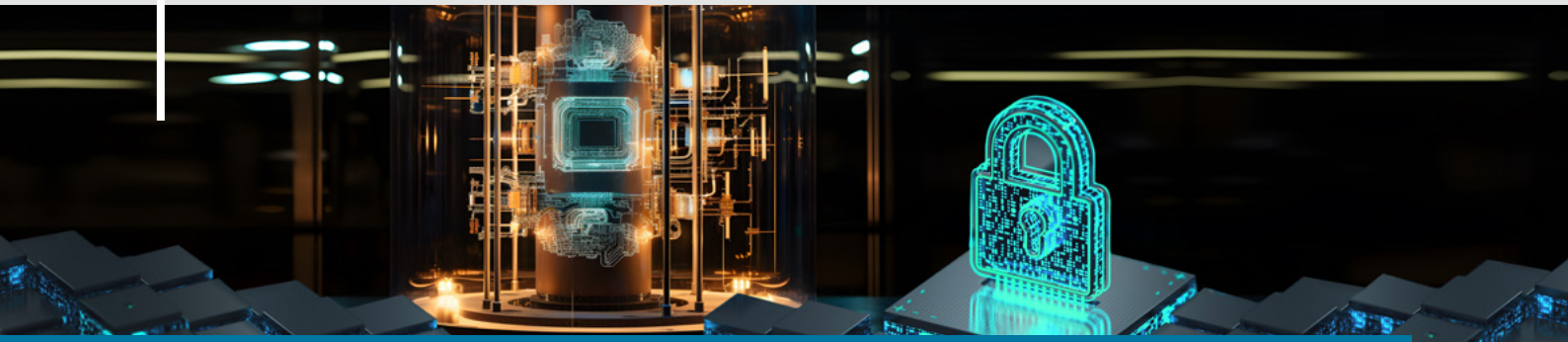

Collage: Patrick Helmholz/AdobeStock und BlackJack3D/iStock

QUANTENCOMPUTER UND IHR EINFLUSS AUF DIE CYBERSICHERHEIT

Impulspapier | März 2024

Zusammenfassung

Quantencomputing ermöglicht nicht nur viele wichtige Anwendungen, sondern bedroht auch die kryptografischen Verfahren, die heute die Grundlage für Cybersicherheit bilden. Dieses Impulspapier gibt erst einen Überblick über die wichtigsten Quantenalgorithmen und den derzeitigen Stand der Quantencomputerhardware, um darauf aufbauend das Gefährdungspotenzial für die aktuell verwendeten kryptografischen Verfahren zu beschreiben. Die Post-Quanten-Kryptografie sowie die Kryptoagilität werden als wichtige Schutzmaßnahmen gegen Angriffe, die durch Quantencomputer möglich werden (Quantenangriffe), herausgestellt und die Notwendigkeit einer sehr zügigen Migration zu den neuen Verfahren wird betont.

1 Einleitung

Die Entwicklung von Quantencomputern macht seit einigen Jahren rasante Fortschritte. Die sogenannte Quantenüberlegenheit (Quantum Advantage) wurde möglicherweise 2019 schon erreicht: Google hat ein sehr spezielles Problem mit einem Quantencomputer schneller gelöst, als dies mit einem klassischen Supercomputer möglich gewesen wäre. IBM hat Ende 2023 einen Quantencomputer mit 1.121 Qubits präsentiert. Solche zunehmend leistungsfähigen Quantencomputer sind jedoch nicht nur nützlich, etwa bei der Untersuchung von Fragestellungen der Quantenchemie, sondern bedrohen auch unsere derzeitige Informationsinfrastruktur.

Dieses Impulspapier gibt einen Überblick über den technischen Stand der Quantencomputer sowie Einschätzungen über künftig daraus resultierende Gefährdungen. Andere Quantentechnologien, wie etwa die Quantensensorik, die sogenannte Seitenkanalangriffe verbessern könnte, werden bewusst ausgelassen. Die betrachteten Gegenmaßnahmen fokussieren auf kryptografische Verfahren, die nach derzeitigem Stand des Wissens sicher gegen Quantenangriffe sind. Quantentechnologien, wie etwa die Quantenkryptografie, die die Informationssicherheit erhöhen können, werden ebenfalls nicht betrachtet, da auf diesem Gebiet noch einige Zeit an den Grundlagen geforscht werden wird und eine Marktreife noch nicht absehbar ist. Ein wichtiges Fazit des Papiers ist, dass kryptografische Verfahren als Maßnahmen gegen die Bedrohung durch Quantencomputer existieren und die Migration zu solchen Verfahren schnellstmöglich beginnen muss. Dies ist von zentraler Bedeutung, da Angriffe nach der Art von „store now, decrypt later“ die Informationssicherheit schon heute bedrohen.

