Quantumcomputing: Funktionsweise und weitere Entwicklung

Joshua Mähl, Danny Marcel Kröger

Nordakademie - Hochschule der Wirtschaft
Köllner Chaussee 11
25337 Elmshorn
joshua.maehl@nordakademie.de
danny_marcel.kroeger@nordakademie.de

1 Einleitung

Die Entwicklung eines Quantencomputers hat das Potenzial, viele Bereiche zu revolutionieren. Von der Pharmaindustrie bis zum Bankwesen sind Einsatzzwecke denkbar, für deren Kalkulationen klassische Computer nicht geeignet sind [CCB18]. Die ersten Unternehmen, wie der Automobilhersteller BMW [Ju21] oder das Pharmaunternehmen Boehringer Ingelheim [Bo21] sind Partnerschaften mit Honeywell respektive Google eingegangen, um den Einsatz von Quantencomputern zu erforschen und voranzutreiben.
Hieraus kann gefolgert werden, dass das Thema Quantencomputing in der Wirtschaft an Relevanz gewinnt, um zusammen mit der Wissenschaft praxisorientierte Lösungen zu erforschen.
In dieser Arbeit werden zuerst theoretische Grundlagen erläutert, um eine Basis für weitere Argumentationen zu bilden. Dabei wird zuerst die Funktionsweise eines Quantencomputers dargestellt. Hierbei wird insbesondere auf die elementare Informationseinheit, dem Qubit, sowie für weitere Erläuterungen auf die im Einsatz befindlichen asymmetrischen Verschlüsselungsverfahren eingegangen. Um einen Überblick über derzeitige Entwicklungen und Herausforderungen beim Stand der Forschung zu entwickeln, wird der State of the Art eruiert und hieraus abgeleitet, in welcher Ära des Quantencomputers sich die Wissenschaft derzeit befindet. Weiterhin werden Konzepte dargestellt, die ein effizientes Arbeiten mit einem Quantencomputer ermöglichen. Weitere Entwicklungen, wie die Fehlerkorrektur von Qubits und auch die Nutzung eines physischen Quanten-Arbeitsspeichers, sind für einige Anwendungen unabdingbar und werden deshalb erläutert.
Anhand bereits entwickelter Algorithmen und vielfältig veröffentlichter Arbeiten können bestimmte Chancen und Risiken ermittelt werden, die funktionierende Quantencomputer implizieren. Diese Chancen und Risiken wiederum bieten eine Grundlage für eine wissenschaftliche Positionierung.

2 Theoretische Grundlagen

Das Prinzip des Quantum Computing nutzt ein grundlegend anderes Paradigma als das der klassischen Computer. Um spezielle Berechnungen zu ermöglichen, die mit klassischen Computern in annehmbarer Zeit nicht gelöst werden können, wird sich insbesondere drei grundlegender Eigenschaften der Quantenphysik bedient, die im weiteren Verlauf erläutert werden. [CvK15, Sv18, TQ19a]
Die kleinste Einheit der Information analog zum Bit im klassischen Computer wird Qubit (oder Quantum Bit) genannt. Während ein Bit in der CPU eines klassischen Computers daraus besteht, ob eine elektrische Spannung herrscht oder nicht, gibt es unterschiedliche Arten, Qubits physisch zu realisieren. Dies wird in Kapitel 3 näher erläutert.
Es gibt heute zwei Arten, um mit Qubits zu rechnen. Die erste Variante, die beispielsweise vom Unternehmen D-Wave benutzt wird, ist das Quantum Annealing. Hierbei werden die Qubits so ausgerichtet, dass spezielle Minimierungsprobleme gelöst werden können. Dabei müssen die Daten insofern vorbereitet werden, dass der Quantencomputer die Daten versteht und ein Ergebnis berechnen kann. [DH17] Ein grundlegend anderes Prinzip, mit dem universale Berechnungen durchgeführt werden können, ist das Quantengatter-Modell. Hierbei werden wie bei herkömmlichen Computern unterschiedliche Gatter verwendet, die den Zustand der eingesetzten Qubits verändern.[Mu19] Aufgrund der Universalität der Berechnungen des Quantengatter-Modells wird dieses Verfahren im Paper näher erläutert.
Jeder Quantenalgorithmus, der auf Quantencomputern auf Basis des Quantengatter-Modells ausgeführt wird, besteht aus initialisierten Anfangszuständen der Qubits, meistens im Zustand 1 oder 0, den Gattern, die einzelne oder mehrere Qubits manipulieren, sowie aus der Messung des Endzustands nach Ausführung des Algorithmus. [DH17, BH17, HS17]
Der entscheidende Unterschied zum klassischen Computer bei der Berechnung von Algorithmen liegt im quantenmechanischen Effekt der Quantenüberlagerung. Die Quantenüberlagerung beschreibt, dass ein Qubit sich in mehreren Zuständen gleichzeitig befinden kann. Dieser Zustand, als ψ bezeichnet, wird mathematisch wie in Formel 1 beschrieben. Dabei ist die Wahrscheinlichkeit, dass sich ein Qubit bei der Messung im Zustand 0 befindet $|\alpha|^2$, respektive beträgt die Wahrscheinlichkeit, dass sich das Qubit im Zustand 1 befindet $|\beta|^2$, wobei $\alpha, \beta \in \mathbb{C}$. Die Dirac-Notation $|0\rangle$ und $|1\rangle$ steht hierbei für Spaltenvektoren $(10)^T$ und $(01)^T$. [BH17, Sv18]

