Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Entwicklungsstand Quantencomputer

Deutsche Zusammenfassung

BSI-Projektnummer: 477

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	Mai 2018		Abschluss der Hauptphase des Projekts
1.1	Juli 2019		Erste Aktualisierung (Details siehe frühere Version dieser Studie)
1.2	Juni 2020		Zweite Aktualisierung (Details siehe frühere Version dieser Studie)
2.0	August 2023		Erste wesentliche Aktualisierung der Studie. Zu den Änderungen gehören eine Umstrukturierung und die Aufnahme von Änderungen auf Hardware-Seite, sowie von NISQ Entwicklungen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: qc@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Was ist ein Quantencomputer?

Heutige Computer behandeln Informationen gemäß den Gesetzen der klassischen Physik: Register und Speicherinhalte haben zu jedem Zeitpunkt einen einzigen Wert. Dies gilt ungeachtet der Tatsache, dass die Bauelemente eines Computers wie Transistoren auf den Gesetzen der Quantenphysik basieren.

In einem Quantencomputer wird die Information selbst quantenmechanisch behandelt: Register und Speicherinhalte können mehrere Werte gleichzeitig in Überlagerung enthalten, und Maschinenbefehle wirken sich simultan auf all diese Werte aus. Damit arbeitet bereits ein einziger Quantenprozessor intrinsisch hochgradig parallel, ohne parallelisierte Hardware wie mehrere Prozessorkerne zu benötigen. Dadurch lässt sich prinzipiell eine Quantenbeschleunigung, auch Quantenüberlegenheit genannt, erreichen. Diese bezeichnet die Realisierung von Berechnungen auf einem Quantencomputer, die von klassischen Rechnern nur unter prohibitivem Aufwand reproduziert werden können.

Nutzung dieser Parallelität erfordert allerdings Umgang mit dem probabilistischen Charakter der Quantenphysik und das Kompilieren von Algorithmen in quantenmechanisch erlaubte Gatter (Quantenschaltkreise). Aus diesem Grund erfordert die Nutzung der Quantenbeschleunigung zunächst die Entdeckung geeigneter Algorithmen. Zu diesen gehören bisher die schnelle Datenbanksuche, das Durchsuchen von Graphen, die Lösung linearer Gleichungssysteme, Anwendungen der schnellen Fouriertransformation einschließlich Faktorisierung und Berechnung diskreter Logarithmen, und die Simulation von Quantensystemen einschließlich Chemikalien und neuer Materialien, sowie Maschinenlernen und Optimierung. Für einige dieser Anwendungen, insbesondere die letztgenannten, ist die Quantifizierung der erreichbaren Quantenbeschleunigung noch Gegenstand aktueller Forschung. Quantencomputer sind – aufgrund der möglichen Anwendungen aber auch aufgrund der aufwändigen Hardware – auf der Ebene von Rechenzentrumstechnologie und Höchstleistungsrechnen anzusiedeln und keine Büro- oder gar mobile Technologie. Entsprechend sind die leistungsfähigsten Quantencomputer unserer Tage Großgeräte für Forschung und Entwicklung – sie erlauben die Entwicklung und Validierung von Algorithmen, sind aber (noch) nicht jenseits der Wissenschaft disruptiv.

Quantencomputer wurden zunächst als hypothetische, theoretische Konstruktion eingeführt. Inzwischen, nach mehr als 25 Jahren Entwicklung seit den ersten Laborexperimenten, konsolidiert sich das Feld der Hardwareplattformen und Zugriff auf Quantenprozessoren wird als Dienstleistung von mehreren Firmen angeboten; zudem wird eine sehr spezielle Quantencomputerplattform, das “Quantenannealing”, auch als Hardware kommerziell angeboten. Obgleich noch in einem frühen Entwicklungsstadium, erlauben all diese Quantenprozessoren die Entwicklung und Evaluation von Quantenalgorithmen.

Der Stand des Gebietes kann als Ära der frühen Quantenüberlegenheit bezeichnet werden. Diese Überlegenheit wurde an mehreren Stellen für sehr spezielle Benchmarkingprobleme erreicht. Nach aktuellem Wissensstand sind die Anforderungen, um bei anwendungsorientierten Problemen Quantenüberlegenheit zu erreichen deutlich höher. Unsere Studie untersucht diese Fragestellung für die Kryptoanalyse.

2 Relevanz von Quantencomputern für die Kryptoanalyse

Ein Großteil der heute auf breiter Basis eingesetzten asymmetrischen kryptographischen Verfahren kann nicht mehr als sicher betrachtet werden, sobald die Faktorisierung großer Ganzzahlen und die Berechnung sogenannter diskreter Logarithmen effizient möglich ist. Dies erklärt das signifikante Interesse an Quantencomputern in der kryptoanalytischen Forschung – Peter Shor zeigte Mitte der 90er Jahre erstmals, dass beide Probleme asymptotisch effizient gelöst werden können, wenn ein hinreichend großer und verlässlicher Quantencomputer verfügbar ist. Die Effizienz der Shor-Algorithmen beruht unter anderem auf der geschickten Nutzung von quantenmechanischer Überlagerung mehrerer Werte, einer Technik, die mit klassischen Bits nicht realisierbar ist. Quantencomputer verwenden als elementare Einheit Quantenbits, kurz Qubits, bei denen den klassischen Werten 0 und 1 lediglich die Rolle von Basiswerten zukommt, und der Wert eines Qubits gewichtete Anteile beider Basiswerte simultan innehaben kann. In ähnlicher Weise werden klassische Bitregister durch komplexe Quantenregister ersetzt, die effiziente hochdimensionale Berechnungen ermöglichen. Aus praktischer Sicht stellt sich die Frage, wie groß ein Quantencomputer sein muss, um real eingesetzte kryptographische Verfahren, etwa die RSA-Verfahren oder solche basierend auf elliptischen Kurven, zu gefährden. Hierzu ist eine genaue Analyse bekannter Quantenalgorithmen erforderlich. Die abstrakten Schritte eines Quantenalgorithmus müssen für das konkret angegriffene Verfahren (effizient) in Elementarschritte umgesetzt werden, die wiederum auf realer Hardware abbildbar sind.

