forschungsgemeinschaft (DFG) und des Community Research and Development Information Service (CORDIS) der EU analysiert.

Die Daten zu **wissenschaftlichen Publikationen** stammen aus den Datenbanken Scopus, IEEE Xplore und dem Preprintserver arXiv. Die Suchergebnisse wurden nach Erscheinungsdatum der Publikation kategorisiert. Dabei wurden die Publikationen zu den Zeitabschnitten »2013 bis 2017« und »Ab 2018« zusammengefasst. Der Vergleich der Gruppen erlaubt Aussagen dazu, wie sich die Publikationstätigkeit zu einer Technologie entwickelt hat.

Die Daten zu **Gründungen** beruhen auf der Auswertung einer Auflistung zu Quanten-Start-ups, die auch der Publikation »The Landscape of the Quantum Start-up Ecosystem« zugrunde lag und uns durch den Autor zugänglich gemacht wurde. Vielen Dank an dieser Stelle an Zeki Seskir.

Für die **Suchanfragen** wurden Statistiken von Google Trends genutzt. Dabei wurden die Häufigkeiten der Suchanfragen für die Zeiträume 2013 bis 2017 und 2018 bis 2022 erfasst. Anhand dieser Zahlen erfolgte eine Einordnung in die Kategorien »Zunahme«, »gleichbleibend« und »Abnahme« für die Entwicklung der Suchanfragen im zeitlichen Verlauf. Nicht für alle Technologien gab es Ergebnisse bei Google Trends, deshalb erfolgte für manche Technologien auch keine Einordnung in eine der drei Kategorien.

Zur Auswertung existierender **Patente** wurde die Datenbank von PatBase genutzt. Dabei wurden die Familien von Patentanträgen gezählt, für die mindestens ein Patent erteilt wurde. Die Daten wurden rein quantitativ erhoben und wurden größenmäßig in die Kategorien »gering«, »mittel« und »hoch« eingeteilt.

Die Kategorie **Medien** basiert auf Statistiken von Google News. Dabei wurde die Erwähnung der Trendbegriffe im Zeitraum 2017 bis 2022 erfasst und größenmäßig in die Kategorien »gering«, »mittel« und »hoch« eingeteilt.