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

Zur Visualisierung des Status eines einzelnen Qubits wird hierbei die Bloch-Sphäre verwendet, auf dessen Oberfläche sich die Zustandsbeschreibung des Qubits befindet. Der dreidimensionale Raum wird hierbei verwendet, um die komplexen Zahlen, in denen sich α, und β befinden können, abzubilden. Hierbei ist der Nordpol der Sphäre als Zustand 0 definiert, der Südpol als Zustand 1. Jede Anwendung eines 1-Qubit-Quantengatters rotiert hierbei den Zustand $|\psi\rangle$ auf der Oberfläche der Bloch-Sphäre.
Die Eigenschaft der Quantenüberlagerung kann verwendet werden, um Berechnungen auf allen überlagerten Zuständen gleichzeitig auszuführen. Dies wird auch als Parallelismus bezeichnet. [BH17, Sv18] Hiermit können beispielsweise bei einem Quantencomputer mit zwei Qubits vier

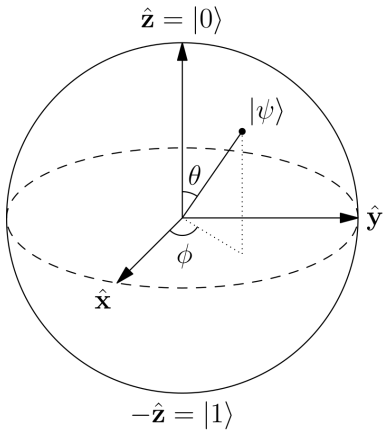

Abbildung 2.1: Bloch-Sphäre, auf dessen Oberfläche sich die Zustandsbeschreibung eines Qubits befindet
Quelle: Von Glosser.ca - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=23263326, Zugriff am 18.08.2021

Zustände gleichzeitig dargestellt werden: 00, 01, 10, 11. Eine Anwendung eines Quantengatters auf einen oder mehreren dieser Qubits verändert alle vier Zustände. Um dieses Verhalten mit einem klassischen Computer darzustellen, sind vier Operationen notwendig. Aufgrund der exponentiell steigenden Anzahl darstellbarer Zustände (2^n, n = Anzahl der Qubits), leiten Mohseni et al. ab, dass ein Quantencomputer mit 49 Qubits nicht auf einem klassischen Computer darstellbar ist [Mo17]. Häner und Steiger haben in 2017 einen 45-Qubit-Quantencomputer mithilfe eines Supercomputers und eines Speichers von 500 Terabytes simuliert. Eine Simulation von Quantencomputern ist insbesondere in der Entwicklungsphase von Relevanz, da hierdurch validiert werden kann, ob Quantencomputer wie erwartet rechnen. [HS17]
Der letzte Schritt eines jeden Quantenalgorithmus ist das Messen der Qubits. Dabei verfällt die Überlagerung in die klassischen Zustände 0 oder 1. Durch mehrfaches Ausführen des Algorithmus ergibt sich eine Wahrscheinlichkeitsverteilung mit den oben genannten Wahrscheinlichkeiten $|\alpha|^2$ und $|\beta|^2$.
Zwei weitere grundlegende quantenphysikalische Konzepte, die bei Quantencomputern zum Einsatz kommen, sind die Quantenverschränkung und Quanteninterferenz. Bei der Quantenverschränkung ist der Zustand eines Qubits mit dem Zustand eines oder mehrerer anderer Qubits so miteinander verbunden, dass die Messung eines Quantenbits den Zustand der anderen Qubits determiniert. Die so hergestellte Verbindung ist nach dem Aufbau örtlich unabhängig. Die folgende Formel 2 zeigt den Sachverhalt zweier quantenverschränkter Qubits mathematisch auf. Hierbei steht $|0_1 0_0\rangle$ dafür, dass, wenn sich das erste Qubit (0_0) im Zustand 0 befindet, das zweite Qubit (0_1) ebenso in Zustand 0 befindet. [TQ19a]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2}$$

Die Quanteninterferenz wird in vielen Algorithmen verwendet, um das erwünschte Ergebnis konstruktiv und unerwünschte Ergebnisse destruktiv zu interferieren. Neben der Beschreibung physischer Qubits unterscheidet man zudem logische Qubits, die als eine fehlertolerante Einheit