Detaillierte Kostenanalysen sind erst in geringem Umfang in der Literatur verfügbar, und es ist realistisch anzunehmen, dass die bislang veröffentlichten Quantenschaltkreise noch weiter optimiert werden können. Aber die verfügbaren Arbeiten lassen es bereits machbar erscheinen, die Shor-Algorithmen für kryptographisch interessante Parameterwahlen in Quantenschaltkreise moderater Komplexität zu übersetzen.

Konkret werden nach aktuellem Forschungsstand für einen Angriff auf 2048 Bit RSA insgesamt $1.4 \cdot 10^{15}$ Elementarschritte auf 4098 logischen Qubits benötigt; andere Trade-offs zwischen der Anzahl der Rechenschritte und der Anzahl der Qubits sind möglich. Wiederum nach aktuellem Forschungsstand für den diskreten Logarithmus auf einer elliptischen Kurve über 256 Bit werden $6.5 \cdot 10^{13}$ Rechenschritte auf 2330 logischen Qubits benötigt. Logische Qubits sollten nicht mit physikalischen Qubits verwechselt werden, deren Konzept und Bedeutung wir in Abschnitt 3 besprechen, und die um Größenordnungen höher liegt. Nach einer aktuellen Abschätzung werden 20.000.000 physikalische Qubits als hinreichend für einen Angriff auf 2048 Bit RSA mit einer Laufzeit von acht Stunden betrachtet.

Für die symmetrische Kryptographie bieten Quantencomputer ebenfalls neue kryptoanalytische Möglichkeiten, aber mit den momentan bekannten Algorithmen sind die Auswirkungen deutlich weniger spektakulär als im asymmetrischen Fall. Auch hier kann davon ausgegangen werden, dass die besten vorhandenen quantitativen Aussagen, etwa zur Schlüsselsuche bei AES-128, noch verbessert werden (es wurden bereits mehrere Optimierungen vorgeschlagen), aber eine Vergrößerung der Schlüssellänge auf 256 Bit erscheint momentan eine wirksame Gegenmaßnahme. Weitere Quantenangriffe auf symmetrische Primitive sind bekannt, aber hierbei werden zum Teil Angriffsmodelle verwendet, die bei heute genutzten Implementierungen nicht realistisch sind.

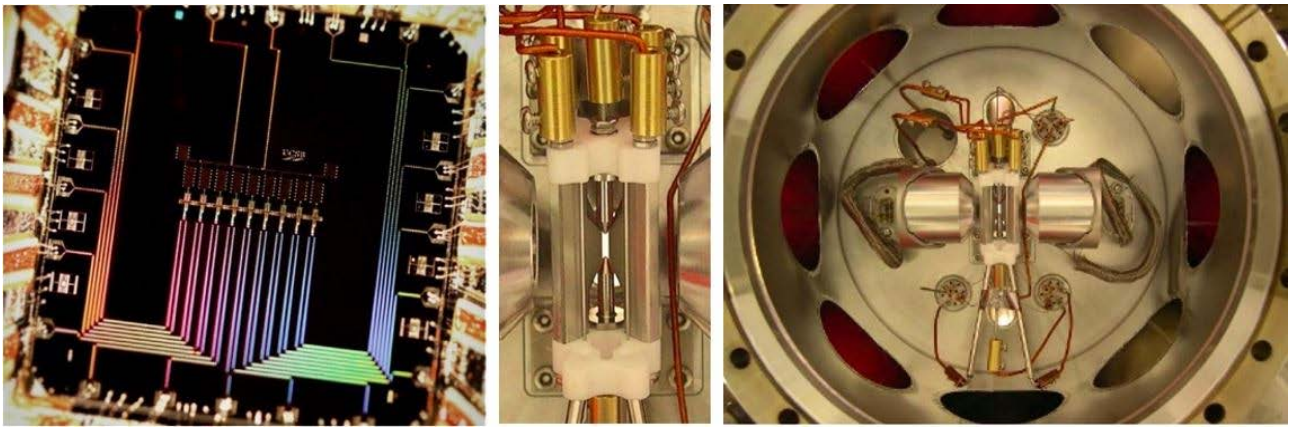

Abbildung 2.1: Die augenblicklich führenden Quantencomputing-Plattformen – mikroskopische Perspektive. Links: Prozessor bestehend aus integrierten supraleitenden Schaltkreisen. (Foto links: Julian Kelly, Google.) Mitte: Lineare Ionenfalle; Elektroden zum Fangen (Stäbe) und Linsen zum Einstrahlen von Lasern für Quantenlogik (links und rechts). Rechts: Die gleiche Ionenfalle eingebettet in ihre Vakuumapparatur. (Fotos mittig und rechts: Jürgen Eschner, Universität des Saarlandes.)

3 Hardware und Algorithmen für Quantencomputer

Die gesicherten Erkenntnisse über Quantenalgorithmen wären nicht relevant, würde nicht gleichzeitig Hardware entwickelt werden. Es wird eine ganze Reihe von Hardwareplattformen weltweit verfolgt, die sehr unterschiedlich sind – etwa vergleichbar mit dem Übergang von mechanischen zu elektronischen Computern. Die augenblicklich führenden Plattformen (siehe Abbildung 2.1) sind

1. Ionenfallen – eine Plattform die u.a. mit der Technologie von Atomuhren verwandt ist.
2. Integrierte Schaltkreise aus Supraleitern – eine Plattform, die Ähnlichkeit mit aktuellen Computerchips hat, jedoch aus anderen Materialien besteht und bei sehr tiefen Temperaturen betrieben wird. Hier ist vor allem eine spezielle Variante, nämlich das sogenannte zweidimensionale (2D) Transmon, ein Vorreiter.