Anhang B: Tabellen

μ: Mittelwert, σ: Standardabweichung

	Zukunfts-fähigkeit		Reife		Angebot		Nachfrage		Standardisie-rung	
	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
Anwendungen										
Optimierung mit Quantencomputern	8,3	2,4	4,9	1,2	4,9	1,7	7,2	2,1	2,7	1,3
Maschinelles Lernen mit Quantencomputern	7,9	2,1	4,0	1,6	3,9	2,1	6,6	2,6	2,4	1,3
Sampling von Wahrscheinlichkeitsverteilungen	7,9	2,4	4,5	1,9	3,9	2,1	4,7	2,0	2,2	1,5
Simulation mit Quantencomputern	9,2	1,5	4,6	1,6	4,0	1,7	6,9	2,4	2,4	1,3
Quantenkommunikation	8,8	1,6	5,8	1,7	5,2	1,8	6,9	2,4	3,7	1,4
Qubits										
Supraleitungs-Qubits	7,8	2,4	5,1	1,1	5,6	1,2	6,0	1,7	2,7	1,4
Ionenfallen-Qubits	8,1	2,3	5,5	1,4	4,6	1,1	5,4	1,5	2,5	1,3
Topologische Qubits	8,5	1,8	2,9	1,5	2,2	1,2	4,5	2,1	1,6	0,8
Stickstoff-Fehlstellen-Qubits	7,9	2,4	4,3	1,9	3,6	1,9	4,9	2,5	2,3	1,4
Photonen-Qubits	8,8	1,9	4,9	2,0	3,8	1,8	5,5	2,8	2,4	1,5
Quantenpunkt-Qubits	8,1	1,5	4,6	2,0	3,6	1,8	4,3	2,1	2,3	1,4
Qudits	7,3	2,7	2,6	1,3	2,2	1,3	3,0	1,8	1,5	0,6
Systemkomponenten										
Quantenschlüsselaustausch	8,9	1,7	6,7	1,9	5,6	1,6	6,6	2,1	4,5	1,8
Trusted Nodes	7,7	2,4	5,4	2,1	5,1	1,8	5,3	2,3	3,6	1,9
Quantenrepeater	8,4	2,0	3,1	2,0	2,6	1,6	5,3	2,3	2,1	1,6
Quantenteleportation	8,3	2,4	3,4	1,8	2,6	1,7	3,4	1,8	1,8	0,9
Quantenfehlerkorrektur	9,4	1,1	4,4	1,5	3,2	1,4	7,3	2,4	2,4	1,3
Quantenzufallsgeneratoren	8,6	1,6	7,8	2,0	7,2	1,9	6,2	1,8	4,1	2,1
Quantenspeicher	8,9	2,1	2,4	1,6	1,8	1,5	4,9	3,0	1,5	1,2
Architektur										
Quanten-Annealer	6,3	2,2	5,9	1,6	5,1	1,8	5,9	1,8	3,0	1,8
Gatterbasierte Quantencomputer	9,0	1,5	3,7	1,6	4,7	1,4	6,5	1,9	2,9	1,5
Quantensimulatoren	7,3	1,9	5,5	1,6	4,1	1,8	5,0	2,0	2,5	1,6
Verteiltes Quantencomputing	8,6	2,0	3,1	1,5	2,7	1,6	4,6	2,4	2,1	1,3
Quantennetzwerke	8,9	1,5	3,5	1,6	2,9	1,4	5,1	2,0	2,6	2,2
Software										
Post-Quanten-Kryptografie	8,5	2,1	6,2	1,8	5,0	1,8	5,8	2,1	4,6	1,9
Variationelle Quantenalgorithmen	7,1	2,7	4,7	1,9	4,2	2,1	5,2	2,2	2,5	1,4
Antivirus für Quantencomputer	5,8	2,8	1,8	1,1	1,6	1,1	2,6	1,8	1,4	0,8
Quantenassemblersprachen	6,3	2,4	6,0	1,8	5,8	2,0	5,1	2,1	3,9	2,1
Höhere Quantenprogrammiersprachen	9,0	1,4	4,3	1,7	4,2	1,9	5,5	2,2	2,6	1,4
Quanten-Benutzerschnittstellen	7,5	2,7	5,0	1,6	4,8	1,3	5,5	1,9	2,8	1,2
Quanten-Benchmarking	8,0	2,2	4,2	1,4	3,8	1,0	5,5	2,1	2,5	1,3
Hardwareagnostische Plattformen	8,8	1,9	3,5	1,6	3,7	1,6	5,8	2,0	2,1	1,2
Simulation von Quantencomputern	7,6	2,0	7,2	1,5	6,4	1,8	6,2	1,7	3,3	1,2

Anhang C: Quellenverzeichnis

ÖFIT-Publikationen:

Opiela, Nicole et al. (2016): »Das ÖFIT-Trendsonar der IT-Sicherheit«, 1. Auflage Mai 2016. Kompetenzzentrum Öffentliche IT, Berlin. www.oeffentliche-it.de/publikationen

Welzel, Christian et al. (2018): »Das ÖFIT-Trendsonar Künstliche Intelligenz«, 1. Auflage April 2018. Kompetenzzentrum Öffentliche IT, Berlin. www.oeffentliche-it.de/publikationen

Grosch, Dorian et al. (2021): »Das ÖFIT-Trendsonar Internet der Dinge«, 1. Auflage Juli 2021. Kompetenzzentrum Öffentliche IT, Berlin. www.oeffentliche-it.de/publikationen

Gumz, Jan Dennis et al. (2022): »Quanten-IKT Quantencomputing und Quantenkommunikation«, 1. Auflage Januar 2022. Kompetenzzentrum Öffentliche IT, Berlin. www.oeffentliche-it.de/publikationen

Datenquellen:

arXiv: https://arxiv.org/

Community Research and Development Information Service (CORDIS): https://cordis.europa.eu/projects/de

Deutsche Forschungsgemeinschaft (DFG): https://gepris.dfg.de/

Google News: https://news.google.com/

Google Trends: https://trends.google.de/trends/

IEEE Xplore: https://ieeexplore.ieee.org/

PatBase: https://patbase.com/

Scopus: https://www.scopus.com/

Gründungen: Seskir, Zeki Can et al. (2022): »The Landscape of the Quantum Start-up Ecosystem«. https://arxiv.org/abs/2205.01999.