2 Arten von Quantenalgorithmen

Obwohl es einen „Zoo“ an Quantenalgorithmen gibt[1], sind für praktische Anwendungen nur wenige Algorithmen bekannt. Um die Gefahr, die von Quantencomputern auf die Informationssicherheit ausgeht, zu beschreiben, genügt es, zwei Quantenalgorithmen zu fokussieren.

Der Algorithmus von Shor ist der bekannteste Algorithmus. Er erlaubt das effiziente Faktorisieren großer Zahlen und kann damit beispielsweise das RSA-Verfahren brechen. Eine Variante des Shor-Algorithmus findet zudem effizient sogenannte diskrete Logarithmen und kann damit auch den Diffie-Hellman-Schlüsselaustausch sowie das Verschlüsselungsverfahren ElGamal brechen. Verfahren, die durch den Shor-Algorithmus gebrochen werden, werden in einer Quantenwelt vollständig unsicher. Daher müssen völlig andere kryptografische Verfahren verwendet werden. Solche Verfahren werden mit dem Begriff Post-Quanten-Kryptografie bezeichnet.

Der Algorithmus von Grover erlaubt es, die Suche in einer unsortierten Datenbank von etwa N Schritten (für eine Datenbank mit N Einträgen) auf Quadratwurzel von N Schritte zu reduzieren. Dies ist erstaunlich, allerdings handelt es sich nicht um eine exponentielle, sondern nur um eine quadratische Beschleunigung. Solange der Algorithmus von Grover der einzige Angriff auf ein Verschlüsselungsverfahren ist, sollte eine Anpassung der Schlüssellänge auf 256 Bit als Gegenmaßnahme genügen.

Nicht unerwähnt bleiben sollten zwei weitere Quantenalgorithmen, die mit einer geringeren Wahrscheinlichkeit eine Gefahr für die Informationssicherheit darstellen.

Der Algorithmus von Simon erlaubt es für eine Funktion, deren Funktionswerte sich in einem bestimmten Abstand wiederholen, diesen Abstand zu ermitteln. Es gibt sehr spezielle symmetrische Verschlüsselungsverfahren, die diese Eigenschaft haben. Solche Verfahren gelten daher nicht als quantensicher und sollten nicht mehr zum Einsatz kommen. Es ist allerdings wichtig festzuhalten, dass Angreifende den Algorithmus von Simon in dieser Weise nur nutzen können, wenn sie das Verschlüsselungsgerät in Superposition anfragen (Superpositionsangriffe). Wie weiter unten beschrieben, ist dies unrealistisch. Demzufolge besteht auf längere Sicht keine Gefahr und daher aktuell kein Handlungsbedarf.

Der Algorithmus von Harrow, Hassidim und Lloyd (HHL) erlaubt es, Informationen über die Lösung eines großen linearen Gleichungssystems exponentiell schneller zu erfahren als mit allen herkömmlichen Algorithmen, allerdings nicht die Lösung selbst. Angesichts der weiten Verbreitung linearer Gleichungssysteme sind viele Anwendungen denkbar. Problematisch ist aber, dass das Gleichungssystem dafür in einen Quantenzustand codiert werden muss, was den Geschwindigkeitsvorteil ggf. wieder wettmachen kann. Zusätzlich muss das Gleichungssystem dünn besetzt sein, d. h. sehr häufig den Wert Null enthalten. Die Erwartungen an den HHL-Algorithmus und die Hoffnung, ihn für Quantum Machine Learning einsetzen zu können, sind hoch, daher sollte man die zukünftige Entwicklung hier genau verfolgen. Derzeit sind aber noch keine Angriffe auf die Informationssicherheit mit dem HHL-Algorithmus bekannt.