Es wird eine Vielzahl weiterer Plattformen erforscht, die zwar im Augenblick weniger weit fortgeschritten sind, aber teils eine steile Entwicklung zeigen. Dazu gehören Donatoren in Silizium-Strukturen, Quantenpunkte in Halbleitern, gezielt dotierte künstliche Diamanten, auch Farbzentren genannt, neutrale Rydberg-Atome in Laserfeldern und photonische Systeme. Es sei darauf hingewiesen, dass Technologien, die derzeit nicht in großem Umfang verfolgt werden, wie molekulare Qubits oder Elektronen, die auf Helium gefangen sind, in einer alten Version dieser Studie behandelt sind.

Die führenden Plattformen werden zunehmend in industriellen oder öffentlich-privaten Partnerschaften erforscht und entwickelt. Dies spiegelt einerseits die Notwendigkeit fortlaufender Grundlagenforschung wider, ermöglicht aber andererseits die Entwicklung von funktionalen und vielschichtigen integrierten Systemen mit Prototypcharakter. Leider sind Teile der industriellen Forschung als Geschäftsgeheimnisse nicht zur Bewertung zugänglich.

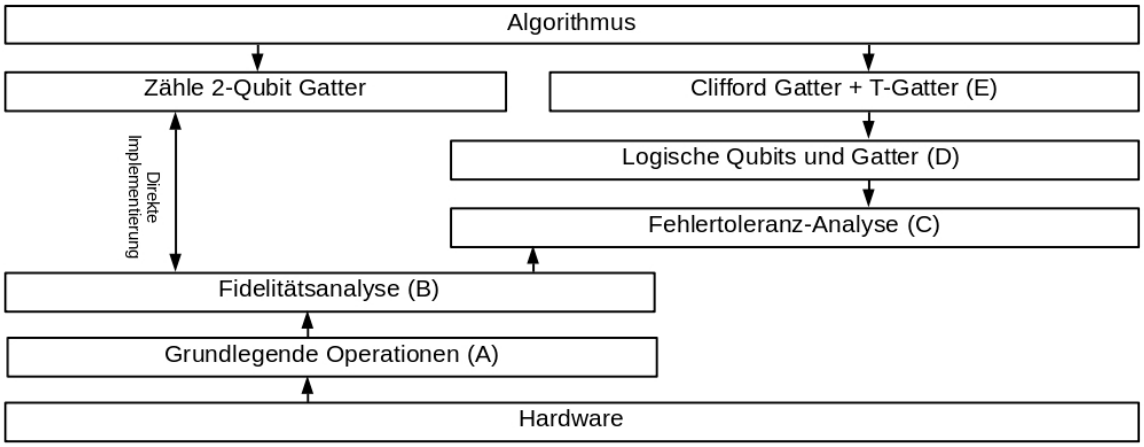

Abbildung 3.1: Abhängigkeitsgraph für Quantencomputer zwischen Algorithmen und Hardware. Daraus ergibt sich das hier verwendete Schichtenmodell zur Bewertung von Quantencomputerplattformen basierend auf NISQ [links, Stufen (A) und (B)] bzw. anhand demonstrierter Schritte zur Fehlertoleranz [rechts, Stufen (A) bis (E)].

Die wichtigste strukturelle Herausforderung des Gebietes ist dabei die Fehleranfälligkeit von Quantencomputern. Diese geht über das rein Technologische hinaus und ist grundsätzlicher Natur – der besondere Glücksfall der geringen Fehleranfälligkeit von klassischen Digitalrechnern tritt hier nicht ein. Auf der einen Seite zeigen belastbare Theorien, dass Quantencomputer kryptoanalytische Aufgaben bewältigen können, wenn sie aktiv fehlerkorrigiert werden. Auf der anderen Seite steht eine jüngere Erforschung kryptoanalytischer Anwendungen mit Quantencomputern, die nicht fehlerkorrigiert werden – auf diese Entwicklung gehen wir weiter unten ein. Ein konsistentes theoretisches Gerüst der Fehlerkorrektur wurde entwickelt. Seine praktische Umsetzung ist Gegenstand intensiver Forschung und erste Erfolge wurden

bereits erzielt. Diese Fehlerkorrektur beeinträchtigt die grundsätzliche Effizienz von Quantencomputing nicht, ist aber trotzdem durch einen enormen Overhead gekennzeichnet – die *logischen* Quantenbits (Qubits), die einen Algorithmus beschreiben, bestehen aus einer großen Zahl von Bauelementen, die *physikalische* Qubits darstellen. Auch bei großem Fortschritt ist davon auszugehen, dass der Bau eines leistungsfähigen fehlertoleranten Quantencomputers nicht nur eine wissenschaftlich-technische Herausforderung darstellt, sondern im Ergebnis eine Großanlage vom Umfang eines Rechenzentrums wäre.

Fehlerkorrektur ist dann effektiv, wenn alle Elemente der Hardware unter einer nativen Fehlerschwelle bleiben, welche je nach Methode und in den günstigsten Fällen zwischen 0.1% und 1% liegt. Praktische Experimente und Demonstrationen in den letzten 18 Monaten haben auf kleiner Skala die wesentlichen Konzepte der Fehlerkorrektur verifiziert und validiert, jedoch zeigt sich, dass in den meisten Fällen bestimme Funktionalitäten der Hardware noch nicht unter der nötigen Schwelle liegen.