Quellen zum technologischen Durchbruch:

Apeldoorn, Joran van und Groenland, Koen (2022): »A professional's guide to Quantum Technology – Part 5: When can we expect a useful Quantum Computer?«. https://www.quantum.amsterdam/part-5-when-can-we-expect-a-useful-quantum-computer-a-closer-look-at-timelines/.

Castellanos, Sara (2021): »Google Aims for Commercial-Grade Quantum Computer by 2029« in The Wall Street Journal. https://www.wsj.com/articles/google-aims-for-commercial-grade-quantum-computer-by-2029-11621359156.

Chapman, Peter (2020): »Scaling IonQ's Quantum Computers: The Roadmap«. https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap.

Cybersecurity and Infrastructure Security Agency (2022): »Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats«. https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum.

European Quantum Flagship (2020): »Strategic Research Agenda«. https://qt.eu/app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf.

Forschungszentrum Jülich GmbH (2020): »Quantum Technology – Lecture Notes« in Schlüsseltechnologien Band 210. https://juser.fz-juelich.de/record/884794/files/Schluesseltech_210.pdf.

Goldstein, Barbara (2021): »The Dream of a Common Language – international standards for the quantum economy«. https://www.itu.int/en/ITU-T/webinars/20210623/Documents/Goldstein%20Final.pdf?csf=1&e=GdALdj.

Gruppo Tim (2020): »Speciale: Quantum Technologies« in notiziario tecnico TIM. https://www.gruppotim.it/content/dam/gt/notiziario-tecnico/pdf/Notiziario-Tecnico-TIM-2020-n2.pdf.

GSM Association (2021): »Quantum Networking and Service«. https://www.gsma.com/newsroom/wp-content/uploads//IG-12-Quantum-Networking-and-Service.pdf.

IBM (2022): »Our new 2022 Development Roadmap«. https://www.ibm.com/quantum/roadmap.

Krelina, Michal (2021): »Quantum Technology for Military Applications«. https://arxiv.org/pdf/2103.12548.pdf.

KTN UK (2021): »Horizon Europe – Quantum Webinar«. https://www.slideshare.net/KTNUK/horizon-europe-quantum-webinar-cluster-4-destinations-4-and-5-slides.

Manzalini, Antonio (2020): »Topological Photonics for Optical Communications and Quantum Computing«. https://www.researchgate.net/publication/346766840_Topological_Photonics_for_Optical_Communications_and_Quantum_Computing.

Mehta, Ivan (2021): »Samsung's new phone has a 2.5 mm quantum random number generator for improved security«. https://thenextweb.com/news/samsungs-new-phone-has-a-2-5-mm-quantum-random-number-generator-for-improved-security.

Meige, Albert et al. (2022): »Unleashing the business potential of quantum computing«. https://www.adlittle.com/en/insights/report/unleashing-business-potential-quantum-computing.

Mustafa H. Balcı (2020): »Strategic Report: Quantum Key Distribution (QKD) Systems«. https://www.researchgate.net/publication/343837483_STRATEGIC_REPORT_Quantum_Key_Distribution_QKD_Systems.

NATO Science & Technology Organization (2020): »Science & Technology Trends 2020-2040«. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

Rigetti (2022): »Corporate Presentation«. https://investors.rigetti.com/static-files/fbac3801-223f-4f0f-a207-47d25084a1d7.