Fazit: Quantencomputer sind nicht prinzipiell schneller als klassische Rechner, sondern es gibt Quantenalgorithmen, die einige Probleme schnell lösen können. Dazu gehören zwei für die Kryptografie wesentliche mathematische Probleme. Quantensichere Verfahren müssen daher auf alternativen mathematischen Problemen basieren. Diese werden weiter unten beschrieben.

3 Arten von Quantencomputern

Das NISQ-Regime
Für die oben beschriebenen Quantenalgorithmen benötigt man einen Quantencomputer, der über viele tausend sogenannte logische Qubits verfügt. Noch ist die Quantentechnologie jedoch nicht so weit. Aktuelle Quantencomputer sind sogenannte NISQ-Rechner. Dabei steht NISQ für Noisy Intermediate Scale Quantum Computing, d. h. für Quantencomputer mit wenigen hundert physikalischen Qubits, auf denen nur kurze Berechnungen möglich sind, weil dann das Rauschen die Ergebnisse überlagert. NISQ-Rechner können bei sehr speziellen Problemen klassischen Rechnern zwar schon überlegen sein, für die Informationssicherheit stellen sie nach heutigem Kenntnisstand jedoch noch keine Bedrohung dar.

Skalierbare Quantencomputer benötigen Fehlerkorrektur
Sobald die Quantenfehlerkorrektur gut genug wird, gibt es einen Punkt, ab dem beliebig lange Quantenberechnungen möglich werden (Fault Tolerant Computing). Geschätzt wird nach aktuellem Stand der Forschung, dass es ca. tausend physikalische Qubits bedarf, um ein stabiles logisches Qubit zu realisieren. Ein Quantencomputer, der etwa den Algorithmus von Shor ausführt, würde damit ungefähr 1.000.000 Qubits benötigen. Andere Ansätze, die näher am NISQ-Regime sind, gehen von 20.000.000 Qubits aus.

Quantum Annealing und adiabatische Quantencomputer
Adiabatische Quantencomputer sind ein völlig anderes Berechnungsmodell als die Gatter-basierten Modelle, in denen die oben genannten Quantenalgorithmen formuliert sind. Bei adiabatischen Berechnungen werden Zustände minimaler Energie so transformiert, dass sie zur Lösung eines Optimierungsproblems werden. Ideale adiabatische Quantencomputer sind universell und können somit prinzipiell jede Quantenberechnung ausführen.

Praktisch realisiert wurden bisher sehr spezielle (und imperfekte) adiabatische Berechnungen durch sogenannte Quantum Annealer, die von der Firma D-Wave kommerziell vertrieben werden. Die Quantencomputer von D-Wave verfügen über sehr viele Qubits (aktuell 5.600), die aber nicht universell verwendet werden können, da keine beliebigen adiabatischen Berechnungen möglich sind. Ein Annealer kühlt einen Quantenzustand, in dem die Qubits eine von der Rechnerarchitektur festgelegte Wechselwirkung haben, langsam, um einen Zustand minimaler Energie bei diesen Wechselwirkungen zu erzeugen. Dieser Quantenzustand ist dann die Lösung eines sehr speziellen Optimierungsproblems. Der Quantum Annealer nutzt quantenmechanische Überlagerung und Tunneleffekte, um das Optimum schneller zu finden, als es klassisch möglich ist. Bisher sind keine Bedrohungen für die Informationssicherheit durch Quantum Annealer bekannt.

Bausteine für Quantencomputer
Welche Technologie für Quantencomputer verwendet wird, sagt einiges darüber aus, wann mit Quantencomputern zu rechnen ist. Hierzu gibt es klare Roadmaps, beispielsweise der Firmen IBM und Google. Diese Roadmaps wirken sehr optimistisch, was für die grundsätzliche Einschätzung der

Gefahren, die von Quantencomputern ausgehen, positiv zu sehen ist. Denn es geht dabei nicht darum, wann der erste Quantencomputer der Öffentlichkeit präsentiert wird, sondern wann ein Quantencomputer prinzipiell einsatzfähig ist – auch in Bereichen, die der Öffentlichkeit verborgen sind. Im Folgenden werden nur die derzeit vielversprechendsten Ansätze beschrieben; einen umfassenden Überblick bietet die Studie „Entwicklungsstand Quantencomputer" des Bundesamts für Sicherheit in der Informationstechnik (BSI)[2].