Forschungsergebnisse und die sie begleitenden Schlagzeilen können im Kontext der benötigten aktiven Fehlerkorrektur evaluiert werden. Diese Studie enthält darum ein Schichtenmodell zur Bewertung von Quantencomputer-Kandidaten, veranschaulicht in Abbildung 3.1. Es beginnt mit der Demonstration von Grundfunktionen (Schicht A) bis hin zur fehlertoleranten Implementierung von Algorithmen (Schicht E).

Wie Abbildung 3.2 verdeutlicht, ist das Feld an Plattformen dicht, und eine schnelle Veränderung der Bewertung wird erwartet – in der Tat, klare Fortschritte wurden innerhalb weniger Jahre erreicht (vgl. Abbildung 3.2 mit der äquivalenten Abbildung aus einer vorherigen Version dieser Studie). Nach wie vor wird das Feld von Ionenfallen und 2D-Transmonen angeführt. Augenblicklich werden von diesen führenden Plattformen einige Elemente von Schicht D realisiert, wobei aber auch dort ein Element von Schicht C noch aussteht. Die Fertigung supraleitender Schaltkreise ist, u.a. durch langjährige Erfahrung mit verwandten Silizium-Strukturen, technologisch weit entwickelt, und lässt sich gut optimieren. Dies führt zu verfügbaren Quantenprozessoren mit über 400 Qubits. Diese größten Quantencomputer-Systeme beruhen dabei auf 2D-Transmonen, alternative Qubit-Schaltkreise werden aber weiterhin verfolgt und machen nennenswerte Fortschritte in der Entwicklung.

Auf die beiden führen Plattformen folgen Farbzentren und neutrale Rydberg-Atome. Bei dem hohen Entwicklungsstand der Rydberg-Atome im Stufenmodell sollte darauf hingewiesen werden, dass die erreichten Zahlen an Qubits pro Quantencomputer-Prozessor eine Größenordnung kleiner ist als die der zwei führenden Plattformen. Zu den außerdem relevanten Plattformen zählen die am weitesten zurückliegenden Halbleiter-Quantenpunkte und Silizium-Donatoren, sowie die Photonen. Letztgenannte weisen eine große Unsicherheit – dargestellt über die Breite in Abbildung 3.2 – im Entwicklungsstadium auf, was vor allem auf die bereits oben angesprochene Verschlossenheit von privaten Unternehmen in diesem Bereich zurückführen ist.

Darüber hinaus enthält diese Studie ein Schichtenmodell zur Einstufung von Quantenalgorithmen, das in Abbildung 3.3 gezeigt ist. Darin werden Algorithmen zunächst in zwei Kategorien unterteilt: einerseits diejenigen, deren Laufzeitverhalten für große Eingaben unbekannt sind und deren Leistung durch Heuristiken bestimmt werden müssen, andererseits solche Algorithmen, für die ein hinreichend solides Grundverständnis vorliegt, sodass eine Leistungsvorhersage für beliebig große Eingabewerte möglich ist. In beiden Fällen ist eine Analyse vonnöten, um die Relevanz des Algorithmus in Bezug auf derzeit eingesetzte kryptografische Verfahren vorherzusagen.

Vor der Etablierung fehlerkorrigierter Quantencomputer steht die Ära der “Noisy Intermediate-Scale Quantum (NISQ) Technologies", in der man die Fehler nicht korrigiert (aber ggf. durch hardwarenahe Methoden mitigiert) und darum nur auf eine begrenzte algorithmische Tiefe zurückgreifen kann, die durch die Fehlerwahrscheinlichkeit limitiert wird. In dieser Domäne werden native Freiheitsgrade der Hardware und alternative Programmierparadigmen kreativ genutzt. Die entstehenden Lösungen sind im Allgemeinen von heuristischer Natur und haben keinen mathematischen Konvergenzbeweis oder gar eine daraus abgeleitete Ressourcenanalyse. Um das Gebiet der NISQ-Algorithmen weiter beobachten zu können, schlagen wir ein separates Bewertungsschema vor. Da numerische Experimente in manchen Fällen Hinweise liefern können, sind NISQ-Algorithmen in unserer Algorithmus-Bewertung häufig Kandidaten für den “linken Zweig” in Abbildung 3.3. Die geringe vorliegende Evidenz lässt bisher keine abschließende Bewertung zu, erlaubt aber die vorsichtige Vermutung geringer Relevanz für die Kryptoanalyse. Da dieses

Gebiet weniger klar gegliedert ist als fehlertolerantes Quantencomputing, müssten hier etwaige disruptive Algorithmen direkt nach dem Passieren von Schicht B evaluiert werden.

Im Kontext des fehlertoleranten Quantencomputing sind noch viele Entwicklungsschritte nötig. Das Framing eines "Rennens" in der Quantencomputerentwicklung in der Öffentlichkeit ist darum nicht sachgerecht: Es sind noch viele Schritte zu gehen, die idealerweise durch Kooperation erreicht würden – mit Wettbewerb allenfalls in den Sprints bis zum nächsten Meilenstein.