mehrerer im Verbund befindlicher physischer Qubits erklärt werden [TQ19b].
Einen algorithmischen Einsatz quantenmechanischer Effekte der Überlagerung und Interferenz bietet der Entwurf eines Datenbank-Such-Algorithmus von Grover aus 1996. Hiermit kann die Komplexität von Datenbanksuchen unsortierter Datensätze von $O(N)$ auf $O(\sqrt{N})$ beschleunigt werden, wobei N die Anzahl an Datensätzen ist. [Gr96]
Weiterhin hat Peter Shor in 1994 einen Quantenalgorithmus entwickelt, der insbesondere im digitalen Zeitalter von Relevanz ist. Ein für klassische Computer bisher nicht in annehmbarer Zeit lösbares Problem ist das Faktorisieren von großen Zahlen, welches durch quantenmechanische Effekte exponentiell beschleunigt werden kann. [Sh94, GE21]
Das RSA-Verschlüsselungsverfahren sowie der Diffie-Hellmann-Key-Exchange nutzen einen öffentlichen und einen unterschiedlichen privaten Schlüssel. Mit dem öffentlichen Schlüssel werden Nachrichten verschlüsselt. Die verschlüsselten Nachrichten können nur mithilfe des privaten Schlüssels entschlüsselt werden. Durch Faktorisierung des öffentlichen Schlüssels kann jedoch der private Schlüssel berechnet werden. Gidney und Ekerå zeigen eine theoretische Faktorisierung eines RSA-2048-Schlüssels mithilfe eines Quantencomputers, welche ca. 8 Stunden mit 20 Millionen Qubits in Anspruch nehmen würde. [GE21] Ein derzeitiger Supercomputer würde für diese Faktorisierung mehrere Milliarden Jahre in Anspruch nehmen. [Ar19] Die Beschleunigung der Faktorisierung stellt ein sicherheitsrelevantes Problem für die Nutzung der meistverbreiteten asymmetrischen Verschlüsselungsverfahren dar.

3 Stand der Forschung und weitere Entwicklung

Der State of the Art im Bereich Quantum Computing wird durch die Betrachtung der Eigenschaften der bereits existierenden und verwendeten Quantencomputer beschrieben. Preskill führt als zusammenfassendes Konzept für den aktuellen Forschungsstand den Begriff „Noisy Intermediate-Scale Quantum“ (NISQ) ein, der einen Quantencomputer mit einer Rechenkapazität zwischen 50 und mehreren Hundert Qubits definiert [Pr18]. Der enthaltende Begriff Noise beschreibt sämtliche Interferenzen, die Qubit-Zustände nach kurzer Zeit zerstören [ASAG19]. Ash-Saki et al. bezeichnen diesen zeitlichen Zerfall als Dekohärenz [ASAG19]. Als Folge dieses Zerfalls sei eine Reduzierung der Qubit-„Qualität“ zu betrachten, wodurch das Zeitintervall für die Verwendung von Qubits für Berechnungen auf den Millisekunden-Bereich eingeschränkt wird [Pr18]. Wie von Preskill vorhergesagt, haben mehrere Unternehmen und Institutionen in der Aktualität Quantencomputer entwickelt, die den Eigenschaften eines NISQ-Computers entsprechen. Laut Hassija et al. sind folgende Unternehmen die „leading organisations“ im Bereich der Quantencomputerforschung: Google, IBM, D-Wave, HRL, Microsoft und Xanadu u.a. [Ha20]. Hierbei werden unterschiedliche Hardware-Technologien verwendet, wie supraleitende Schaltungen, Kernspinresonanz oder isolierte Ionen [Ha20]. In diesem Kontext wird der Stand der Forschung anhand der supraleitenden Schaltungen untersucht, da dieses Feld die größte Anzahl an aktiven Forschungen und Entwicklungen darstellt.[Ha20]
Quantencomputer mit supraleitenden Schaltungen im NISQ-Zeitalter verwenden annähernd widerstandslose Materialen wie Aluminium, die auf niedrigste Temperaturen nahe des absoluten