Supraleitende Qubits:
Die Umsetzung supraleitender Qubits beruht auf existierender Chiptechnologie. Die Qubits müssen stark gekühlt werden und sind zudem sehr fehleranfällig. Es wird davon ausgegangen, dass zwischen 100 und 1.000 Qubits benötigt werden, um mit Fehlerkorrektur ein einzelnes logisches Qubit zu implementieren. IBM und Google setzen auf diesen Ansatz. Die Quantenüberlegenheit (Quantum Advantage) wurde mit supraleitenden Qubits demonstriert.

Ionenfallen:
Der damit realisierte Ansatz beruht auf Ionen, die in einer magnetischen Falle gefangen sind, kontrolliert miteinander wechselwirken und über Laserlicht manipuliert werden können. Die Qubits sind relativ stabil und optimistische Schätzungen der Firma IonQ gehen davon aus, dass wenige Qubits genügen, um ein einzelnes logisches Qubit zu realisieren. IonQ verfolgt diesen Ansatz.

Topologische Quantenbits:
Topologische Quantenbits ermöglichen einen sehr vielversprechenden Ansatz, da diese Qubits inhärent stabiler sind und somit weniger Fehlerkorrektur benötigen. Microsoft setzt sehr stark auf diesen Ansatz. Leider ist es bisher nicht gelungen, die Existenz dieser Qubits nachzuweisen.

Photonische Qubits:
Hierfür werden die Quanteninformationen in Photonen codiert. Lineare Operationen sind mit den Photonen einfach zu realisieren, nichtlineare Wechselwirkung nur sehr schwer. Ein eingeschränktes Modell ist das sogenannte Boson-Sampling-Modell, das als nicht berechnungsuniversell gilt. Die Quantenüberlegenheit (Quantum Advantage) wurde im Boson-Sampling-Modell bereits demonstriert. Das Unternehmen PsiQuantum setzt auf photonische Qubits und will durch Integration der Systeme bis Ende des Jahrzehnts auf 1.000.000 Qubits skalieren.

Roadmaps für die Entwicklung von Quantencomputern zeigen, dass Quantencomputer sehr bald schon realisiert werden könnten. Solche Roadmaps gibt es von IBM[3] und Google[4], aber auch von kleineren Firmen wie der auf Ionenfallen spezialisierten Firma IonQ[5] und der Firma PsiQuantum[6], die auf photonische Qubits setzt. Zusätzlich gibt es eine deutsche Quantenroadmap[7], die von einem Gremium aus Expertinnen und Experten im Auftrag der Bundesregierung erstellt wurde.

Die Roadmaps sind bei Zwischenschritten relativ konkret, bei dem Ziel, einen voll skalierbaren Quantencomputer zu realisieren, sind die Schätzungen etwas unkonkreter, weisen aber allesamt auf das Ende der 20er-Jahre.

Fazit: Übliche Schätzungen aus der Industrie sehen den skalierbaren Quantencomputer also in weniger als 10 Jahren. Im Hochsicherheitsbereich berücksichtigt die Bundesregierung ab Anfang der 30er-Jahre kryptografisch relevante Quantencomputer, was sich mit einer Studie des Global Risk Institute deckt[8]. Da eine Umstellung kryptografischer Standards Zeit braucht und geheime Informationen für einen gewissen Zeitraum relevant bleiben, sollte so schnell wie möglich auf Post-Quanten-Kryptografie umgestellt werden.

4 Gefahren für die Informationssicherheit

Gefahren für die asymmetrische Kryptografie (Public-Key-Kryptografie)
Die Bedrohung für die Public-Key-Kryptografie ist die bekannteste Auswirkung von Quantencomputern. Der Algorithmus von Shor bedroht alle kryptografischen Verfahren, die auf der Schwierigkeit der Faktorisierung oder des diskreten Logarithmus basieren und damit alle derzeit gängigen Schlüsselaustausch- oder Authentisierungsverfahren wie das RSA-Verfahren, den Diffie-Hellman-Schlüsselaustausch sowie das ElGamal-Verfahren. Public-Key-Verschlüsselungsverfahren und digitale Signaturen müssen deshalb künftig auf neuen Annahmen beruhen. Eine kurze Beschreibung dieser neuen kryptografischen Verfahren der Post-Quanten-Kryptografie folgt unten.