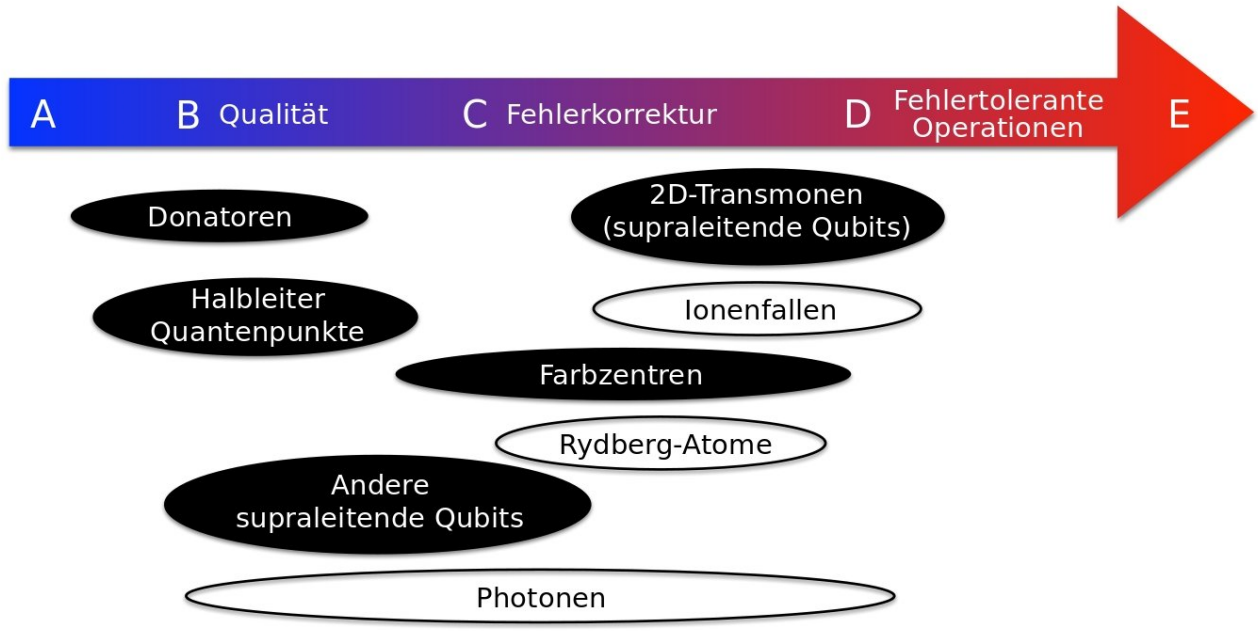

Abbildung 3.2: Einordnung verschiedener Plattformen im Schichtenmodell (siehe Abbildung 3.1). Die Breite der Ovale quantifiziert die Variabilität und die Ungewissheit (bspw. aufgrund fehlender belastbarer Veröffentlichungen von Daten) der verschiedenen Plattformen. Atomphysikalisch/optische Systeme sind weiß und Festkörpersysteme schwarz hinterlegt.

Es ist zu beachten, dass inzwischen deutlich mehr alternative Entwicklungspfade und technologische Optionen verfolgt werden als zur Zeit der vorherigen Versionen dieser Studie. Im Bereich Hardware werden einerseits die bisher führenden Plattformen (Supraleiter und Ionenfallen mit Surface- oder Color-Code) kontinuierlich weiterentwickelt. Andererseits entstehen neue Hardwareplattformen (z.B. Rydberg-Atome) die in einigen Aspekten bereits aufgeholt haben, andererseits aber auch neue Fehlerkorrekturmethoden (bosonische Codes und effiziente LDPC-Codes). Diese Alternativen haben das Potenzial, schon bald eine Führungsrolle einzunehmen – es aber noch nicht realisiert. Ferner ist die Bewertung teilweise dadurch erschwert, dass viele Akteure aus der Industrie wenig publizieren.

Der große Aufwand der Fehlerkorrektur macht es für akademische und industrielle Labors auf absehbare Zeit unwahrscheinlich und vermutlich auch wirtschaftlich uninteressant, einen kryptographisch relevanten Quantencomputer zu realisieren. Wenn jedoch eine große Industrienation ihre Forschungsanstrengungen auf dieses Ziel konzentrieren würde, ähnlich den Manhattan- und Apollo-Projekten des 20. Jahrhunderts, so erscheint ein Quantencomputer mit wenigen Millionen physikalischer Qubits, der zumindest in 100 Tagen 2048-Bit RSA brechen kann, erreichbar, wenn auch die physikalische Fehlerrate angemessen sinkt und in einen Bereich von 1:10000 gebracht werden kann. Dies wäre eine Großanlage, die in mehrerlei Hinsicht technologische Rekorde benötigen würde und ggf. Zugriff auf seltene Materialien erfordert.

Die Forschung an Quantencomputern entwickelt sich sehr schnell, allerdings vor allen Dingen im Bereich der Qubit-Zahl, während Fortschritt bei den Fehlerraten deutlich langsamer ist. Letzterer ist aber entscheidend, um überhaupt von der Fehlerkorrektur profitieren zu können – wie sich gerade an den neuen Experimenten zeigt, die sich an den Details der Fehlerschwelle abarbeiten.