Nullpunkts ($<$ 1 Kelvin) abgekühlt werden. Damit wird ein Zustand erschaffen, in dem Qubits, abgesehen von externen Interferenzen, fehlerfrei funktionieren [Ha20]. Das US-Unternehmen IBM stellt seine Quantencomputer mit dieser Technologie her [Ha20]. Diese NISQ-Geräte reichen von einer Anzahl von 1 bis 127 Qubits und befinden sich an verschiedenen Standorten weltweit, wo sie u.a. durch eine Cloud-Anbindung von Forschenden sowie der Öffentlichkeit über ein interaktives Menü oder per Softwareentwicklung (Python) programmiert werden können. Ein beispielhaftes Experiment testet eine durch Quantengatter programmierte Additionsschaltung auf mehreren unterschiedlichen IBM-Quantencomputern. Das Experiment zeigt, dass nur einer der getesteten Quantencomputer ein konstant korrektes Ergebnis berechnet, während die restlichen Rechner in 50% der Fälle fehlerhaft addieren. Eine Erhöhung auf eine 2-Qubit-Schaltung verschlechtert das Ergebnis signifikant. [MC20]
Eine weitere aktuell verwendete Technologie ist das Quantum-Annealing, welches wie in Kapitel 2 angesprochen insbesondere durch den von D-Wave entwickelten Quantencomputer bekannt ist. Diese verwendet ebenfalls supraleitende Schaltungen und wendet unterschiedliche physikalische Prozesse auf die Qubits an, um deren Zustand zu verändern, ohne hierbei Quantengatter zu verwenden [Ay21]. Auf diese Weise wurde ein NISQ-Rechner entwickelt („Advantage“), der 5000 Qubits bereitstellt [AHF20]. Ähnlich wie beim Quantengatter-Modell werden die Qubits am Ende des Algorithmus gemessen. Viele Qubits erreichen bei der Messung jedoch nicht das erforderliche Energielevel, um korrekt ausgelesen zu werden. [Ay21] Durch Regulierung der Energielevel der Teilchen bieten Ayanzadeh et al. einen Ansatz zur Single- und Multi-Qubit-Correction [Ay21], um die hohe Anzahl an Qubits effektiv nutzen zu können.
Durch die beschriebene fehlende Persistenz der Qubit-Zustände und ineffizienter Qubit-Fehlerkorrektur sind weitere datenverarbeitende und -speichernde Quanten-Hardwarekomponenten wie Arbeitsspeicher und Festplatten bisher lediglich simulierbar. Während einige Algorithmen kein Laden der Daten aus einem Quanten-Arbeitsspeicher (qRAM) benötigen, ist dies bei anderen eine Voraussetzung für die Anwendung des Überlagerungsprinzips (siehe Kapitel 2) [Ve20].
Neben den beschriebenen Forschungsfragen bei der Bereitstellung von Hardware für Quantencomputer ist ein Entwurf für die Erstellung und Nutzen von spezieller Quantencomputer-Software notwendig. Im Zusammenhang mit den genannten Shor- und Grover-Algorithmen (siehe Kapitel 2) sind weitere spezielle Algorithmen, wie z. B. zur Nutzung der Hardware, und Programmierparadigmen etabliert. Auf der Konferenz „1st International Workshop on Quantum Software“ wurde sich auf allgemeingültige Quantum Software Engineering Prinzipien, wie z. B. eine Agnostik (Neutralität) gegenüber bestehenden Programmiersprachen und die Sicherstellung einer Koexistenz zwischen klassischen und Quantencomputern, geeinigt [PPPC20].
Auf Basis des State of the Art lässt sich eine Abschätzung für weitere Entwicklungen durchführen, die ebenfalls Teil des aktuellen wissenschaftlichen Diskurses sind. Grundvoraussetzung für signifikante Fortschritte ist das Lösen der in diesem Abschnitt beschriebenen Probleme und das einhergehende Verlassen der NISQ-Ära. Langione et al. skizzieren den Fortschritt im Quantum Computing wie in Abbildung 3.1 für die Anwendung in der Pharmaindustrie [La19].
Die Abbildung 3.1 zeigt, dass das gegenwärtige NISQ-Zeitalter zeitnah verlassen werden kann, nachdem der Meilenstein der Fehlerkorrektur erreicht wird. Das Szenario der „Full-scale fault tolerance“ stellt den weitesten Horizont mit einer integrierten, modularen Quantenrechnerarchitektur dar. Cavaliere et al. sehen noch keine kosteneffizienten Einsatzmöglichkeiten für Quan-

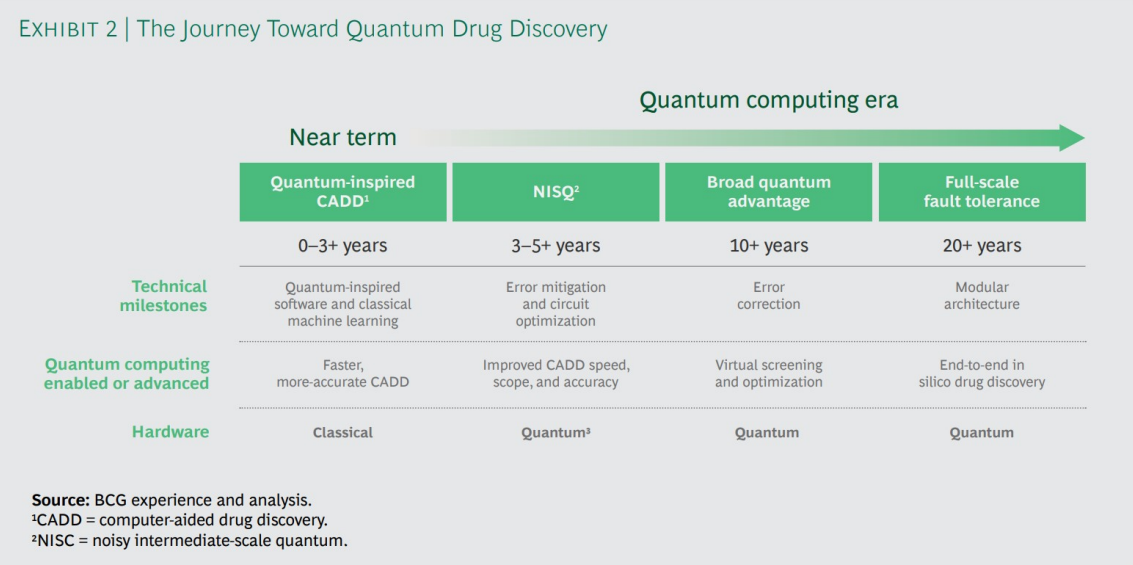

Abbildung 3.1: Meilensteine im Pharmabereich für den Einsatz von Quantencomputing [Ma19]

tencomputer, weisen jedoch auf das wachsende Leistungsvermögen der entstandenen Rechner hin [CMS20]. Diese Sprünge weisen ein Moore's Law überlegenes überexponenzielles Wachstum auf, welche Cavaliere et al. als Neven's Law (nach dem Quantenforscher Hartmut Neven) bezeichnen [CMS20]. Unter diesen Voraussetzungen ist eine Einsatzfähigkeit und Erfüllung des abgebildeten Zeitplans möglich.