Gefahren für die symmetrische Kryptografie (Secret-Key-Kryptografie)
In der symmetrischen Kryptografie, wenn also Sender und Empfänger über einen gemeinsamen geheimen Schlüssel verfügen, oder für Hashfunktionen werden Verfahren eingesetzt, die nicht so stark strukturiert sind, wie es für die Public-Key-Kryptografie nötig ist. Deshalb gilt der Grover-Algorithmus als einziger Angriff auf symmetrische Verfahren, wobei eine Verdoppelung der Schlüssellänge auf 256 Bit die quadratische Beschleunigung des Angriffs ausgleichen kann. Trotzdem ist Vorsicht geboten, denn es gibt spezielle symmetrische Verfahren, bei denen sogenannte Superpositionsangriffe mit dem Simon-Algorithmus möglich sind.

Superpositionsangriffe sind mit Seitenkanalangriffen vergleichbar. Dabei verschaffen sich Angreifende Zugriff auf ein Gerät, in dem vertrauliche Daten, etwa ein Schlüssel, gespeichert sind. Dieses Gerät können Angreifende mit Quanten-Eingaben in Überlagerung abfragen und so beispielsweise den Algorithmus von Grover verwenden, um effizienter zu sein als klassisch mögliche Seitenkanalangriffe. Diese Superpositionsangriffe sind sehr speziell und für die meisten Geräte wahrscheinlich unmöglich. Beispielsweise lässt sich eine Chipkarte, die stark gekühlt wird, nicht in eine Art Quantum Device transformieren. Daher sind Superpositionsangriffe zwar ein interessantes Forschungsthema, aber besteht derzeit kein akuter Handlungsbedarf.

Weitere Gefahren für die Kryptografie

Existierende Sicherheitsanalysen oder kryptografische Sicherheitsbeweise können falsch werden, wenn Angreifende über Quantenfähigkeiten verfügen. Beweise mit der Random-Oracle-Heuristik könnten nicht mehr richtig sein, wenn man nicht berücksichtigt, dass die Anfragen an das Random Oracle in Überlagerung möglich sein müssen. Dies betrifft etwa digitale Signaturen nach dem Fiat-Shamir-Paradigma oder die Fujisaki-Okamoto-Transformation in der Public-Key-Kryptografie. Auch Beweise, die den Zustand des Angreifers mehrfach im selben Zustand benutzen (Rewinding), werden falsch. Dies bedeutet zwar nicht automatisch, dass kryptografische Verfahren sofort unsicher werden, wirft aber Fragen zu den genauen Sicherheitsgarantien auf, die sie bieten können.[9] In diesem Bereich herrscht ein hoher Forschungsbedarf, auch wenn aktuell kein dringender Handlungsbedarf besteht.

5 Schutzmaßnahmen gegen Quantenangriffe

Neue kryptografische Verfahren (Post-Quanten-Kryptografie)

Aufgrund des Algorithmus von Shor benötigt die Post-Quanten-Kryptografie neue Annahmen, von denen Expertinnen und Experten glauben, dass sie selbst mit Quantencomputern nicht gebrochen werden können.

Die bekanntesten Ansätze sind der Vollständigkeit halber kurz aufgezählt, aber nicht näher erläutert.

- Gitter-basierte Verfahren, die auf der Annahme „Learning with Errors“ (LWE) beruhen,
- Verfahren, die auf klassischen fehlerkorrigierenden Codes beruhen, etwa auf der Annahme „Learning Parity with Noise“ (LPN) oder das McEliece-Verfahren, das noch eine zusätzliche Annahme macht,
- Verfahren, die auf polynomialen Gleichungssystemen mit mehreren Variablen beruhen, wie MQ-Verfahren, bei denen MQ für Multivariate Quadratic steht,
- sogenannte isogeniebasierte Verfahren können in der Literatur gefunden werden, gelten aber derzeit nicht mehr als sicher[10],
- Hash-basierte Verfahren, speziell für digitale Signaturen, die als sehr sicher gelten, da ausschließlich Annahmen aus der symmetrischen Kryptografie verwendet werden.

Weiterführende Literatur bietet der Leitfaden „Kryptografie quantensicher gestalten“ des BSI[11].