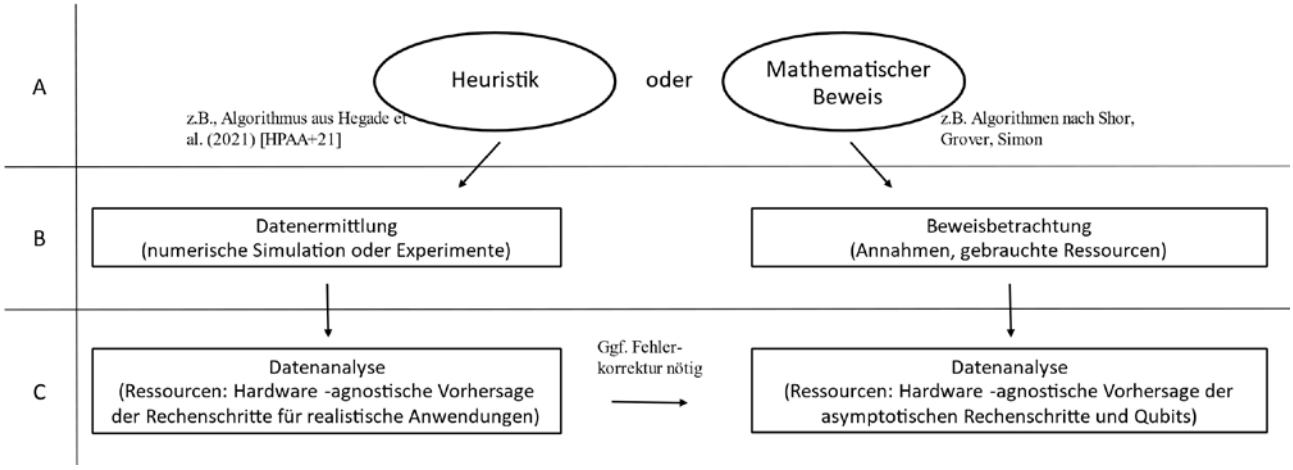

Abbildung 3.3: Schichtenmodell zur Bewertung von Quantencomputer-Algorithmen basierend auf fehlertolerantem Quantencomputing (links) bzw. NISQ (rechts).

4 Jüngste Entwicklungen

Die rasche Entwicklung von Quantencomputern hat ihre Bewertung anhand der Anforderungen der Kryptoanalyse zu einem mehrdimensionalen Unterfangen gemacht.

Auf der Seite der Algorithmen ist der Shor-Algorithmus immer noch der Hauptkandidat mit einer rigorosen Laufzeitanalyse im Hinblick auf einen zugänglichen Quantenvorteil. Stetige Fortschritte bei seiner Implementierung und Kompilierung führen zu einer schrittweisen Verringerung der Hardwareanforderungen, erfordern aber immer noch große Gattertiefen von über einer Billion für RSA 2048-Instanzen. Bei elliptischen Kurven über 256 Bit ist die Situation ähnlich. Andererseits gibt es inzwischen eine breite Palette neuer heuristischer Algorithmen, die oft an bestimmte Rechenmodelle angepasst sind, z. B. adiabatische Quantenberechnungen oder Algorithmen mit geringer Tiefe für kurzfristig realisierbare Hardware, die nicht aktiv fehlerkorrigiert wird. Diese werden zwar oft mit markigen Behauptungen angekündigt, aber keiner von ihnen wird mit einem Konvergenznachweis geliefert, der ein zentraler Bestandteil einer quantitativen Leistungsanalyse wäre. Das beste Surrogat dafür, eine gründliche heuristische Skalierungsanalyse, ist ebenfalls für keinen dieser Algorithmen veröffentlicht worden. Auch wenn sich viele dieser neuen Algorithmen möglicherweise als Nebenprodukt des Quantenhypes herausstellen werden, ist es wichtig, sie weiter zu beobachten und zu bewerten, möglicherweise in einer unabhängigen Benchmarking-Aktivität.

Auf der Seite der Berechnungsmodelle, d. h. der mathematischen Modelle für die Durchführung einer Berechnung, stellen das gatterbasierte und das adiabatische Quantencomputing nach wie vor die wichtigsten Pole dar, doch haben Variationen und Mischformen dieser beiden Modelle an Bedeutung gewonnen, oft in Verbindung mit den Hardware-Plattformen, an die sie angepasst sind. Die meisten dieser Modelle sind in Bezug auf ihre Berechnungskomplexität gleichwertig. Allerdings ist die quantitative Leistungsanalyse eine größere Herausforderung, insbesondere die Identifikation von Komponenten-Leistungsdaten, die es erlauben, größere Systeme beliebiger Plattformen zu vergleichen. Besonders erwähnenswert unter diesen nicht standardisierten Rechenmodellen sind diejenigen, die mit dem photonischen Quantencomputing in Verbindung gebracht werden, wie das Gaußsche Boson-Sampling und das fusionsbasierte Quantencomputing.

Selbst innerhalb des Modells der gatterbasierten Quantenrechner ist die Unterscheidung zwischen fehlertoleranten Quantencomputern auf der Grundlage der Quantenfehlerkorrektur und der verrauschten Quanteninformatik im mittleren Maßstab (NISQ) entscheidend. Ersteres hat eine gut etablierte Leistung, aber einen großen Overhead, während letzteres effiziente nicht-fehlerkorrigierte Algorithmen von geringer Tiefe beschreibt, die in der Regel eine externe klassische Optimierung beinhalten. Letztere ermöglichen den Zugang zu einer reichhaltigeren Gattermenge und die gemeinsame Entwicklung von Software und Hardware, was bei kleinen Problemfällen oft zu einer überraschend guten Leistung führen kann. Aufgrund der unbekannten Skalierung dieser Algorithmen und auf der Grundlage größerer theoretischer Argumente ist es jedoch unwahrscheinlich, dass im NISQ-Bereich ein kryptoanalytischer Quantenvorteil erreicht werden kann. Dies unterstreicht den allgemeinen Punkt, dass Fehler derzeit das begrenzende Merkmal der gatterbasierten Quantencomputertechnologie sind – und nicht die Anzahl der Qubits.