4 Potenzielle Anwendungen eines Quantencomputers

4.1 Chancen

Nachdem der State of the Art im Bereich Quantum Computing dargestellt und auf dessen Basis die mittel- und langfristige Leistungsfähigkeit abgeschätzt wurde, ist eine Betrachtung der Anwendungsszenarien notwendig. Das Ausnutzen der Parallelität sehen Hughes et al. als Hauptvorteil gegenüber klassischen Computern [Hu21, S. 81]. Wie in Kapitel 2 aufgezeigt, bietet der Grover-Algorithmus hierbei eine Lösung, um Datenbanksuchen mit einer Komplexität $O(\sqrt{N})$ durchzuführen, die nur einen Bruchteil der aktuell notwendigen Rechenkosten darstellt. Auf Basis der Parallelität lassen sich zudem weitere Optimierungen finden. Harwood et al. stellen quantenrechnerbasierte Algorithmen vor, die im Logistikbereich für eine Optimierung der Wegrouten und benötigten Transportmittel eingesetzt werden können [Ha21]. Während ein klassischer Computer alle möglichen Transportwege und -mittel sequenziell berechnet und bei komplexen Sachverhalten an limitierter Rechenleistung scheitert, kann ein Quantencomputer durch die Quantenüberlagerung alle Auswahlmöglichkeiten gleichzeitig betrachten. Dies würde ebenfalls zu einer Lösung des in der klassischen Informatik offenen Problems des Handelsreisenden

führen.
Eine weitere durch Quantencomputer ermöglichte Chance ist die Simulation komplexer Sachverhalte. Eine Branche, die von der Rechenleistung der Quantencomputer profitieren kann, ist die Pharmaindustrie, die sich hierdurch einen signifikanten Forschungssprung erhofft. Preskill beschreibt, dass die Simulation von komplexen Molekülen wie Proteinen zur Erschaffung neuer Medikamente führen könnte, um bisher unheilbare Krankheiten bekämpfen zu können [Pr18]. Zudem biete eine Simulation der Quantenphysik durch Qubits die weitere Möglichkeit, das Verständnis der Quantenphysik zu erhöhen. Simulationen der Quantenphysik lassen sich durch klassische Computer bisher nicht ausreichend darstellen. [Pr18]
Des Weiteren ergeben sich effiziente Anwendungsbereiche im Finanzwesen. Egger et al. untersuchen publizierte Quantencomputer-Algorithmen und sehen durch die Simulation von Preisentwicklungen Vorteile bei der Bestimmung von Preisen von Derivaten und Investmentoptimierungen [Eg20]. Ein wichtiger Aspekt bei der Betrachtung von potenziellen Vorteilen wird von Preskill dargestellt: Im Zeitalter der NISQ-Computer (siehe Kapitel 3) besteht kein Beweis aus den beschriebenen Wirtschaftsbereichen, die eine effektive Wirksamkeit und Einsetzbarkeit nachweisen, sondern nur theoretische Studien [Pr18]. Hinzu kommt, dass dieser Faktor der Ungewissheit auch weitere Chancen für noch nicht erforschte Bereiche aus Wirtschaft und Wissenschaft darstellt - ähnlich wie die ständige Erkundung neuer Möglichkeiten während der Weiterentwicklung des klassischen Computers.

4.2 Risiken

Wie bereits im Kapitel 2 beschrieben, hat ein funktionierender Quantencomputer mit genügend Qubits die Möglichkeit, derzeitige im Einsatz befindliche Public-Key-Verschlüsselungen innerhalb weniger Stunden zu entschlüsseln. Die Tabelle 1 gibt einen Überblick über derzeit verwendete Verschlüsselungs- und Hashalgorithmen, von denen die asymmetrischen Verfahren durch den Einsatz von Quantencomputern unter anderem durch Shor's Algorithmus generell als unsicher eingeschätzt werden. Die Implikationen hieraus sind ein unsicherer Datenverkehr fast aller etablierter Internetanwendungen, inklusive Banksysteme, Krankenversicherungssysteme etc. [Mo20] Auch kann ein solches Ausspähen dazu genutzt werden, Geheiminformationen von Staaten und Unternehmen zu beschaffen, die mit öffentlichen Schlüsseln verschlüsselt sind. Damit ist das Erstellen der und das Schützen vor Quantencomputern ein Wettlauf gegen die Zeit.
Das National Institute of Standards and Technology (NIST), welches bereits das symmetrische Verschlüsselungsverfahren AES etablierte, begann 2017 das Projekt „Post-Quantum Cryptography". Diese Verfahren sollen selbst dann Sicherheit bzw. Verschlüsselung gewährleisten, wenn Quantencomputer kommerziell genutzt werden können [Ch17]. Zum aktuellen Zeitpunkt befindet sich das Verfahren in der dritten Runde, um einen Public-Key-Algorithmus als neuen Standard auszuwählen [Al19]. Selbst wenn es einen Algorithmus gibt, mit dem quantencomputersichere Public-Key-Verschlüsselungsverfahren ermöglicht werden, bedeutet dies nicht, dass dieser auch sofortige Anwendung findet. So sind auch in anderen IT-Sicherheitsbereichen viele öffentlich bekannte Sicherheitslücken lange Zeit nicht geschlossen, oftmals durch fehlendes Patchen dieser [Em20]. Daher sollte ein solcher Algorithmus, insofern dieser als sicher emp-