Die US-amerikanische Standardisierungsorganisation National Institute of Standards and Technology (NIST) hat einen Wettbewerb ausgerufen und 2022 die ersten vielversprechendsten Post-Quanten-Verfahren für Public-Key-Verschlüsselung und digitale Signaturen festlegt. Dabei sind fast alle ausgewählten Verfahren gitterbasiert. In einer vierten Runde sollen nun insbesondere codebasierte Verfahren betrachtet werden. Abgesehen von der NIST-Initiative gibt es weitere wichtige Standardisierungsinitiativen, etwa bei der Internationalen Organisation für Normung ISO (unter Beteiligung des BSI).

Im Bereich neuer kryptografischer Verfahren sind also einige Aktivitäten zu verzeichnen. Es besteht weiterhin ein großer Forschungsbedarf bezüglich der Sicherheit dieser Verfahren. Allerdings ist aktuell kein umfangreicher zusätzlicher Handlungsbedarf erkennbar.

Kryptoagilität bezeichnet die Herangehensweise, kryptografische Verfahren flexibel austauschbar zu machen, sollten Schwächen dieser Verfahren bekannt werden. Eine Herausforderung dabei ist, dass dieser Austausch selbst wieder kryptografisch abgesichert werden muss, damit kein Einfallstor für Angriffe entsteht. Da noch nicht klar ist, welche Post-Quanten-Verfahren sich längerfristig durchsetzen werden, ist Kryptoagilität ein extrem wichtiges Konzept. Unabhängig von Post-Quanten-Verfahren kann mit Kryptoagilität schnell auf neue Erkenntnisse reagiert werden, aber insbesondere die Migration zu Post-Quanten-Verfahren ist eine Chance, bei der Kryptoagilität voranzukommen. Trotzdem besteht hier noch hoher Forschungs- und Entwicklungsbedarf – etwa dahingehend, dass die Hardware zur Beschleunigung kryptografischer Algorithmen flexibler werden muss, wenn man nicht mit jedem Austausch der Verfahren auch die Hardware ändern will. Daher sollte insbesondere ein Rückfall auf effiziente symmetrische Schlüsselaustauschprotokolle, die eine Schlüsselzentrale verwenden, vorgesehen sein, wie beispielsweise Kerberos.

Migration zu quantensicheren Verfahren

Eine kritische Phase, die im Vergleich zu wenig Beachtung findet, ist die Phase des Übergangs, in der sowohl die bisher üblichen Verfahren als auch die neuen Post-Quanten-Verfahren verwendet werden. Hier ergeben sich Kompatibilitäts- und Sicherheitsprobleme. Beispielsweise sind „Downgrade Attacks" eine mögliche Gefahr, bei denen Angreifende eine Kommunikation oder Verbindung absichtlich auf unsichere, veraltete Protokolle oder Verschlüsselungsstandards herabstufen, um Sicherheitslücken auszunutzen. Dem sollte unbedingt vorgebeugt werden, indem die Kompatibilität der neuen zu den alten Verfahren nicht zu lange gegeben sein darf. Ein weiteres Problem ist, dass die neuen Verfahren noch nicht im Detail verstanden sind und heute durchaus noch nicht absehbare Schwächen wie etwa Seitenkanäle aufweisen könnten. Daher bietet es sich an, sogenannte Robust Combiner zu verwenden. Hierbei handelt es sich um hybride Verfahren, die nur gebrochen werden können, wenn sowohl das alte als auch das neue Verfahren unsicher ist. Zudem sollten Übergangslösungen verwendet werden, wie Encrypted Key Exchange (EKE), bei denen ein nicht quantensicherer Schlüsselaustausch mit einem vorverteilten symmetrischen Verfahren überverschlüsselt wird, um diesen vor Quantenangriffen zu schützen.

Fazit: Die Post-Quanten-Kryptografie ist ein wesentlicher Teil der Schutzmaßnahmen gegen Quantencomputer. Wichtig ist aber zusätzlich die Kryptoagilität, die es erlaubt, in Zukunft flexibler auf neue Bedrohungen zu reagieren. Die Sicherheit des Umstellungsprozesses von alten auf neue Verfahren sollte umfassend berücksichtigt werden.

6 Handlungsempfehlungen

Die dringlichsten Handlungsempfehlungen betreffen die Verwendung neuer quantensicherer kryptografischer Verfahren.