Der Bereich der Quantenfehlerkorrektur hat in ähnlicher Weise große Fortschritte gemacht: Treiber der groß angelegten Entwicklung, der Surface Code und die Color Codes, werden schrittweise in Form von effizienteren Decodern optimiert, die ihren Overhead reduzieren und Details verbessern. Andererseits könnten Techniken zur Fehlervermeidung auf niedriger Ebene oder neue Codes aus der Familie der Low-Density-Parity-Check-Codes zu schnelleren Fortschritten in diesem Bereich führen, die sich dramatisch auf unsere Extrapolation auswirken – diese sind jedoch nicht hinreichend ausgearbeitet. Auf der experimentellen Seite werden diese Fehlerkorrekturcodes in immer größeren Versuchsaufbauten getestet, und der Fehlerkorrekturfahrplan wird immer weiter umgesetzt – etwas langsamer als erwartet, aber ohne Rückschläge und mit klaren weiteren technologischen Schritten. Die am weitesten fortgeschrittenen Experimente demonstrieren die Wirksamkeit der erweiterten Fehlerkorrekturcodes und zeigen einige erste fehlerkorrigierte Gatteroperationen. Bemerkenswerterweise erreichen sie nicht die Gewinnschwelle, d. h. sie führen nicht zu einem Gatterfehler des korrigierten Gatters (oder Speichers), der niedriger ist als der der physikalischen Operation. Dies zeigt, wie schwierig es ist, realistische Fehlerraten mit einer Vielzahl von

Fehlermechanismen mit einem einzigen durchschnittlichen Fehler zu vergleichen, wie er in der Fehlerkorrekturtheorie angenommen wird. Die Angleichung dieser Aktivitäten ist auf dem Weg, und die nächsten Jahre werden Informationen liefern, um dies realistischer zu bewerten.

Nach aktuellem Stand ist der Surface Code der optimale Fehlerkorrekturcode für supraleitende Qubits. Für ionische Systeme ist der Color Code gegenüber dem Surface Code vorteilhaft. Es gibt zwar vielversprechende Entwicklungen bei den LDPC-Codes, aber für einen klaren Vergleich fehlen wesentliche Komponenten und Analysen - insbesondere Auswertungen geeigneter Decoder und damit zuverlässige Schwellenwertschätzungen. Nur wenn diese Lücken geschlossen werden, können solche neuartigen Codes einen Einfluss auf die Entwicklung von fehlertolerantem Quantencomputing haben. Entwicklungen aus dem NISQ-Bereich wie Fehlermitigation skalieren nicht in dem Sinn, dass sie nach aktuellem Stand für die großen Aufgaben der Kryptoanalyse nennenswerte Alternativen darstellen würden.

Im Juni 2023 hat IBM den Stand der Technik bei der Demonstration des Quantenvorteils auf vielen Ebenen erheblich verbessert, Konsequenzen in Bezug auf Quantenüberlegenheit werden debattiert. IBM hat einen vollständig programmierbaren Prozessor von beispielloser Größe (127 Qubits) mit einem durchgängig sehr niedrigen Zwei-Qubit-Fehler verwendet. Anstelle einer synthetischen Aufgabe des Samplings eines Schaltkreises haben sie ein Problem aus der Simulation von Quantenmagneten als Benchmark-Algorithmus verwendet - der immer noch recht gut an die klassische Hardware angepasst ist. Insbesondere wurde dieses Resultat mit Techniken der Fehlermitigation anstelle von Fehlerkorrektur erreicht. Bei der Fehlermitigation handelt es sich um eine Methode, die es ermöglicht, den Fehler von NISQ-Quantenprozessoren zu reduzieren, ohne das vollständige Programm des fehlertoleranten Quantencomputings zu implementieren, indem der Fehler des Algorithmus durch die Ausführung mehrerer Versionen diagnostiziert und diese Informationen dann zur Korrektur der Ausgabe verwendet werden. Die bekannten Methoden zur Fehlerbegrenzung sind nicht skalierbar. Die Arbeit von IBM hat bekannte Fehlermitigationsmethoden auf ein neues Niveau gebracht. Dieses Ergebnis unterstreicht die Notwendigkeit, eine niedrige Fehlerquote mit der Größe des Prozessors zu kombinieren, um die Fehlerbegrenzung effizient zu gestalten. Bei gleicher Fehlerrate hätten mehr Qubits das Ergebnis nicht verbessert.

Diese Arbeit ist ein bedeutender technischer Fortschritt auf vielen Ebenen. Vor allem zeigt sie das Potenzial der Fehlerminderung, den Break-even-Punkt des Quantencomputers deutlich zu verbessern. Es ist nicht zu erwarten, dass dies so weit geht, dass ein fehlerreduzierter Shor-Algorithmus die Kryptographie im NISQ-Zeitalter beeinflusst, aber wenn es eine NISQ-freundlichere Alternative gäbe (die wir bisher nicht identifiziert haben), würde dies das Feld voranbringen und eine weitere Dimension in unserem Bewertungssystem schaffen.

Auf dem Gebiet der Plattformen für Quantencomputer sind Prozessoren basierend auf Supraleitern bzw. gefangenen Ionen immer noch klare Spitzenreiter. Trotz unterschiedlicher Basisparameter – supraleitende Prozessoren haben kürzere Kohärenzzeiten, aber schnellere Operationen als Ionenfallenprozessoren – ist ihre algorithmische Leistung erstaunlich ähnlich. Beide Plattformen haben Fortschritte gemacht – Supraleiter zeigen stetige Fortschritte als Systeme mit nur geringen Fortschritten bei den Kohärenzzeiten, Ionen arbeiten an der Skalierung in dem Sinne, dass sie ihre starke Leistung in linearen Fallen auch in zweidimensionalen Anordnungen reproduzieren können. Es ist ein wichtiger aktueller Trend, dass mehr Plattformen aufholen. Auf der Festkörperseite erreichen Halbleiter-Qubits in kleinen Systemen eine hohe Fidelität, die sich noch nicht auf die Skalierung auswirkt (und es gibt bemerkenswerte Vielfalt bei der Identifizierung der führenden Halbleiterplattform), aber jetzt scheint es so weit zu sein, dass es keine grundlegenden Hindernisse für weiteren Fortschritt gibt. Auf der atomaren Seite haben neutrale Atome in Rydberg-Zuständen – ursprünglich eine Plattform für Quantensimulationen, d.h. nicht-universelle Quantenberechnungen – große Fortschritte bei bestimmten Klassen von NISQ-Algorithmen gemacht und betreten nun das Feld der Quantencomputer-Plattformen mit vielen Qubits. Sie sind zwar noch nicht auf dem Niveau der Spitzenreiter bei Standardkomponenten-Benchmarks, könnten aber bald problemlos skalieren. Schließlich gibt es Berichte über große Fortschritte bei photonischen Qubits, insbesondere im Bereich des Gauß-Boson-Samplings und potenziell anderer photonenangepasster Berechnungsmodelle wie Fusionsgatter – sie können jedoch nicht genau bewertet werden, da relevante Akteure die Leistung von Komponenten und Teilsystemen nicht veröffentlichen. Topologische Qubits haben nach einer Kontroverse über die Datenselektion in hoch angesehenen Arbeiten einen Rückschlag erlitten.