Algorithmus	Symm./ Asymm.	Einsatz	Sicherheit bei funktionierenden Quantencomputern
AES-256	Symm.	Verschlüsselung	Sicher
SHA-256, SHA-3	-	Hash-Funktionen	Sicher
RSA	Asymm.	Signaturen Schlüsseleinrichtung	Unsicher
ECDSA ECDH (Elliptic Curve Cryptography)	Asymm.	Signaturen Schlüsselaustausch	Unsicher
DSA (Finite Field Cryptography)	Asymm.	Signaturen Schlüsselaustausch	Unsicher

Tabelle 1: Einschätzung der Sicherheit eingesetzter Verschlüsselungs-und Hashalgorithmen nach Einführung von Quantencomputern [Ma18]

funden wird, Jahre vor der kommerziellen Nutzung von Quantencomputern technisch umgesetzt werden. Wie bereits mit alten Standards geschehen ist, sollten die Software-Hersteller die Verwendung veralteter Verschlüsselungs-Verfahren frühzeitig unterbinden.
Zusätzlich zum Risiko der Entschlüsselung kritischer Daten bergen Quantencomputer die Gefahr, dass die erste Volkswirtschaft, die einen einsatzfähigen Quantencomputer besitzt und die Ressourcen für die Entwicklung von Quantenalgorithmen aufweisen kann, einen technologischen Vorteil gegenüber anderen Ländern haben wird. Die Chancen aus Kapitel 4.1 könnten dazu genutzt werden, um die eigene Überlegenheit eines Landes auszubauen. Dies wirft ethische Fragen auf, ob eine Entwicklung eines Quantencomputers für eine weitere Disparität des technologischen Fortschritts für Kontinente wie Afrika sorgen werden. [Pe21]

5 Positionierung und Fazit

Das vorherige Kapitel 4 zeigt einige der Chancen und Risiken auf, die mit dem Einsatz von nutzbaren Quantencomputern entstehen können. Das Risiko der potenziellen Berechnung der privaten Schlüssel in asymmetrischen Verschlüsselungsverfahren stellt eine ernstzunehmende Gefahr dar. Diese kann jedoch rechtzeitig abgewehrt werden, indem die derzeitigen Standards ersetzt werden. Das NIST stellt hier in den kommenden Jahren Vorschläge für eine quantensichere asymmetrische Verschlüsselung bereit. Die symmetrischen Verschlüsselungsverfahren, insbesondere AES-256, sind laut diverser Untersuchungen trotz Quantencomputern nicht in annehmbarer Zeit entschlüsselbar. Besonders kritische Informationen sind bereits oder sollten anhand dieses Verfahrens gesichert werden. Um einen Einsatz neuer Algorithmen und Technologien zu ermöglichen, muss die Öffentlichkeit rechtzeitig über die Gefahren der Quantencomputer aufgeklärt und neue Verschlüsselungsverfahren schnellstmöglich implementiert werden.
Durch die genannten Chancen, die im Kapitel 4.1 erläutert werden, sollte aufgrund eines be-

hebbaren Risikos nicht von der Entwicklung eines Quantencomputers abgesehen werden. Insbesondere durch die Erforschung neuartiger Medikamente, die bisher vielfach durch langwierige Experimente oder per Zufall entdeckt wurden, bieten Quantencomputer ein ungeahntes Potenzial, den Wohlstand der gesamten Weltbevölkerung zu erhöhen. Weiterhin sind die Einsatzmöglichkeiten des Quantencomputers bisher nur bedingt erforscht. Dennoch ist alleine das Potenzial Grund genug, um die Forschung an Quantencomputern voranzutreiben.
Bis zum vollwertigen Einsatz eines Quantencomputers sind noch einige Probleme zu beheben. Ob die bisherigen Quantencomputer genug skalierbar sind, wird sich nur zeigen, indem weiter daran geforscht wird. Die vielversprechenden Ansätze zur Optimierung der Hardware und Software eines Quantencomputers, siehe Kapitel 3, können die Forschung positiv vorantreiben. Durch den globalen und kommerziellen Wettbewerb zur Herstellung von Quantencomputern beschleunigt sich die Entwicklung derzeit rasant.

Literatur

[AHF20] Ayanzadeh, Ramin; Halem, Milton; Finin, Tim: Reinforcement Quantum Annealing: A Hybrid Quantum Learning Automata. Scientific Reports, 10(1):7952, 2020.

[Al19] Alagic, Gorjan; Alperin-Sheriff, Jacob; Apon, Daniel; Cooper, David; Dang, Quynh; Liu, Yi-Kai; Miller, Carl; Moody, Dustin; Peralta, Rene; Perlner, Ray; Robinson, Angela; Smith-Tone, Daniel: Status report on the first round of the NIST post-quantum cryptography standardization process. `https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf`, 2019, Stand 15.08.2021.