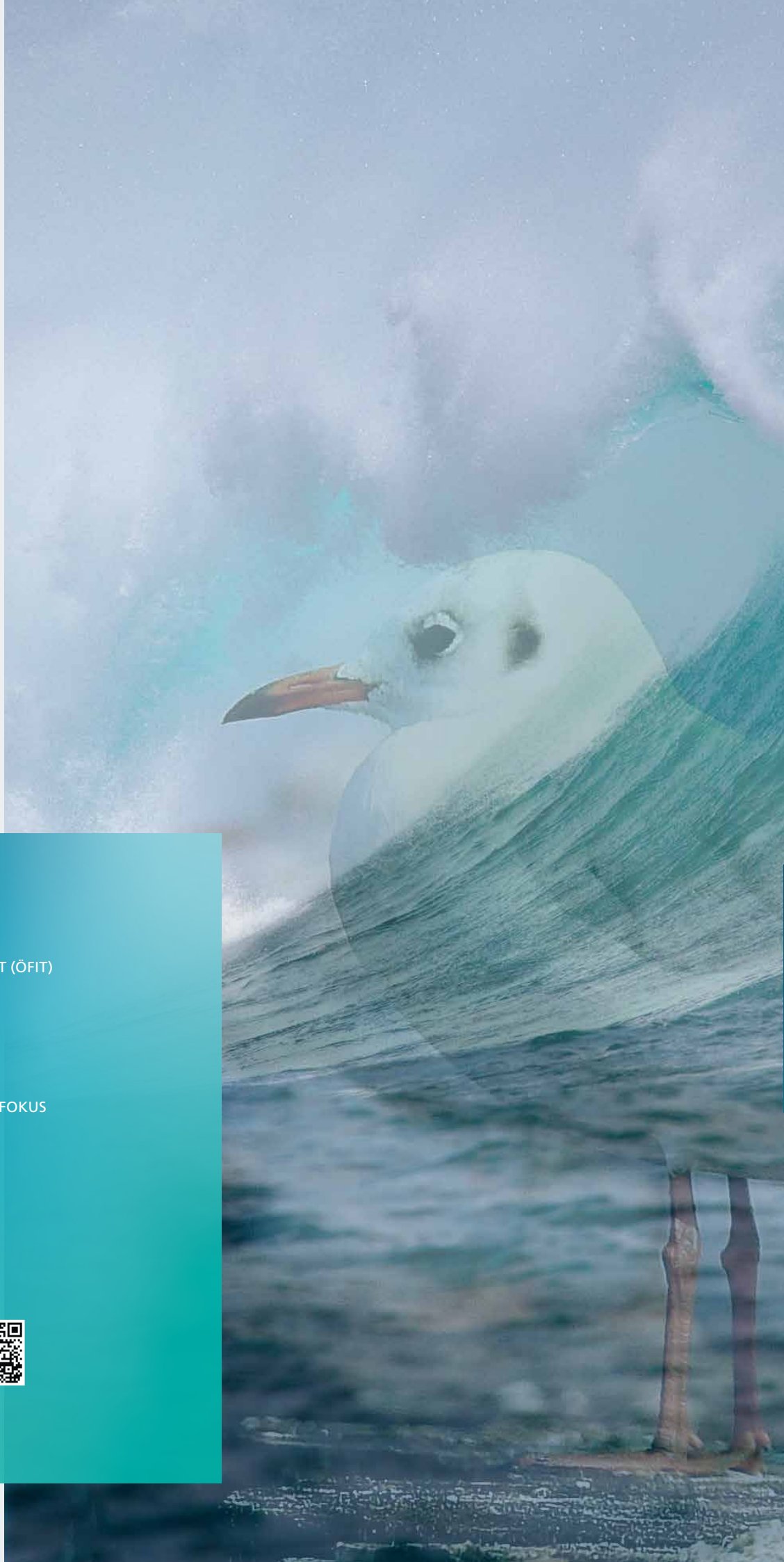
Sevilla, Jaime und Riedel, C. Jess (2020): »Forecasting timelines of quantum computing«. https://arxiv.org/pdf/2009.05045.pdf.

Siliezar, Juan (2021): »Team develops quantum simulator with 256 qubits, largest of its kind ever created«. https://phys.org/news/2021-07-team-quantum-simulator-qubits-largest.html.

The Australian Army (2021): »Army Quantum Technology Roadmap«. https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf.

VDI Technologiezentrum GmbH (2021): »Roadmap Quantencomputing«. https://quantumbusinessnetwork.de/wp-content/uploads/2021/02/Roadmap-Quantencomputing-bf-C1.pdf.

VentureBeat (2020): »IonQ's roadmap: Quantum machine learning by 2023, broad quantum advantage by 2025«. https://venturebeat.com/business/ionq-roadmap-quantum-machine-learning-2023-broad-quantum-advantage-2025/.



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: 978-3-948582-18-0

01123