Die Normung von Quantentechnologien wird auf europäischer und internationaler Ebene von mehreren Standardisierungsorganisationen vorangetrieben, wobei die Aktivitäten in den letzten Jahren stark zugenommen haben. Diese Initiativen bestehen aus offenen Gemeinschaften mit Vertretern aus dem privaten und öffentlichen Sektor, die die Perspektiven von Wissenschaft, Industrie und Politik abdecken. So hat beispielsweise die Focus Group on Quantum Technologies von CEN/CENELEC vor kurzem ihre Roadmap zu Quantentechnologien veröffentlicht.[1] Auf der Grundlage dieser Arbeit wurde im Jahr 2023 das neue CEN/CENELEC JTC 22 gegründet, das nun Normen aus der Bedarfsanalyse ableitet. Zusammen mit Aktivitäten von ETSI werden diese europäischen Normungsinitiativen dazu beitragen, auf internationaler Ebene in bestehenden und zukünftigen Komitees bei ISO/IEC, ITU, IEEE und anderen Standardisierungsorganisationen mitzuwirken und somit eine starke Vertretung Europas zu schaffen. Ein Teil der Normungsarbeit zu Quantencomputern ist auf Benchmarks ausgerichtet, die in dieser Studie diskutiert werden, sowie auf eine Aufschlüsselung der einzelnen Komponenten, die sich auf die Diskussion der technischen Anforderungen an Quantencomputer in dieser Studie bezieht (siehe Teil IV).

Die Quanteninformatik wird derzeit in öffentlich-privaten Partnerschaften verschiedener Art betrieben. Starke kommerzielle Akteure, die in der Lage (und willens) sind, die Systemintegration in großem Maßstab selbst durchzuführen, stehen auf den Schultern von Programmen des öffentlichen Sektors. An diesen Programmen sind Universitäten und Forschungsinstitute, aber auch Unternehmen beteiligt. Erfolgreiche Akteure bringen eine integrierte Sichtweise auf Software und Hardware mit, was für frühe Technologien wichtig ist, und die Fähigkeit, schrittweises Engineering mit risikoreicher Forschung zu verbinden. Sie benötigen Personen, die in der Lage sind, hochwertige Ingenieurleistungen mit Quantenkenntnissen und der erforderlichen interdisziplinären Denkweise zu verbinden, was im Allgemeinen schwer zu finden ist. Geografisch gesehen kommen die beeindruckendsten Ergebnisse von nordamerikanischen Akteuren. Europa kommt schnell voran und nutzt sein technologisches Potenzial seit dem Start des EU-Quantenflaggschiffs und der damit verbundenen nationalen Initiativen viel besser als in der Vergangenheit. Vor allem in China sind inzwischen viele beeindruckende Leistungen zu verzeichnen, die oft quantitativ weltweit führend sind, auch wenn sie qualitativ (noch) kein Neuland betreten. Australien und Japan sind starke Akteure in bestimmten Bereichen, und es gibt eine Reihe bemerkenswerter Aktivitäten in anderen Ländern, darunter Indien, Brasilien, Argentinien und Südafrika. Das russische Quantenprogramm hat (recht vernünftig) versucht, die traditionelle Stärke der Wissenschaft aus der Sowjetära mit der Zusammenarbeit mit Forschern aus anderen Ländern zu verbinden. Dieses wurde 2022 eingestellt, und Russland ist jetzt bestenfalls ein kleiner Akteur.

[1] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

5 Fazit

Mit Blick auf die Zukunft lautet die Schlussfolgerung der Studie einerseits, dass die Quanteninformatik stetige Fortschritte in Richtung kryptoanalytische Relevanz macht, die nach dem etablierten Mainstream (fehlertoleranter Shor-Algorithmus, der entweder auf einem supraleitenden System mit dem Surface Code oder einem ionenbasierten System mit dem Color Code ausgeführt wird) mindestens ein Jahrzehnt, wahrscheinlicher zwei, dauern wird - sofern keine Disruptionen stattfinden. Andererseits gibt es inzwischen eine Fülle neuer Entwicklungen bei den Algorithmen im NISQ-Bereich, aber auch der Fehlerkorrektur und -mitigation sowie der Hardware, von denen noch keine einen echten Durchbruch darstellt. Das bedeutet aber, dass der Zehn-Jahres-Horizont deutlich wahrscheinlicher werden kann, sollten sich hier aktuelle heuristische Ergebnisse verfestigen.

Auch die Vielfalt der Akteure und Ansätze macht Vorhersagen schwierig. Unternehmen hüten einige Komponenten ihrer Technologie als Geschäftsgeheimnis - einige, selbst große Unternehmen, arbeiten im Stealth-Modus. Die Quanteninformatik wird aus Gründen der Wettbewerbsfähigkeit oder der nationalen Sicherheit gehütet, so dass einige Entwicklungen natürlich vertraulich bleiben. Es ist zwar unwahrscheinlich, dass die als geheim eingestufte Forschung in qualitativer Hinsicht weit voraus ist, doch könnte sich dies in Zukunft ändern.