[Ar19] Arute, Frank; Arya, Kunal; Babbush, Ryan; Bacon, Dave; Bardin, Joseph C.; Barends, Rami; Biswas, Rupak; Boixo, Sergio; Brandao, Fernando G. S. L.; Buell, David A.; Burkett, Brian; Chen, Yu; Chen, Zijun; Chiaro, Ben; Collins, Roberto; Courtney, William; Dunsworth, Andrew; Farhi, Edward; Foxen, Brooks; Fowler, Austin; Gidney, Craig; Giustina, Marissa; Graff, Rob; Guerin, Keith; Habegger, Steve; Harrigan, Matthew P.; Hartmann, Michael J.; Ho, Alan; Hoffmann, Markus; Huang, Trent; Humble, Travis S.; Isakov, Sergei V.; Jeffrey, Evan; Jiang, Zhang; Kafri, Dvir; Kechedzhi, Kostyantyn; Kelly, Julian; Klimov, Paul V.; Knysh, Sergey; Korotkov, Alexander; Kostritsa, Fedor; Landhuis, David; Lindmark, Mike; Lucero, Erik; Lyakh, Dmitry; Mandrà, Salvatore; McClean, Jarrod R.; McEwen, Matthew; Megrant, Anthony; Mi, Xiao; Michielsen, Kristel; Mohseni, Masoud; Mutus, Josh; Naaman, Ofer; Neeley, Matthew; Neill, Charles; Niu, Murphy Yuezhen; Ostby, Eric; Petukhov, Andre; Platt, John C.; Quintana, Chris; Rieffel, Eleanor G.; Roushan, Pedram; Rubin, Nicholas C.; Sank, Daniel; Satzinger, Kevin J.; Smelyanskiy, Vadim; Sung, Kevin J.; Trevithick, Matthew D.; Vainsencher, Amit; Villalonga, Benjamin; White, Theodore; Yao, Z. Jamie; Yeh, Ping; Zalcman, Adam; Neven, Hartmut; Martinis, John M.: Quantum supremacy using a programmable superconducting processor. Nature, 574(7779):505–510, 2019.

[ASAG19] Ash-Saki, Abdullah; Alam, Mahabubul; Ghosh, Swaroop: QURE: Qubit Re-Allocation in Noisy Intermediate-Scale Quantum Computers. In: Proceedings of the 56th Annual Design Automation Conference 2019. DAC '19, Association for Computing Machinery, New York, NY, USA, 2019.

[Ay21] Ayanzadeh, Ramin; Dorband, John; Halem, Milton; Finin, Tim: Multi-qubit correction for quantum annealers. Scientific Reports, 11(1):16119, 2021.

[BH17] Britt, Keith A.; Humble, Travis S.: High-Performance Computing with Quantum Processing Units. ACM Journal on Emerging Technologies in Computing Systems, 13(3):1–13, 2017.

[Bo21] Boehringer Ingelheim: Partnerschaft bei Quantencomputern für Pharmaforschung — Presse. https://www.boehringer-ingelheim.de/pressemitteilung/partnerschaft-mit-google-bei-quantencomputern, 22.08.2021, Stand 22.08.2021.

[CCB18] Caleffi, Marcello; Cacciapuoti, Angela Sara; Bianchi, Giuseppe: Quantum internet. In (Benediktsson, Jon Atli; Dressler, Falko, Hrsg.): Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication. ACM, New York, NY, USA, S. 1–4, 09052018.

[Ch17] Chase, Melissa; Derler, David; Goldfeder, Steven; Orlandi, Claudio; Ramacher, Sebastian; Rechberger, Christian; Slamanig, Daniel; Zaverucha, Greg: Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. In (Thuraisingham, Bhavani, Hrsg.): CCS'17. Association for Computing Machinery, New York, NY, S. 1825–1842, 2017.

[CMS20] Cavaliere, Fabio; Mattsson, John; Smeets, Ben: The security implications of quantum cryptography and quantum computing. Network Security, 2020(9):9–15, 2020.

[CvK15] Chien, Chia-Hung; van Meter, Rodney; Kuo, Sy-Yen: Fault-Tolerant Operations for Universal Blind Quantum Computation. ACM Journal on Emerging Technologies in Computing Systems, 12(1):1–26, 2015.

[DH17] Dinneen, Michael J.; Hua, Richard: Formulating graph covering problems for adiabatic quantum computers. In: Proceedings of the Australasian Computer Science Week Multiconference. ACM, New York, NY, USA, S. 1–10, 01302017.

[Eg20] Egger, Daniel J.; Gambella, Claudio; Marecek, Jakub; McFaddin, Scott; Mevissen, Martin; Raymond, Rudy; Simonetto, Andrea; Woerner, Stefan; Yndurain, Elena: Quantum Computing for Finance: State-of-the-Art and Future Prospects. IEEE Transactions on Quantum Engineering, 1:1–24, 2020.

[Em20] Emrah Yasasin; Julian Prester; Gerit Wagner; Guido Schryen: Forecasting IT security vulnerabilities – An empirical analysis. Computers & Security, 88:101610, 2020.

[GE21] Gidney, Craig; Ekerå, Martin: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. https://quantum-journal.org/papers/q-2021-04-15-433/pdf/, 2021, Stand 15.08.2021.

[Gr96] Grover, Lov K.: A fast quantum mechanical algorithm for database search. In (Miller, Gary L., Hrsg.): Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, New York, NY, S. 212–219, 1996.