1. Die Migration zu quantensicheren Verfahren sollte sofort begonnen werden. Quantencomputer bedrohen auch die Vertraulichkeit von Nachrichten, die in der Vergangenheit verschlüsselt wurden. Die Migration sollte also abgeschlossen sein, lange bevor Quantencomputer Verschlüsselungsverfahren brechen können.
2. Die Migration sollte genutzt werden, um Kryptoagilität umzusetzen. Bei allen kryptografischen Verfahren, also auch bei den neuen quantensicheren Verfahren, besteht das Risiko, dass diese zu irgendeinem Zeitpunkt unsicher werden könnten. Kryptoagilität würde eine schnelle Anpassung an die veränderte Situation erlauben, muss allerdings sorgfältig umgesetzt werden, damit die leichte Austauschbarkeit von kryptografischen Verfahren nicht selbst zu Sicherheitslücken führt. So sollten beispielsweise digitale Signaturen, die Updates als authentisch ausweisen, sehr sicher sein. Hier empfiehlt sich der Einsatz von Hash-basierten Verfahren.
3. In Zukunft sollten quantensichere Schlüsselaustausch- und Authentisierungsverfahren (sogenannte Post-Quanten-Kryptografie) Standard sein. In einer Übergangsphase, solange man noch wenig Erfahrung mit den neuen Verfahren hat, sollten sogenannte hybride Verfahren benutzt werden. Diese verwenden zwei verschiedene kryptografische Ansätze und können nur gebrochen werden, wenn beide Verfahren unsicher sind. So kann eine Kombination eines etablierten, aber nicht quantensicheren Verfahrens und eines neuen, quantensicheren Verfahrens sehr hohe Sicherheit bieten. Die kryptografischen Protokolle, die Schlüsselaustauschverfahren verwenden, um eine sichere Verbindung aufzubauen, müssen an die neuen und hybriden Verfahren angepasst werden.
4. Die symmetrische Verschlüsselung oder Hashfunktionen sind durch Quantencomputer weniger bedroht, weil sie keine durch Quantenalgorithmen ausnutzbare Struktur haben. Aufgrund möglicher Angriffe mittels des Grover-Algorithmus sollte die Schlüssellänge jedoch doppelt so groß sein wie zur Absicherung gegen rein klassische Angriffe notwendig.
5. Sehr zeitnah sollten – wo dies möglich ist – Übergangslösungen realisiert werden, wie etwa eine Kombination von Schlüsselaustauschverfahren mit vorverteilten Schlüsseln. So kann ein Schlüsselaustausch verschlüsselt werden und ist für Angriffe, die durch einen Quantencomputer möglich werden, nicht mehr zugänglich.
6. Forschung und Entwicklung im Bereich der quantensicheren Verfahren müssen gefördert werden. Deutschland und Europa müssen die Bedrohungslage verstehen und die Migration so vorantreiben, dass wir bei Sicherheitstechnik eine technologische Souveränität erreichen. Der Nationale Cyber-Sicherheitsrat (NCSR) sollte über die weiteren Entwicklungen kontinuierlich informiert werden.
7. Auch wenn es in diesem Papier nicht näher betrachtet wurde, haben Quantentechnologien neben der Bedrohung derzeit verwendeter kryptografischer Verfahren noch andere Auswirkungen. Die Quantenkryptografie etwa schafft neue Möglichkeiten, hochsicher zu kommunizieren. Zudem könnte die Quantensensorik verwendet werden, um mit hochpräzisen Messungen Seitenkanalangriffe besser und somit gefährlicher zu machen. Diese Aspekte sollten in der Forschung und Entwicklung genau betrachtet werden. Es besteht jedoch kein Handlungsbedarf mit derselben Dringlichkeit wie in den oben genannten Punkten.

1 quantumalgorithmzoo.org
2 https://www.bsi.bund.de/qcstudie
3 https://www.ibm.com/roadmaps/quantum
4 https://quantumai.google/learn/map
5 https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap
6 https://www.psiquantum.com/approach
7 https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Roadmap-Quantencomputing-bf-C1.pdf
8 https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/
9 https://eprint.iacr.org/2021/571
10 https://eprint.iacr.org/2022/975
11 https://www.bsi.bund.de/PQ-Migration

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Die Wissenschaftliche Arbeitsgruppe wurde im Oktober 2018 gegründet und ist Mitglied des Nationalen Cyber-Sicherheitsrats. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner

Hauptautor des Impulspapiers „Quantencomputer und ihr Einfluss auf die Cybersicherheit“: Prof. Dr. Jörn Müller-Quade