[Ha20] Hassija, Vikas; Chamola, Vinay; Saxena, Vikas; Chanana, Vaibhav; Parashari, Prakhar; Mumtaz, Shahid; Guizani, Mohsen: Present landscape of quantum computing. IET Quantum Communication, 1(2):42–48, 2020.

[Ha21] Harwood, Stuart; Gambella, Claudio; Trenev, Dimitar; Simonetto, Andrea; Neira, David; Greenberg, Donny: Formulating and Solving Routing Problems on Quantum Computers. IEEE Transactions on Quantum Engineering, PP:1, 2021.

[HS17] Häner, Thomas; Steiger, Damian S.: 0.5 petabyte simulation of a 45-qubit quantum circuit. In (Mohr, Bernd; Raghavan, Padma, Hrsg.): Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis. ACM, New York, NY, USA, S. 1–10, 11122017.

[Hu21] Hughes, Ciaran; Isaacson, Joshua; Perry, Anastasia; Sun, Ranbel; Turner, Jessica: Quantum Computing for the Quantum Curious. 2021.

[Ju21] Jung, Jakob: Quantencomputing: BMW kooperiert mit Honeywell. https://www.zdnet.de/88391466/quantencomputing-bmw-kooperiert-mit-honeywell/, 28.01.2021, Stand 22.08.2021.

[La19] Langione, Matt; Bobier, Jean-François; Meier, Christoph; Hasenfuss, Sebastian; Schulze, Ulrik: Will Quantum Computing Transform Biopharma R&D? Boston Consulting Group, 2019.

[Ma18] Mavroeidis, Vasileios; Vishi, Kamer; D., Mateusz; Jøsang, Audun: The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3), 2018.

[Ma19] Matt Langione; Jean-François Bobier; Christoph Meier; Sebastian Hasenfuss; and Ulrik Schulze: Will Quantum Computing Transform Biopharma R&D? https://image-src.bcg.com/Images/BCG-Will-Quantum-Computing-Transform-Biopharma-R-and-D-Dec-2019_tcm9-236195.pdf, 2019, Stand 15.08.2021.

[MC20] Methachawalit, Wiphoo; Chongstitvatana, Prabhas: Adder Circuit on IBM Universal Quantum Computers. In: 7th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), S. 92–95. 2020.

[Mo17] Mohseni, Masoud; Read, Peter; Neven, Hartmut; Boixo, Sergio; Denchev, Vasil; Babbush, Ryan; Fowler, Austin; Smelyanskiy, Vadim; Martinis, John: Commercialize quantum technologies in five years. Nature, 543(7644):171–174, 2017.

[Mo20] Mone, Gregory: The Quantum Threat. Commun. ACM, 63(7):12–14, 2020.

[Mu19] Murali, Prakash; Linke, Norbert Matthias; Martonosi, Margaret; Abhari, Ali Javadi; Nguyen, Nhung Hong; Alderete, Cinthia Huerta: Full-stack, real-system quantum computer studies. In (Manne, Srilatha; Hunter, Hillery; Altman, Erik, Hrsg.): Proceedings of the 46th International Symposium on Computer Architecture. ACM, New York, NY, USA, S. 527–540, 06222019.

[Pe21] Perrier, Elija: , Ethical Quantum Computing: A Roadmap, 2021.

[PPPC20] Piattini, Mario; Peterssen, Guido; Pérez-Castillo, Ricardo: Quantum Computing. ACM SIGSOFT Software Engineering Notes, 45(3):12–14, 2020.

[Pr18] Preskill, John: Quantum Computing in the NISQ era and beyond. Quantum, 2:79, 2018.

[Sh94] Shor, P. W.: Algorithms for quantum computation: discrete logarithms and factoring. In (Goldwasser, Shafi, Hrsg.): Proceedings / 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Soc. Pr, Los Alamitos, Calif., S. 124–134, 1994.

[Sv18] Svore, Krysta; Roetteler, Martin; Geller, Alan; Troyer, Matthias; Azariah, John; Granade, Christopher; Heim, Bettina; Kliuchnikov, Vadym; Mykhailova, Mariia; Paz, Andres: Q#. In (Unknown, Hrsg.): Proceedings of the Real World Domain Specific Languages Workshop 2018 on - RWDSL2018. ACM Press, New York, New York, USA, S. 1–10, 2018.

[TQ19a] Tannu, Swamit S.; Qureshi, Moinuddin K.: Not All Qubits Are Created Equal. In (Bahar, Iris; Herlihy, Maurice; Witchel, Emmett; Lebeck, Alvin, Hrsg.): Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems. ACM, New York, NY, USA, S. 987–999, 04042019.

[TQ19b] Tannu, Swamit S.; Qureshi, Moinuddin K.: Mitigating Measurement Errors in Quantum Computers by Exploiting State-Dependent Bias. In: Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture. ACM, New York, NY, USA, S. 279–290, 10122019.

[Ve20] Veras, Tiago M. L.; de Araujo, Ismael C. S.; Park, K. Daniel; Dasilva, Adenilton J.: Circuit-based quantum random access memory for classical data with continuous amplitudes. IEEE Transactions on Computers, S. 1, 2020.

6 Autoren der Kapitel

Joshua Mähl: Kapitel 1, 3, 4.1
Danny Kröger: Kapitel 2, 4.2, 5